This document is scheduled to be published in the
Federal Register on 10/16/2015 and available online at
http://federalregister.gov/a/2015-25597, and on FDsys.gov

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Part 170

RIN 0991-AB93

2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications

AGENCY: Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services (HHS).

ACTION: Final rule.

SUMMARY: This final rule finalizes a new edition of certification criteria (the 2015 Edition health IT certification criteria or "2015 Edition") and a new 2015 Edition Base Electronic Health Record (EHR) definition, while also modifying the ONC Health IT Certification Program to make it open and accessible to more types of health IT and health IT that supports various care and practice settings. The 2015 Edition establishes the capabilities and specifies the related standards and implementation specifications that Certified Electronic Health Record Technology (CEHRT) would need to include to, at a minimum, support the achievement of meaningful use by eligible professionals (EPs), eligible hospitals, and critical access hospitals (CAHs) under the Medicare and Medicaid EHR Incentive Programs (EHR Incentive Programs) when such edition is required for use under these programs.

DATES: These regulations are effective [INSERT DATE - 90 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER], except for § 170.523(m) and (n), which are effective on April 1, 2016.

The incorporation by reference of certain publications listed in the rule is approved by the Director of the Federal Register as of [INSERT DATE - 90 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER**]**.

FOR FURTHER INFORMATION CONTACT: Michael Lipinski, Office of Policy, Office of the National Coordinator for Health Information Technology, 202-690-7151.

SUPPLEMENTARY INFORMATION:

Commonly Used Acronyms

API	Application Programming Interface
CAH	Critical Access Hospital
CDA	Clinical Document Architecture
CDC	Centers for Disease Control and Prevention
CDS	Clinical Decision Support
CEHRT	Certified Electronic Health Record Technology
CFR	Code of Federal Regulations
CHPL	Certified Health IT Product List
CLIA	Clinical Laboratory Improvement Amendments
CMS	Centers for Medicare & Medicaid Services
CQM	Clinical Quality Measure
EHR	Electronic Health Record
FDA	Food and Drug Administration

HHS	Department of Health and Human Services
HISP	Health Information Service Providers
HIT	Health Information Technology
HITPC	HIT Policy Committee
HITSC	HIT Standards Committee
HL7	Health Level Seven
IG	Implementation Guide
LOINC®	Logical Observation Identifiers Names and Codes
NIST	National Institute of Standards and Technology
ONC	Office of the National Coordinator for Health Information Technology
SDO	Standards Developing Organization
SNOMED CT®	Systematized Nomenclature of Medicine Clinical Terms

Table of Contents

I. Executive Summary
A. Purpose of Regulatory Action
B. Summary of Major Provisions
1. Overview of the 2015 Edition Health IT Certification Criteria
2. Health IT Definitions
3. The ONC Health IT Certification Program and Health IT Module
C. Costs and Benefits
II. Background
A. Statutory Basis
1. Standards, Implementation Specifications, and Certification Criteria
2. HIT Certification Programs
B. Regulatory History
1. Standards, Implementation Specifications, and Certification Criteria Rules
2. Medicare and Medicaid EHR Incentive Programs Rules
3. ONC Health IT Certification Programs Rules
III. Provisions of the Proposed Rule affecting Standards, Implementation Specifications, Certification Criteria, and Definitions
A. 2015 Edition Health IT Certification Criteria
1. Applicability
2. Standards and Implementation Specifications
3. Adopted Certification Criteria

4. 2015 Edition Gap Certification Eligibility Table
5. Not Adopted Certification Criteria
B. Health IT Definitions
1. Base EHR Definitions
2. Certified EHR Technology Definition
3. Common Clinical Data Set Definition
4. Cross-Referenced FDA Definitions
IV. Provisions of the Proposed Rule Affecting the ONC Health IT Certification Program
A. Subpart E – ONC Health IT Certification Program
B. Modifications to the ONC Health IT Certification Program
1. Health IT Modules
2. "Removal" of Meaningful Use Measurement Certification Requirements
3. Types of Care and Practice Settings
4. Referencing the ONC Health IT Certification Program
C. Health IT Module Certification Requirements
1. Privacy and Security
2. Design and Performance (§ 170.315(g))
D. Principles of Proper Conduct for ONC-ACBs
1. "In-the-Field" Surveillance and Maintenance of Certification
2. Transparency and Disclosure Requirements
3. Open Data Certified Health IT Product List (CHPL)
4. Records Retention
5. Complaints Reporting
6. Adaptations and Updates of Certified Health IT
E. "Decertification" of Health IT – Request for Comments
V. Incorporation by Reference
VI. Collection of Information Requirements
VII. Regulatory Impact Statement
A. Statement of Need
B. Overall Impact
1. Executive Orders 12866 and 13563 – Regulatory Planning and Review Analysis
2. Regulatory Flexibility Act
3. Executive Order 13132 -– Federalism
4. Unfunded Mandates Reform Act of 1995
Regulation Text

I. Executive Summary

A. Purpose of Regulatory Action

Building on past rulemakings, we issued a proposed rule ("Proposed Rule") (80 FR 16804) that identified how health IT certification to the proposed 2015 Edition health IT certification criteria could support the establishment of an interoperable nationwide health

information infrastructure. The Proposed Rule reflected stakeholder feedback received through various outreach initiatives, including the regulatory process, and was designed to broadly support the health care continuum through the use of certified health IT. This final rule, taking into account public comments received on the Proposed Rule, continues to focus on the establishment of an interoperable nationwide health information infrastructure, through the same means identified in the Proposed Rule and recited below, but with an additional focus on reducing health IT developer and provider burden as compared to the Proposed Rule. To this end, this final rule will:

- Improve interoperability for specific purposes by adopting new and updated vocabulary and content standards for the structured recording and exchange of health information, including a Common Clinical Data Set composed primarily of data expressed using adopted standards; and rigorously testing an identified content exchange standard (Consolidated Clinical Document Architecture (C-CDA));
- Facilitate the accessibility and exchange of data by including enhanced data export, transitions of care, and application programming interface (API) capabilities in the 2015 Edition Base Electronic Health Record (EHR) definition;
- Establish a framework that makes the Office of the National Coordinator for Health Information Technology (ONC) Health IT Certification Program open and accessible to more types of health IT, health IT that supports a variety of care and practice settings, various HHS programs, and public and private interests;
- Support the Centers for Medicare & Medicaid Services (CMS) Medicare and Medicaid EHR Incentive Programs (EHR Incentive Programs) through the adoption of a set of certification criteria that align with proposals for Stage 3;

- Address health disparities by providing certification: to standards for more granular capture of race and ethnicity; the collection of sexual orientation, gender identity, social, psychological, and behavioral data; for the exchange of sensitive health information (Data Segmentation for Privacy); and for the accessibility of health IT;
- Ensure all health IT presented for certification possess the relevant privacy and security capabilities;
- Improve patient safety by: applying enhanced user-centered design principles to health IT, enhancing patient matching, requiring health IT to be capable of exchanging relevant patient information (e.g., Unique Device Identifiers), improving the surveillance of certified health IT, and making more information about certified products publicly available and accessible;
- Increase the reliability and transparency of certified health IT through surveillance and disclosure requirements; and
- Provide health IT developers with more flexibility, opportunities, and time for development and certification of health IT that supports interoperability, usability, and innovation.

B. Summary of Major Provisions

1. Overview of the 2015 Edition Health IT Certification Criteria

The 2015 Edition health IT certification criteria ("2015 Edition" or "2015 Edition certification criteria") facilitates greater interoperability for several clinical health information purposes and enables health information exchange through new and enhanced certification criteria, standards, and implementation specifications. It incorporates changes that are designed to spur innovation, open new market opportunities, and provide more choices to providers when

it comes to electronic health information exchange. To achieve these goals, new "application access" (also known as "API") certification criteria have been adopted that will require the demonstration of an API that responds to data requests for any one category of the data referenced in the Common Clinical Data Set as well as for all of the data referenced in the Common Clinical Data Set. We note that in response to comments, we have separated this criterion into 3 criteria to provide health IT developers and providers more flexibility. To further validate the continued interoperability of certified health IT and the ability to exchange electronic health information with health IT certified to the 2014 Edition, 2015 Edition, and potentially future editions, a new "transitions of care" certification criterion will rigorously assess a product's ability to create and receive an interoperable C-CDA. We have also adopted certification criteria that both support interoperability and other settings and use cases, such as the "Common Clinical Data Set summary record," "data segmentation for privacy," and "care plan" certification criteria.

We refer readers to section III.A for an overview table (Table 2) of certification criteria adopted in this final rule as compared to the certification criteria proposed in the Proposed Rule and the adopted 2014 Edition. We also refer readers to sections III.A.3 and III.A.5 of this preamble for full discussions of certification criteria adopted as part of the 2015 Edition in this final rule (III.A.3) and the proposed certification criteria not adopted in this final rule (III.A.5).

2. Health IT Definitions

a. Base EHR Definitions

This final rule adopts a Base EHR definition specific to the 2015 Edition (i.e., a 2015 Edition Base EHR definition) at § 170.102 and renames the current Base EHR definition at §

170.102 as the 2014 Edition Base EHR definition. The 2015 Edition Base EHR definition differs from the 2014 Edition Base EHR definition in the following ways:

- It does not include privacy and security capabilities and certification criteria.
- It only includes capabilities to record and export clinical quality measure (CQM) data (§ 170.315(c)(1)) and not other CQM capabilities such as import, calculate, and "report to CMS."
- It includes the 2015 Edition "smoking status" certification criterion as patient demographic and clinical health information data consistent with statutory requirements.[1]
- It includes the 2015 Edition "implantable device list" certification criterion as patient demographic and clinical health information data consistent with statutory requirements.[2]
- It includes the 2015 Edition "API" certification criteria as capabilities that support both the capture and query of information relevant to health care quality and exchange electronic health information with, and integrate such information from other sources.[3]
- It includes the proposed 2015 Edition certification criteria that correspond to the remaining 2014 Edition certification criteria referenced in the "2014 Edition" Base EHR definition (i.e., CPOE, demographics, problem list, medication list, medication

[1] A Base EHR is the regulatory term we have given to what the HITECH Act defines as a "qualified EHR." Our Base EHR definition(s) include all capabilities found in the "qualified EHR." Please see the 2014 Edition final rule (77 FR 54262) for further explanation.
[2] A capability included in the Base EHR definition, which originates from the "qualified EHR" definition found in the HITECH Act.
[3] These are capabilities included in the Base EHR definition, which originate from the "qualified EHR" definition found in the HITECH Act.

allergy list, CDS, transitions of care, data portability, and relevant transport certification criteria). For the transport certification criteria, we include the "Direct Project" criterion (§ 170.315(h)(1)) as well as the "Direct Project, Edge Protocol and XDR/XDM" criterion (§ 170.315(h)(2)) as equivalent alternative means for meeting the 2015 Edition Base EHR definition.

We refer readers to section III.B.1 of this preamble for a more detailed discussion of the 2015 Edition Base EHR definition and to section III.A.3 of this preamble for a full discussion of the criteria that have been included in the Base EHR definition. Of note, the "demographics" certification criterion (§ 170.315(a)(5)) now includes sexual orientation and gender identity as data elements, the "smoking status" certification criterion (§ 170.315(a)(11)) is now only a functional requirement, the "API" criterion has been separated into 3 distinct criteria as mentioned above, and the Direct-related criteria have been updated from "unchanged" to "revised" to incorporate updated and necessary interoperability standards.

As discussed in more detail under the "privacy and security" heading in section IV.C.1 of this preamble, Health IT Modules presented for certification to criteria listed in the 2015 Base EHR definition and other 2015 Edition certification criteria <u>will be</u> subject to the applicable privacy and security criteria for the purposes of certification.

The CQM capabilities noted above as not included in the 2015 Edition Base EHR definition have, however, been included the Certified EHR Technology (CEHRT) definition under the EHR Incentive Programs. We refer readers to the next section ("b. CEHRT definition") for further information and guidance on the relationship of the 2015 Edition Base EHR definition and the 2015 Edition certification criteria with the CEHRT definition. We also refer readers to the CEHRT definition finalized in the EHR Incentive Programs Stage 3 and Modifications final

rule published elsewhere in this issue of the **Federal Register** as the authoritative source for the requirements to meet the CEHRT definition.

b. CEHRT Definition

This final rule removes the CEHRT definition from § 170.102 for the following reasons. The CEHRT definition has always been defined in a manner that supports the EHR Incentive Programs. As such, the CEHRT definition more appropriately resides solely within the EHR Incentive Programs regulations. This is also consistent with our approach in this final rule to make the ONC Health IT Certification Program more open and accessible to other types of health IT beyond EHR technology and for health IT that supports care and practice settings beyond those included in the EHR Incentive Programs. Further, this adds administrative simplicity in that regulatory provisions, which EHR Incentive Programs participants must meet (e.g., the CEHRT definition), are defined within the context of rulemakings for those programs.

We note that the CEHRT definition finalized by CMS continues to include the Base EHR definition(s) defined by ONC, including the 2015 Edition Base EHR definition adopted in this final rule. We also refer readers to Table 4 ("2015 Edition Health IT Certification Criteria Associated with the EHR Incentive Programs Stage 3") found in section III.A.3 of this preamble. Table 4 crosswalks 2015 Edition certification criteria with the finalized CEHRT definition and EHR Incentive Programs Stage 3 objectives. It also identifies mandatory and conditional certification requirements (i.e., the application of certain certification criteria to Health IT Modules) that Health IT Modules presented for certification must meet regardless of the setting or program the Health IT Module is designed to support.

For the full requirements to meet the CEHRT definition under the EHR Incentive Programs, including for years before 2018 and for 2018 and subsequent years, we refer readers

to the EHR Incentive Programs Stage 3 and Modifications final rule published elsewhere in this issue of the **Federal Register**.

c. Common Clinical Data Set

We revised the "Common MU Data Set" definition in § 170.102. We changed the name to "Common Clinical Data Set," which aligns with our approach throughout this final rule to make the ONC Health IT Certification Program more open and accessible to other types of health IT beyond EHR technology and for health IT that supports care and practice settings beyond those included in the EHR Incentive Programs. We also changed references to the "Common MU Data Set" in the 2014 Edition (§ 170.314) to "Common Clinical Data Set."

We revised the definition to account for the new and updated standards and code sets we have adopted in this final rule for the 2015 Edition that will improve and advance interoperability through the exchange of the Common Clinical Data Set. We also revised the definition to support patient safety and improve care through clearly referenced data elements ("care plan data") and the inclusion of new patient data (e.g., Unique Device Identifiers (UDIs) and immunizations (with standards)). These revisions will <u>not</u> change the standards, codes sets, and data requirements specified in the Common Clinical Data Set for 2014 Edition certification, which remain unchanged. They only apply to health IT certified to the 2015 Edition certification criteria that reference the Common Clinical Data Set.

We refer readers to section III.B.3 of this preamble for a detailed discussion of the Common Clinical Data Set and a table listing the data and standards included in the Common Clinical Data Set for both the 2014 and 2015 Editions.

3. The ONC Health IT Certification Program and Health IT Module

We have changed the name of the ONC HIT Certification Program to the "ONC Health IT Certification Program." We have also modified the ONC Health IT Certification Program in ways that will make it more accessible to other types of health IT beyond EHR technology and for health IT that supports care and practice settings beyond the ambulatory and inpatient settings. These modifications will also serve to support other public and private programs that may reference the use of health IT certified under the ONC Health IT Certification Program. When we established the certification program (76 FR 1262)[4], we stated our initial focus would be on EHR technology and supporting the EHR Incentive Programs, which at the time, focused on the ambulatory setting and inpatient setting (76 FR 1294).

This final rule permits other types of health IT, such as technology implemented by health information service providers (HISPs) and health information exchanges (HIEs), to receive appropriate attribution and not be referenced by a certificate with "EHR" included in it. This final rule also supports health IT certification for other care and practice settings, such as long-term post-acute care (LTPAC), behavioral health, and pediatrics. Further, this final rule will make it simpler for certification criteria and certified health IT to be referenced by other HHS programs (e.g., Medicare and Medicaid payment programs and various grant programs), other public programs, and private entities and associations.

a. Program Alignment Changes

As part of our approach to evolve the ONC Health IT Certification Program, we have replaced prior rulemaking use of "EHR" and "EHR technology" with "health IT." The term health IT is reflective of the scope of ONC's authority under the Public Health Service Act (§ 3000(5) as "health information technology" is so defined), and represents a broad range of

[4] Please see section II.B.3 of this preamble for a regulatory history of the ONC Health IT Certification Program, including changes to the program's name.

technology, including EHR technology. It also more properly represents some of the technology, as noted above, that has been previously certified to editions of certification criteria under the ONC Health IT Certification Program and may be certified to the 2015 Edition. Similarly, to make the ONC Health IT Certification Program more open and accessible, we have renamed the EHR Module as "Health IT Module."

b. "Meaningful Use Measurement"

We have adopted our proposed approach in that we will not require ONC-Authorized Certification Bodies (ONC-ACBs) to certify Health IT Modules to the 2015 Edition "meaningful use measurement" certification criteria. We note, however, that CMS has included the 2015 Edition "meaningful use measurement" certification criteria in the CEHRT definition as a program requirement for the EHR Incentive Programs. Accordingly, we encourage health IT developers supporting providers participating in the EHR Incentive Programs or providers' quality improvement needs to seek certification to these criteria as appropriate for their Health IT Modules (e.g., a Health IT Module is presented for certification to a criterion that supports a Stage 3 objective with a percentage-based measure and the Health IT Module can meet the "automated numerator recording" criterion or "automated measure calculation" criterion).

c. Privacy and Security Certification Framework

We have adopted a new, simpler, straight-forward approach to privacy and security certification requirements for Health IT Modules certified to the 2015 Edition. In sum, the privacy and security certification criteria applicable to a Health IT Module presented for certification is based on the other capabilities included in the Health IT Module and for which certification is sought. Under the 2015 Edition privacy and security certification framework, a health IT developer will know exactly what it needs to do in order to get its Health IT Module

certified and a purchaser of a Health IT Module will know exactly what privacy and security functionality against which the Health IT Module had to be tested in order to be certified.

d. Principles of Proper Conduct (PoPC) for ONC-ACBs

We have adopted new and revised PoPC for ONC-ACBs. ONC-ACBs are now required to report an expanded set of information to ONC for inclusion in the open data file that would make up the Certified Health IT Product List (CHPL). ONC-ACBs must ensure that health IT developers provide more meaningful disclosure of certain types of costs and limitations that could interfere with the ability of users to implement certified health IT in a manner consistent with its certification. ONC-ACBs must retain records for a period of time that will support HHS program needs. ONC-ACBs must also obtain a record of all adaptations and updates affecting "safety-enhanced design" criteria on a quarterly basis each calendar year. ONC-ACBs must also report to the National Coordinator complaints received on certified health IT. We have also adopted new requirements for "in-the-field" surveillance under the ONC Health IT Certification Program that clarify and expand ONC-ACBs' existing surveillance responsibilities by specifying requirements and procedures for in-the-field surveillance. We believe these new and revised PoPC promote greater transparency and accountability for the ONC Health IT Certification Program.

C. Costs and Benefits

Our estimates indicate that this final rule is an economically significant rule as its overall costs for health IT developers may be greater than $100 million in at least one year. We have, therefore, projected the costs and benefits of the final rule. The estimated costs expected to be incurred by health IT developers to develop and prepare health IT to be tested and certified in accordance with the 2015 Edition certification criteria (and the standards and implementation

specifications they include) are represented in monetary terms in Table 1 below. We note that this final rule does not impose the costs cited as compliance costs, but rather as investments which health IT developers voluntarily take on and may expect to recover with an appropriate rate of return. We further note that, based on the estimates provided by a health IT developer association in response to the Proposed Rule, we have reduced the estimated burden of the 2015 Edition by over 40,000 burden hours per health IT developer by not adopting certain proposed certification criteria, functionality and standards.

The dollar amounts expressed in Table 1 are expressed in 2014 dollars.

Table 1. Distributed Total 2015 Edition Development and Preparation Costs for Health IT Developers (4-year period) – Totals Rounded

Year	Ratio	Total Low Cost Estimate ($M)	Total High Cost Estimate ($M)	Total Average Cost Estimate ($M)
2015	15%	39.07	60.48	49.77
2016	35%	91.15	141.12	116.14
2017	35%	91.15	141.12	116.14
2018	15%	39.07	60.48	49.77
4-Year Totals		260.44	403.19	331.82

As noted above, we expect that health IT developers will recover an appropriate rate of return for their investments in developing and preparing their health IT for certification to the 2015 Edition certification criteria adopted in this final rule. However, we do not have data available to quantify these benefits or other benefits that will likely arise from health IT developers certifying their health IT to the 2015 Edition.

We believe that there will be several significant benefits that may arise from this final rule for patients, health care providers, and health IT developers. The 2015 Edition continues to improve health IT interoperability through the adoption of new and updated standards and implementation specifications. For example, many proposed certification criteria include

standards and implementation specifications for interoperability that directly support the EHR Incentive Programs, which include objectives and measures for the interoperable exchange of health information and for providing patients electronic access to their health information in structured formats. In addition, the adopted certification criteria that support the collection of patient data that could be used to address health disparities would not only benefit patients, but the entire health care delivery system through improved quality of care. The 2015 Edition also supports usability and patient safety through new and enhanced certification requirements for health IT.

This final rule also makes the ONC Health IT Certification Program open and accessible to more types of health IT and for health IT that supports a variety of care and practice settings. This should benefit health IT developers, providers practicing in other care/practice settings, and consumers through the availability and use of certified health IT that includes capabilities that promote interoperability and enhanced functionality.

II. Background

A. Statutory Basis

The Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (the Recovery Act) (Pub. L. 111–5), was enacted on February 17, 2009. The HITECH Act amended the Public Health Service Act (PHSA) and created "Title XXX – Health Information Technology and Quality" (Title XXX) to improve health care quality, safety, and efficiency through the promotion of HIT and electronic health information exchange.

1. Standards, Implementation Specifications, and Certification Criteria

The HITECH Act established two new federal advisory committees, the Health IT Policy Committee (HITPC) and the Health IT Standards Committee (HITSC) (sections 3002 and 3003 of the PHSA, respectively). Each is responsible for advising the National Coordinator for Health Information Technology (National Coordinator) on different aspects of standards, implementation specifications, and certification criteria. The HITPC is responsible for, among other duties, recommending priorities for the development, harmonization, and recognition of standards, implementation specifications, and certification criteria. Main responsibilities of the HITSC include recommending standards, implementation specifications, and certification criteria for adoption by the Secretary under section 3004 of the PHSA, consistent with the ONC-coordinated Federal Health IT Strategic Plan.

Section 3004 of the PHSA identifies a process for the adoption of health IT standards, implementation specifications, and certification criteria and authorizes the Secretary to adopt such standards, implementation specifications, and certification criteria. As specified in section 3004(a)(1), the Secretary is required, in consultation with representatives of other relevant federal agencies, to jointly review standards, implementation specifications, and certification criteria endorsed by the National Coordinator under section 3001(c) and subsequently determine whether to propose the adoption of any grouping of such standards, implementation specifications, or certification criteria. The Secretary is required to publish all determinations in the **Federal Register**.

Section 3004(b)(3) of the PHSA titled, Subsequent Standards Activity, provides that the Secretary shall adopt additional standards, implementation specifications, and certification criteria as necessary and consistent with the schedule published by the HITSC. We consider this

provision in the broader context of the HITECH Act to grant the Secretary the authority and discretion to adopt standards, implementation specifications, and certification criteria that have been recommended by the HITSC and endorsed by the National Coordinator, as well as other appropriate and necessary health IT standards, implementation specifications, and certification criteria.

2. Health IT Certification Programs

Section 3001(c)(5) of the PHSA provides the National Coordinator with the authority to establish a certification program or programs for the voluntary certification of health IT. Specifically, section 3001(c)(5)(A) specifies that the National Coordinator, in consultation with the Director of the National Institute of Standards and Technology (NIST), shall keep or recognize a program or programs for the voluntary certification of health information technology as being in compliance with applicable certification criteria adopted under this subtitle (i.e., certification criteria adopted by the Secretary under section 3004 of the PHSA).

The certification program(s) must also include, as appropriate, testing of the technology in accordance with section 13201(b) of the [HITECH] Act. Overall, section 13201(b) of the HITECH Act requires that with respect to the development of standards and implementation specifications, the Director of the NIST, in coordination with the HITSC, shall support the establishment of a conformance testing infrastructure, including the development of technical test beds. The HITECH Act also indicates that the development of this conformance testing infrastructure may include a program to accredit independent, non-Federal laboratories to perform testing.

B. Regulatory History

1. Standards, Implementation Specifications, and Certification Criteria Rules

The Secretary issued an interim final rule with request for comments titled, "Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology" (75 FR 2014, Jan. 13, 2010) (the "S&CC January 2010 interim final rule"), which adopted an initial set of standards, implementation specifications, and certification criteria. After consideration of the comments received on the S&CC January 2010 interim final rule, a final rule was issued to complete the adoption of the initial set of standards, implementation specifications, and certification criteria and realign them with the final objectives and measures established for the EHR Incentive Programs Stage 1 (formally titled: Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology; Final Rule, (75 FR 44590, July 28, 2010) and referred to as the "2011 Edition final rule"). The 2011 Edition final rule also established the first version of the CEHRT definition. Subsequent to the 2011 Edition final rule (October 13, 2010), we issued an interim final rule with a request for comment to remove certain implementation specifications related to public health surveillance that had been previously adopted in the 2011 Edition final rule (75 FR 62686).

The standards, implementation specifications, and certification criteria adopted by the Secretary in the 2011 Edition final rule established the capabilities that CEHRT must include in order to, at a minimum, support the achievement of EHR Incentive Programs Stage 1 by eligible professionals (EPs), eligible hospitals, and critical access hospitals (CAHs) under the Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule (75 FR 44314) (the "EHR Incentive Programs Stage 1 final rule").

The Secretary issued a proposed rule with request for comments titled "Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology" (77 FR 13832, March 7, 2012) (the "2014 Edition proposed rule"), which proposed new and revised standards, implementation specifications, and certification criteria. After consideration of the comments received on the 2014 Edition proposed rule, a final rule was issued to adopt the 2014 Edition set of standards, implementation specifications, and certification criteria and realign them with the final objectives and measures established for the EHR Incentive Programs Stage 2, as well as Stage 1 revisions (Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology (77 FR 54163, Sept. 4, 2012) (the "2014 Edition final rule"). The standards, implementation specifications, and certification criteria adopted by the Secretary in the 2014 Edition final rule established the capabilities that CEHRT must include in order to, at a minimum, support the achievement of the EHR Incentive Programs Stage 2 by EPs, eligible hospitals, and CAHs under the Medicare and Medicaid Programs; Electronic Health Record Incentive Program—Stage 2 final rule (77 FR 53968) (the "EHR Incentive Programs Stage 2 final rule").

On December 7, 2012, an interim final rule with a request for comment was jointly issued and published by ONC and CMS to update certain standards that had been previously adopted in the 2014 Edition final rule. The interim final rule also revised the EHR Incentive Programs by adding an alternative measure for the Stage 2 objective for hospitals to provide structured electronic laboratory results to ambulatory providers, corrected the regulation text for the

measures associated with the objective for hospitals to provide patients the ability to view online, download, and transmit information about a hospital admission, and made the case number threshold exemption policy for clinical quality measure (CQM) reporting applicable for eligible hospitals and CAHs beginning with FY 2013. In addition, the interim final rule provided notice of CMS's intent to issue technical corrections to the electronic specifications for CQMs released on October 25, 2012 (77 FR 72985). On September 4, 2014, a final rule (Medicare and Medicaid Programs; Modifications to the Medicare and Medicaid Electronic Health Record (EHR) Incentive Program for 2014 and Other Changes to the EHR Incentive Program; and Health Information Technology: Revisions to the Certified EHR Technology Definition and EHR Certification Changes Related to Standards; Final Rule) (79 FR 52910) was published adopting these proposals.

On November 4, 2013, the Secretary published an interim final rule with a request for comment, 2014 Edition Electronic Health Record Certification Criteria: Revision to the Definition of "Common Meaningful Use (MU) Data Set" (78 FR 65884), to make a minor revision to the Common MU Data Set definition. This revision was intended to allow more flexibility with respect to the representation of dental procedures data for EHR technology testing and certification.

On February 26, 2014, the Secretary published a proposed rule titled "Voluntary 2015 Edition Electronic Health Record (EHR) Certification Criteria; Interoperability Updates and Regulatory Improvements" (79 FR 10880) ("Voluntary Edition proposed rule"). The proposed rule proposed a voluntary edition of certification criteria that was designed to enhance interoperability, promote innovation, and incorporate "bug fixes" to improve upon the 2014 Edition. A correction notice was published for the Voluntary Edition proposed rule on March 19,

2014, entitled "Voluntary 2015 Edition Electronic Health Record (EHR) Certification Criteria; Interoperability Updates and Regulatory Improvements; Correction" (79 FR 15282). This correction notice corrected the preamble text and gap certification table for four certification criteria that were omitted from the list of certification criteria eligible for gap certification for the 2015 Edition EHR certification criteria. On September 11, 2014, a final rule was published titled "2014 Edition Release 2 Electronic Health Record (EHR) Certification Criteria and the ONC HIT Certification Program; Regulatory Flexibilities, Improvements, and Enhanced Health Information Exchange" (79 FR 54430) ("2014 Edition Release 2 final rule"). The final rule adopted a small subset of the original proposals in the Voluntary Edition proposed rule as optional and revised 2014 Edition EHR certification criteria that provide flexibility, clarity, and enhance health information exchange. It also finalized administrative proposals (i.e., removal of regulatory text from the Code of Federal Regulations (CFR)) and proposals for the ONC HIT Certification Program that provide improvements.

On May 23, 2014, CMS and ONC jointly published the "Medicare and Medicaid Programs; Modifications to the Medicare and Medicaid Electronic Health Record Incentive Programs for 2014; and Health Information Technology: Revisions to the Certified EHR Technology Definition" proposed rule (79 FR 29732). The rule proposed to update the EHR Incentive Programs Stage 2 and Stage 3 participation timeline. It proposed to revise the CEHRT definition to permit the use of EHR technology certified to the 2011 Edition to meet the CEHRT definition for FY/CY 2014. It also proposed to allow EPs, eligible hospitals, and CAHs that could not fully implement EHR technology certified to the 2014 Edition for an EHR reporting period in 2014 due to delays in the availability of such technology to continue to use EHR technology certified to the 2011 Edition or a combination of EHR technology certified to the

2011 Edition and 2014 Edition for the EHR reporting periods in CY 2014 and FY 2014. On September 4, 2014, a final rule ("CEHRT Flexibility final rule") was published (79 FR 52910) adopting these proposals.

On March 30, 2015, the Secretary published a proposed rule titled "2015 Edition Health Information Technology (Health IT) Certification Criteria; 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications" (80 FR 16804) ("2015 Edition Proposed Rule" or "Proposed Rule"). The Proposed Rule proposed an edition of certification criteria that was designed to enhance interoperability and is the subject of this final rule.

2. Medicare and Medicaid EHR Incentive Programs Rules

On January 13, 2010, CMS published the Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Proposed Rule (75 FR 1844). The rule proposed the criteria for Stage 1 of the EHR Incentive Programs and regulations associated with the incentive payments made available under Division B, Title IV of the HITECH Act. Subsequently, CMS published a final rule (75 FR 44314) for Stage 1 of the EHR Incentive Programs on July 28, 2010, simultaneously with the publication of the 2011 Edition final rule. The EHR Incentive Programs Stage 1 final rule established the objectives, associated measures, and other requirements that EPs, eligible hospitals, and CAHs must satisfy to meet Stage 1.

On March 7, 2012, CMS published the Medicare and Medicaid Programs; Electronic Health Record Incentive Program—Stage 2; Proposed Rule (77 FR 13698). Subsequently, CMS published a final rule (77 FR 53968) for the EHR Incentive Programs on September 4, 2012, simultaneously with the publication of the 2014 Edition final rule. The EHR Incentive Programs Stage 2 final rule established the objectives, associated measures, and other requirements that

EPs, eligible hospitals, and CAHs must satisfy to meet Stage 2. It also revised some Stage 1 requirements.

As described above in Section II.B.1, ONC and CMS jointly issued an interim final rule with a request for comment that was published on December 7, 2012 and a final rule that was published on September 4, 2014. Also, as described above in Section II.B.1, ONC and CMS jointly issued proposed and final rules that were published on May 23, 2014 and September 4, 2014, respectively.

On March 30, 2015, CMS published the Medicare and Medicaid Programs; Electronic Health Record Incentive Program—Stage 3; Proposed Rule (80 FR 16732) ("EHR Incentive Programs Stage 3 proposed rule") outlining objectives, associated measures, and other requirements that EPs, eligible hospitals, and CAHs would need to meet to participate in Stage 3 of the EHR Incentives Programs.

On April 15, 2015, CMS published the Medicare and Medicaid Programs; Electronic Health Record Incentive Program—Modifications to Meaningful Use in 2015 Through 2017; Proposed Rule (80 FR 20346) ("EHR Incentive Programs Modifications proposed rule") proposing modifications to the EHR Incentive Programs for the EHR reporting periods and meaningful use measures in 2015 through 2017.

3. ONC Health IT Certification Program Rules

On March 10, 2010, ONC published a proposed rule (75 FR 11328) titled, "Proposed Establishment of Certification Programs for Health Information Technology" (the "Certification Programs proposed rule"). The rule proposed both a temporary and permanent certification program for the purposes of testing and certifying HIT. It also specified the processes the National Coordinator would follow to authorize organizations to perform the certification of

HIT. A final rule establishing the temporary certification program was published on June 24, 2010 (75 FR 36158) ("Temporary Certification Program final rule") and a final rule establishing the permanent certification program was published on January 7, 2011 (76 FR 1262) ("the Permanent Certification Program final rule").

On May 31, 2011, ONC published a proposed rule (76 FR 31272) titled "Permanent Certification Program for Health Information Technology; Revisions to ONC-Approved Accreditor Processes." The rule proposed a process for addressing instances where the ONC–Approved Accreditor (ONC–AA) engaged in improper conduct or did not perform its responsibilities under the permanent certification program, addressed the status of ONC–Authorized Certification Bodies in instances where there may be a change in the accreditation organization serving as the ONC–AA, and clarified the responsibilities of the new ONC–AA. All these proposals were finalized in a final rule published on November 25, 2011 (76 FR 72636).

The 2014 Edition final rule made changes to the permanent certification program. The final rule adopted a proposal to change the Permanent Certification Program's name to the "ONC HIT Certification Program," revised the process for permitting the use of newer versions of "minimum standard" code sets, modified the certification processes ONC-ACBs need to follow for certifying EHR Modules in a manner that provides clear implementation direction and compliance with the new certification criteria, and eliminated the certification requirement that every EHR Module be certified to the "privacy and security" certification criteria.

The Voluntary Edition proposed rule included proposals that focused on improving regulatory clarity, simplifying the certification of EHR Modules that are designed for purposes other than meeting requirements of the EHR Incentive Programs, and discontinuing the use of the Complete EHR definition. As noted above, we issued the 2014 Edition Release 2 final rule to

complete the rulemaking for the Voluntary Edition proposed rule. The 2014 Edition Release 2 final rule discontinued the "Complete EHR" certification concept beginning with the proposed 2015 Edition, adopted an updated standard (ISO/IEC 17065) for the accreditation of ONC-ACBs, and adopted the "ONC Certified HIT" certification and design mark for required use by ONC-ACBs under the ONC Health IT Certification Program.

As noted above, on March 30, 2015, the Secretary published the Proposed Rule which, in addition to proposing the 2015 Edition, proposed revisions to the ONC Health IT Certification Program.

III. Provisions of the Proposed Rule affecting Standards, Implementation Specifications, and Certification Criteria

A. 2015 Edition Health IT Certification Criteria

This rule finalizes new, revised, and unchanged certification criteria that establish the capabilities and related standards and implementation specifications for the certification of health IT, including EHR technology. We refer to these new, revised, and unchanged certification criteria as the "2015 Edition health IT certification criteria" and have added this term and its definition to § 170.102. As noted in the Executive Summary, we also refer to these criteria as the "2015 Edition" in this preamble. We codified the 2015 Edition in § 170.315 to set them apart from other editions of certification criteria and make it easier for stakeholders to quickly determine the certification criteria included in the 2015 Edition.

In the Proposed Rule, we identified the 2015 Edition certification criteria as new, revised, or unchanged in comparison to the 2014 Edition. In the 2014 Edition final rule we gave meaning to the terms "new," "revised," and "unchanged" to both describe the differences between the 2014 Edition certification criteria and the 2011 Edition certification criteria, as well as establish

what certification criteria in the 2014 Edition were eligible for gap certification (see 77 FR 54171, 54202, and 54248). Given that beginning with the 2015 Edition, "Complete EHR" certifications will no longer be issued (see also 79 FR 54443-45) and that we proposed to make the ONC Health IT Certification Program more open and accessible to other health care/practice settings, we also proposed to give new meaning to these terms for the purpose of a gap certification analysis as so specified:

- "New" certification criteria are those that as a whole only include capabilities never referenced in previously adopted certification criteria editions and to which a Health IT Module presented for certification to the 2015 Edition could have never previously been certified. As a counter example, the splitting of a 2014 Edition certification criterion into two criteria as part of the 2015 Edition would not make those certification criteria "new" for the purposes of a gap certification eligibility analysis.
- "Revised" certification criteria are those that include within them capabilities referenced in a previously adopted edition of certification criteria as well as changed or additional new capabilities; and to which a Health IT Module presented for certification to the 2015 Edition could not have been previously certified to all of the included capabilities.
- "Unchanged" certification criteria are those that include the same capabilities as compared to prior certification criteria of adopted editions; and to which a Health IT Module presented for certification to the 2015 Edition could have been previously certified to all of the included capabilities.

Comments. While we received no specific comments on these terms, we received comments both supporting and opposing the adoption of certification criteria that go beyond specifically supporting an objective and measure under the EHR Incentive Programs.

Response. We continue to maintain the same meanings for the terms "new," "revised," and "unchanged" as described in the Proposed Rule with a slight modification to the meaning of "unchanged" to state that "unchanged" certification criteria are certification criteria that include the same or less of the same capabilities as compared to prior certification criteria of adopted editions. We refer readers to section III.A.4 ("2015 Edition Gap Certification Eligibility Table") of this preamble for a complete description of gap certification and the identification of 2015 Edition certification criteria eligible for gap certification. In sum, "unchanged" criteria are eligible for gap certification. For health IT previously certified to the 2011 or 2014 Edition certification criteria, this permits, where applicable, the use of prior test results for certification to the 2015 certification criteria. This creates efficiencies and substantially reduces burden.

As described in the Proposed Rule and Executive Summary of this final rule as well as discussed in more detail in section IV.B of this preamble, we believe the availability and use of certified health IT for other use cases and health care settings beyond the EHR Incentive Programs has significant value. Therefore, we have adopted certification criteria that support those purposes. Table 2 below provides an overview of certification criteria adopted in this final rule as compared to the certification criteria proposed in the Proposed Rule and the adopted 2014 Edition.

Table 2. 2015 Edition Health IT Certification Criteria
Not Adopted Proposed Criteria (14)
Vital Signs
Image Results
Family Health History – Pedigree
Patient List Creation
Electronic Medication Administration Record
Decision Support – Knowledge Artifact
Decision Support – Service
Incorporate Laboratory Tests and Values/Results
Transmission of Laboratory Test Reports
Accessibility Technology
SOAP Transport and Security Specification and XDR/XDM for Direct Messaging

Healthcare Provider Directory – Query Request
Healthcare Provider Directory – Query Response
Electronic Submission of Medical Documentation
Unchanged Criteria as Compared to the 2014 Edition (Gap Certification Eligible) (16)
Computerized Provider Order Entry (CPOE) – Medications
CPOE – Laboratory
CPOE – Diagnostic Imaging
Drug-Drug, Drug-Allergy Interaction Checks for CPOE
Medication List
Medication Allergy List
Drug-Formulary and Preferred Drug List Checks
Smoking Status
Authentication, Access Control, Authorization
Audit Report(s)
Amendments
Automatic Access Time-Out
Emergency Access
End-User Device Encryption
Accounting of Disclosures
Transmission to Public Health Agencies – Reportable Laboratory Tests and Values/Results
Revised Criteria as Compared to the 2014 Edition (25)
Demographics
Problem List
Clinical Decision Support
Family Health History
Patient-Specific Education Resources
Transitions of Care
Clinical Information Reconciliation and Incorporation
Electronic Prescribing
Data Export
Clinical Quality Measures – Record and Export
Clinical Quality Measures – Import and Calculate
Clinical Quality Measures – Report
View, Download, and Transmit to 3rd Party
Transmission to Immunization Registries
Transmission to Public Health Agencies – Syndromic Surveillance
Transmission to Cancer Registries
Automated Numerator Recording
Automated Measure Calculation
Safety-enhanced Design
Quality Management System
Auditable Events and Tamper-Resistance*
Integrity*
Secure Messaging*
Direct Project*
Direct Project, Edge Protocol, and XDR/XDM*
New Criteria as Compared to the 2014 Edition (19)
Implantable Device List
Social, Psychological, and Behavioral Data

Data Segmentation for Privacy – Send	
Data Segmentation for Privacy – Receive	
Care Plan	
Common Clinical Data Set Summary Record – Create	New criteria based on request for comment in the Proposed Rule
Common Clinical Data Set Summary Record – Receive	
Clinical Quality Measures – Filter	
Trusted Connection	New for privacy and security certification framework and API approach
Auditing Actions on Health Information	New for privacy and security certification framework and API approach
Patient Health Information Capture	
Transmission to Public Health Agencies – Electronic Case Reporting	
Transmission to Public Health Agencies – Antimicrobial Use and Resistance Reporting	
Transmission to Public Health Agencies – Health Care Surveys	
Consolidated CDA Creation Performance	
Application Access – Patient Selection	Split the proposed API criterion into three criteria based on public comments
Application Access – Data Category Request	
Application Access – All Data Request	
Accessibility-centered Design	

[*] The criterion was proposed as unchanged, but has been adopted as revised in this final rule.

We proposed that readers should interpret the following terms used in the 2015 Edition with the same meanings we adopted in the 2014 Edition final rule (77 FR 54168-54169), in response to comment: "user," "record," "change," "access," "incorporate," "create," and "transmit," but apply to all health IT, not just "EHR technology." For the term "incorporate," we also proposed that readers should interpret the term as we further explained it under the "transitions of care" certification criterion (77 FR 54218) in the 2014 Edition final rule and in the Voluntary Edition proposed rule (79 FR 10898). We proposed that the scope of a 2015 Edition certification criterion was the same as the scope previously assigned to a 2014 Edition certification criterion (for further explanation, see the discussion at 77 FR 54168). That is, certification to the 2015 Edition certification criteria at § 170.315 would occur at the second paragraph level of the regulatory section and encompass all paragraph levels below the second paragraph level. We also proposed to continue to use the same specific descriptions for the different types of "data summaries" established in the 2014 Edition final rule (77 FR 54170-

54171) for the 2015 Edition certification criteria (i.e., "export summary," "transition of care/referral summary," "ambulatory summary," and "inpatient summary.")

We received no specific comments on these proposals and have adopted these meanings and approaches for certification to the 2015 Edition.

As with the adoption of the 2011 and 2014 editions of certification criteria (see the introductory text to §§ 170.302, 170.304, 170.306, and 170.314), all capabilities mentioned in certification criteria are expected to be performed electronically, unless otherwise noted. Therefore, we no longer include "electronically" in conjunction with each capability included in a certification criterion under § 170.315 because the introductory text to § 170.315 (which covers all the certification criteria included in the section) clearly states that health IT must be able to electronically perform the following capabilities in accordance with all applicable standards and implementation specifications adopted in the part.

Health IT certified to the 2015 Edition certification criteria and associated standards and implementation specifications can be implemented as part of an EP's, eligible hospital's, or CAH's CEHRT and used to demonstrate meaningful use (as identified in Table 4 of section III.A.3 below). We note that Table 4 also identifies certification criteria that are mandatory and conditional certification requirements for Health IT Modules, such as safety-enhanced design (conditional), and quality management system (mandatory), accessibility-centered design (mandatory), and privacy and security certification criteria (conditional). To note, we use the term mandatory to mean that all Health IT Modules must be certified to the certification criterion (see also § 170.550(g)(2) and (3)). Conditional means that certification to the certification criterion (e.g., the "Consolidated CDA creation performance," "safety-enhanced design," "automatic access timeout," or "integrity" certification criterion) depends on what other

certification criteria a Health IT Module is presented for certification to (see § 170.550(g)(1) and (4) and § 170.550(f)). For more information on "conditional" certification related to privacy and security, we also refer readers to section IV.C.1 ("Privacy and Security") of this preamble.

Health IT certified to the 2015 Edition certification criteria and associated standards and implementation specifications can also be used to meet other HHS program requirements (e.g., Medicare chronic care management services) or private sector requirements (e.g., The Joint Commission performance measurement initiative ("ORYX" vendor)). We refer readers to section IV.B.4 of this preamble for further programs that reference the use of certified health IT.

1. Applicability

Section 170.300 establishes the applicability of subpart C – Certification Criteria for Health Information Technology. We proposed to revise paragraph (d) of § 170.300 to add in a reference to § 170.315 and revise the parenthetical in the paragraph to say "i.e., apply to any health care setting" instead of "i.e., apply to both ambulatory and inpatient settings."

We received no comments on these specific proposed revisions and have adopted the proposed revisions. As noted in the Proposed Rule, these revisions clarify which specific capabilities <u>within</u> a certification criterion included in § 170.315 have general applicability (i.e., apply to any health care setting) or apply only to an inpatient setting or an ambulatory setting. The revision to change the language of the parenthetical aligns with our approach to make the ONC Health IT Certification Program more agnostic to health care settings and accessible to health IT that supports care and practice settings beyond the ambulatory and inpatient settings. We refer readers to section IV.B of this preamble for a detailed discussion of modifications to the ONC Health IT Certification Program responses to public comments received on the proposed modifications.

We note that, with the 2015 Edition, we no longer label an entire certification criterion as either optional or ambulatory/inpatient (at the second paragraph level of § 170.315). For example, the 2015 Edition certification criterion for transmission to cancer registries is simply "transmission to cancer registries" instead of "optional – ambulatory setting only – transmission to cancer registries." Similarly, the 2015 Edition certification criterion for "accounting of disclosures" is simply "accounting of disclosures" instead of "optional – accounting of disclosures." These simplifications are possible given that, beginning with the 2015 Edition certification criteria, "Complete EHR" certifications will no longer be issued (see 79 FR 54443-45). Therefore, there is no longer a need to designate an entire certification criterion in this manner. Again, this approach also supports our goal to make the ONC Health IT Certification Program more agnostic to health care settings and accessible to health IT that supports care and practice settings beyond the ambulatory and inpatient settings. We note that we still use "optional," "inpatient setting only," and "ambulatory setting only" designations within certification criteria to provide flexibility and reduce burden where feasible and appropriate.

We proposed to replace the term "EHR technology" in paragraphs (d)(1) and (d)(2) of § 170.300 with "health IT" to align with our approach to make the ONC Health IT Certification Program more clearly open to the certification of all types of health IT. We received no comments on this specific proposal and have replaced "EHR technology" with "health IT" in the referenced paragraphs. Again, we refer readers to section IV.B of this preamble for a detailed discussion of modifications to the ONC Health IT Certification Program and responses to public comments received on the proposed modifications.

2. Standards and Implementation Specifications

a. National Technology Transfer and Advancement Act

The National Technology Transfer and Advancement Act (NTTAA) of 1995 (15 U.S.C. 3701 et. seq.) and the Office of Management and Budget (OMB) Circular A–119[5] require the use of, wherever practical, technical standards that are developed or adopted by voluntary consensus standards bodies to carry out policy objectives or activities, with certain exceptions. The NTTAA and OMB Circular A-119 provide exceptions to selecting only standards developed or adopted by voluntary consensus standards bodies, namely when doing so would be inconsistent with applicable law or otherwise impractical. In this final rule, we refer to voluntary consensus standards, except for:

- The standards adopted in § 170.202. (These industry standards were developed by groups of industry stakeholders committed to advancing the Direct Project[6], which included initiatives under the Standards and Interoperability (S&I) Framework[7]. These groups used consensus processes similar to those used by voluntary consensus standards bodies.);
- The standards adopted at § 170.205(d)(4) and (e)(4) for reporting of syndromic surveillance and immunization information to public health agencies, respectively (These standards go through a process similar within the public health community to those used by other industry stakeholders and voluntary consensus standards bodies.);
- The standard adopted at § 170.207(f)(2) for race and ethnicity; and
- Certain standards related to the protection of electronic health information adopted in § 170.210.

[5] http://www.whitehouse.gov/omb/circulars_a119
[6] http://www.healthit.gov/policy-researchers-implementers/direct-project
[7] http://www.healthit.gov/policy-researchers-implementers/standards-interoperability-si-framework

We are aware of no voluntary consensus standard that would serve as an alternative to these standards for the purposes that we have identified in this final rule.

b. Compliance with Adopted Standards and Implementation Specifications

In accordance with Office of the **Federal Register** regulations related to "incorporation by reference," 1 CFR part 51, which we follow when we adopt proposed standards and/or implementation specifications in a final rule, the entire standard or implementation specification document is deemed published in the **Federal Register** when incorporated by reference therein with the approval of the Director of the Federal Register. Once published, compliance with the standard and implementation specification includes the entire document unless we specify otherwise. For example, for the Health Level Seven (HL7) Implementation Guide (IG) for CDA Release 2: National Health Care Surveys (NHCS), Release 1 adopted in this final rule, health IT certified to the certification criterion referencing this IG will need to demonstrate compliance with all mandatory elements and requirements of the IG. If an element of the IG is optional or permissive in any way, it will remain that way for testing and certification unless we specified otherwise in regulation. In such cases, the regulatory text preempts the permissiveness of the IG.

c. "Reasonably Available" to Interested Parties

The Office of the **Federal Register** has established new requirements for materials (e.g., standards and implementation specifications) that agencies incorporate by reference in the **Federal Register** (79 FR 66267; 1 CFR 51.5(b)). To comply with these requirements, in section V ("Incorporation by Reference") of this preamble, we provide summaries of, and uniform resource locators (URLs) to, the standards and implementation specifications we have adopted and incorporated by reference in the **Federal Register**. To note, we also provide relevant

information about these standards and implementation specifications throughout this section of the preamble (section III), including URLs.

d. "Minimum Standards" Code Sets

In the Proposed Rule, we proposed to adopt newer versions of four previously adopted minimum standards code sets for the 2015 Edition. The code sets proposed were: the September 2014 Release of the U.S. Edition of SNOMED CT®, LOINC® version 2.50, the February 2, 2015 monthly version of RxNorm, and the February 2, 2015 version of the CVX code set. We also proposed to adopt two new minimum standards code sets (the National Drug Codes (NDC) – Vaccine Codes, updates through January 15, 2015 and the "Race & Ethnicity – CDC" code system in the PHIN Vocabulary Access and Distribution System (VADS) Release 3.3.9 (June 17, 2011)). We reiterated, as we have previously articulated (77 FR 54170), the adoption of newer versions improve interoperability and health IT implementation, while creating little additional burden through the inclusion of new codes. We further stated that, as many of these minimum standards code sets are updated frequently throughout the year, we would consider whether it may be more appropriate to adopt a version of a minimum standards code set that is issued before we publish a final rule for the Proposed Rule.

Comments. A number of commenters were supportive of the proposal to adopt more recent versions of the U.S. Edition of SNOMED CT®, LOINC®, RxNorm, and the CVX code set. Commenters supported adoption of NDC codes for vaccines, but also recommended we adopt the MVX codes for vaccine manufacturer as part of this list. One commenter requested identification of the steward for the PHIN VADS "Race & Ethnicity – CDC" code system, noting that it did not appear to have been updated since 2007. This commenter also requested verification that the code set has been reviewed on a regular basis.

A few commenters suggested that we do not specify an exact version and release of a standard (e.g., allow for adoption of version/release 1.x of the HL7 Implementation Guide for CDA Release 2: National Health Care Surveys (NHCS) where "x" could be any version/release within the version/release 1 family). Another commenter suggested that we consider adopting a "rolling" upgrade cycle for all standardized code systems and value sets. Specifically, the commenter recommended that a certified Health IT Module should not be more than two versions behind the most currently released version of the code system or value set. Commenters also suggested that the vocabulary code set versions in the Proposed Rule are now outdated and have since been updated per a regular update cycle. Commenters suggested we adopt these more recent versions of these vocabulary code sets as they provide the most up-to-date clinical information for clinical relevance and interoperability.

Response. As many of the proposed minimum standards code sets are updated frequently throughout the year, we considered whether it was more appropriate to adopt versions of minimum standards code sets that were issued after the Proposed Rule and before we published this final rule. In making such determination, as we have done with prior finalized versions of minimum standards code sets, we gave consideration to whether these newer versions included any new substantive requirements and their effects on interoperability. We have found no negative effects on interoperability with the newer versions we have adopted as compared to the proposed versions. Rather, these newer versions will further support and improve the structured recording of data. To note, the adopted newer version of a minimum standards code set will serve as the baseline for certification. As with all adopted minimum standards code sets, health IT can be certified to newer versions of the adopted baseline version minimum standards code

sets for purposes of certification, unless the Secretary specifically prohibits the use of a newer version (see § 170.555 and 77 FR 54268).

We have adopted newer versions of four 2014 Edition minimum standards code sets in this final rule for the 2015 Edition. These code sets are the September 2015 Release of the U.S. Edition of SNOMED CT®, LOINC® version 2.52, the September 8, 2015 monthly version of RxNorm, and the August 17, 2015 version of the CVX code set. We have also adopted three new minimum standards code sets. These code sets are the National Drug Codes (NDC) – Vaccine NDC Linker, updates through August 17, 2015; the CDC Race and Ethnicity Code Set Version 1.0 (March 2000)[8]; and the Crosswalk: Medicare Provider/Supplier to Healthcare Provider Taxonomy, April 2, 2015.

We have not adopted MVX codes for vaccine manufacturers as detailed further in the discussion on the "transmission to immunization registries" certification criterion in section III.A.3 of the preamble. Therefore, we do not see a need to include MVX codes in this list of code sets.

We confirm that CDC continues to steward the CDC Race and Ethnicity Code Set, Version 1.0 (March 2000). We also confirm that we have reviewed this version and believe it is appropriate to adopt it as the minimum standard code set for race and ethnicity. Any updates to the code set, including the issuance of newer versions, are within the oversight of the CDC.

As we stated in the 2014 Edition final rule (77 FR 54169-54170), the Office of the Federal Register regulations related to "incorporation by reference" are limited to a specific version that is approved rather than future versions or revisions of a given publication. Thus, we

[8] We have more specifically identified the CDC Race and Ethnicity code set as compared to the identification in the Proposed Rule. We note this code set remains part of the PHIN Vocabulary Access and Distribution System (VADS) Release 3.3.9. http://www.cdc.gov/phin/resources/vocabulary/index.html

do not include regulation language that refers to a version/release as, for example "Version/Release 1.X" when "X" remains variable. Further, to remain in compliance with the Administrative Procedure Act and address any potential interoperability concerns, we would need to issue regulations to adopt a newer version minimum standards code set as a "baseline" standard and cannot require health IT developers to upgrade on a rolling basis.

e. Object Identifiers (OIDs) for Certain Code Systems

We are providing the following table (Table 3) of OIDs for certain code systems to assist health IT developers in the proper identification and exchange of health information coded to the vocabulary standards referenced in this final rule.

Table 3. Code System Object Identifiers (OIDs)	
Code system OID	**Code System Name**
2.16.840.1.113883.6.96	IHTSDO SNOMED CT®
2.16.840.1.113883.6.1	LOINC®
2.16.840.1.113883.6.88	RxNorm
2.16.840.1.113883.12.292	HL7 Standard Code Set CVX-Vaccines Administered
2.16.840.1.113883.6.69	National Drug Code Directory
2.16.840.1.113883.6.8	Unified Code of Units of Measure (UCUM[9])
2.16.840.1.113883.6.13	Code on Dental Procedures and Nomenclature (CDT)
2.16.840.1.113883.6.4	International Classification of Diseases, 10th Revision, Procedure Coding System (ICD-10-PCS)
2.16.840.1.113883.6.238	CDC Race and Ethnicity Code Set Version 1.0 (March 2000)
2.16.840.1.113883.6.316	Tags for Identifying Languages – Request for Comment (RFC) 5646 (preferred language)
2.16.840.1.113883.6.101	Healthcare Provider Taxonomy

f. Subpart B – Standards and Implementation Specifications for Health Information Technology

We proposed to remove the term "EHR Modules" from § 170.200 and add in its place "Health IT Modules" We proposed to remove the term "EHR technology" from § 170.210 and add in its place "health IT." We noted that these proposals were consistent with our overall

[9] Copyright © 1998-2013, Regenstrief Institute, Inc. and the UCUM Organization. All rights reserved.

approach to this rulemaking as discussed in the Proposed Rule Executive Summary and recited in this final rule's Executive Summary. We received no comments on these specific proposals and have adopted these proposals. We refer readers to section IV.B of this preamble for a detailed discussion of modifications to the ONC Health IT Certification Program and responses to public comments received on the proposed modifications.

3. Adopted Certification Criteria

We discuss the certification criteria that we have adopted as part of the 2015 Edition in this section. We discuss each certification criterion in the chronological order in which it would appear in the CFR. In other words, the preamble that follows discusses the adopted certification criteria in § 170.315(a) first, then § 170.315(b), and so on through section (h). Due to certain proposed certification criteria not being adopted as well as further consideration of proper categorization of criteria, the designation of some criteria within § 170.315 has changed in comparison to the Proposed Rule (e.g., the 2015 Edition "smoking status" criterion has been codified in § 170.315(a)(11) instead of proposed (a)(12) and the 2015 Edition "patient health information capture" criterion has been codified in § 170.315(e)(3) instead of proposed (a)(19)).

We note that we have restructured the regulatory text of certification criteria to remove the use of "or" in many places where it was proposed to indicate certification optionality. We have replaced it with language that we believe will better convey that same optionality. This restructuring of the regulatory text will provide further clarity regarding when a health IT developer has flexibility to select one of two or more options for certifying its Health IT Module as compared to when it is expected that the Health IT Module demonstrate all listed methods for certification. This restructuring, by itself, did not alter any of the proposed certification criteria requirements.

Table 4 below identifies the 2015 Edition certification criteria associated with the EHR Incentive Programs Stage 3 as finalized in EHR Incentive Programs Stage 3 and Modifications final rule published elsewhere in this issue of the **Federal Register**. While these certification criteria can be used to support other use cases and health care settings beyond the EHR Incentive Programs, we have also adopted additional 2015 health IT certification criteria that support other specific use cases and health care settings. These criteria were listed in Table 2 and are discussed in this section of the preamble.

Table 4. 2015 Edition Health IT Certification Criteria Associated with the EHR Incentive Programs Stage 3

CFR Section 170.315	**Certification Criterion**	**Relationship to the CEHRT[10] Definition and Stage 3 Objectives[11]**	**Health IT Module Certification Requirements**
(a)(1)	Computerized Provider Order Entry (CPOE) – Medications[12]	Specifically included in the CEHRT definition Associated with Objective 4	
(a)(2)	CPOE – Laboratory[13]	Specifically included in the CEHRT definition Associated with Objective 4	
(a)(3)	CPOE – Diagnostic Imaging[14]	Specifically included in the CEHRT definition Associated with Objective 4	
(a)(4)	Drug-Drug, Drug-Allergy Interaction Checks for CPOE	Associated with Objective 3	
(a)(5)	Demographics	Specifically included in the CEHRT definition	
(a)(6)	Problem List	Specifically included in the CEHRT definition	

[10] The EHR Incentive Programs CEHRT definition includes the criteria adopted in the 2015 Edition Base EHR definition. These criteria are identified in this table as specifically included in CEHRT definition, as are other criteria specifically included in the CEHRT definition but are not part of the 2015 Edition Base EHR definition. For more information on the 2015 Edition Base EHR definition, please see section III.B.1of this final rule's preamble. For more details on the CEHRT definition, please see the EHR Incentive Programs Stage 3 and Modifications final rule published elsewhere in this issue of the **Federal Register**.

[11] Criteria "associated with objectives" support requirements of the EHR Incentive Programs to use certified EHR technology to meet objectives. For further information on these requirements, please see the EHR Incentive Programs Stage 3 and Modifications final rule published elsewhere in this issue of the **Federal Register**.

[12] Technology needs to be certified to § 170.315(a)(1), (a)(2), or (a)(3).

[13] Technology needs to be certified to § 170.315(a)(1), (a)(2), or (a)(3).

[14] Technology needs to be certified to § 170.315(a)(1), (a)(2), or (a)(3).

(a)(7)	Medication List	Specifically included in the CEHRT definition	
(a)(8)	Medication Allergy List	Specifically included in the CEHRT definition	
(a)(9)	Clinical Decision Support	Specifically included in the CEHRT definition Associated with Objective 3	
(a)(10)	Drug-Formulary and Preferred Drug List Checks	Associated with Objective 2	
(a)(11)	Smoking Status	Specifically included in the CEHRT definition	
(a)(12)	Family Health History	Specifically included in the CEHRT definition	
(a)(13)	Patient-Specific Education Resources	Associated with Objective 5	
(a)(14)	Implantable Device List	Specifically included in the CEHRT definition	
(b)(1)	Transitions of Care	Specifically included in the CEHRT definition Associated with Objective 7	
(b)(2)	Clinical Information Reconciliation and Incorporation	Associated with Objective 7	
(b)(3)	Electronic Prescribing	Associated with Objective 2	
(b)(6)	Data Export	Specifically included in the CEHRT definition	
(c)(1)	Clinical Quality Measures – Record and Export	Specifically included in the CEHRT Definition	
(c)(2)	Clinical Quality Measures – Import and Calculate	Specifically included in the CEHRT Definition	
(c)(3)	Clinical Quality Measures – Report	Specifically included in the CEHRT Definition	
(e)(1)	View, Download, and Transmit to 3rd Party	Associated with Objective 5 Associated with Objective 6	
(e)(2)	Secure Messaging	Associated with Objective 6	
(e)(3)	Patient Health Information Capture	Specifically included in the CEHRT definition Associated with Objective 6	
(f)(1)	Transmission to Immunization Registries	Associated with Objective 8[15]	
(f)(2)	Transmission to Public Health Agencies – Syndromic Surveillance	Associated with Objective 8	
(f)(3)	Transmission to Public Health Agencies – Reportable Laboratory Tests and Values/Results	Associated with Objective 8	
(f)(4)	Transmission to Cancer Registries	Associated with Objective 8	

[15] For the public health certification criteria in § 170.315(f), health IT will only need to be certified to those criteria that are required to meet the measures the provider intends to report on to meet Objective 8: Public Health and Clinical Data Registry Reporting.

(f)(5)	Transmission to Public Health Agencies – Electronic Case Reporting	Associated with Objective 8	
(f)(6)	Transmission to Public Health Agencies – Antimicrobial Use and Resistance Reporting	Associated with Objective 8	
(f)(7)	Transmission to Public Health Agencies – Health Care Surveys	Associated with Objective 8	
(g)(1)	Automated Numerator Recording	Specifically included in the CEHRT definition	
(g)(2)	Automated Measure Calculation	Specifically included in the CEHRT definition	
(g)(7)	Application Access – Patient Selection	Specifically included in the CEHRT definition Associated with Objective 5 Associated with Objective 6	
(g)(8)	Application Access – Data Category Request	Specifically included in the CEHRT definition Associated with Objective 5 Associated with Objective 6	
(g)(9)	Application Access – All Data Request	Specifically included in the CEHRT definition Associated with Objective 5 Associated with Objective 6	
(h)(1)	Direct Project[16]	Specifically included in the CEHRT definition	
(h)(2)	Direct Project, Edge Protocol, and XDR/XDM[17]	Specifically included in the CEHRT definition	
(g)(4)	Quality Management System		Mandatory
(g)(5)	Accessibility-Centered Design		Mandatory
(d)(1)	Authentication, Access Control, Authorization		Conditional
(d)(2)	Auditable Events and Tamper-Resistance		Conditional
(d)(3)	Audit Report(s)		Conditional
(d)(4)	Amendments		Conditional
(d)(5)	Automatic Access Time-Out		Conditional
(d)(6)	Emergency Access		Conditional
(d)(7)	End-User Device Encryption		Conditional
(d)(8)	Integrity		Conditional
(d)(9)	Trusted Connection		Conditional
(d)(10)	Auditing Actions on Health Information		Conditional
(g)(3)	Safety-Enhanced Design		Conditional
(g)(6)	Consolidated CDA Creation		Conditional

[16] Technology needs to be certified to § 170.315(h)(1) or (h)(2) to meet the 2015 Edition Base EHR definition and CEHRT definition.
[17] Technology needs to be certified to § 170.315(h)(1) or (h)(2) to meet the 2015 Edition Base EHR definition and CEHRT definition.

	Performance		
Key Mandatory: All Health IT Modules must be certified to the certification criterion. Conditional: A Health IT Module is certified to the certification criterion depending on the other certification criteria the Health IT Module is presented for certification to.			

- Computerized Provider Order Entry

We proposed to adopt three separate 2015 computerized provider order entry (CPOE) certification criteria based on the clinical purpose (i.e., medications, laboratory, and diagnostic imaging), which was consistent with the 2014 Edition CPOE certification criteria we adopted in the 2014 Edition Release 2 final rule (79 FR 54435-36).

Comments. We received only a few comments on this proposed approach, all which expressed support for separating the functionality based on clinical purpose.

Response. We have adopted separate CPOE certification criteria based on clinical purposes that are described in more detail below.

We requested comment on whether we should specify, for the purposes of testing and certification to the 2015 Edition CPOE criteria, certain data elements that a Health IT Module must be able to include in a transmitted order. In particular, we requested comment on whether a Health IT Module should be able to include any or all of the following data elements: secondary diagnosis codes; reason for order; and comment fields entered by the ordering provider, if they are provided to the ordering provider in their order entry screen. We also requested comment on whether there are any other data elements that a Health IT Module should be able to include as part of an order for the purposes of testing and certification.

Comments. Most commenters opposed the inclusion of specific data elements for certification. These commenters most often cited burden on health IT developers and concern that new data elements might lead to inefficient workflow for the order entry process as reasons for not including additional data elements. Some commenters expressed support for the inclusion

of additional data elements mentioned in the Proposed Rule, but varied in their support for the specific data elements that should we included. These commenters did, however, agree that the "reason for order" data element was a data element that should be included with an order.

Response. We acknowledge the lack of agreement as to what data elements should be required for certification, but also the support for the "reason for order" data elements. With consideration of commenters concerns about burden and workflow inefficiencies, we have adopted the "reason for order" data element as an optional certification provision in each of the three CPOE certification criteria. We agree with commenters that the reason for an order data element has value. The designation of this provision as optional in all three criteria gives flexibility to health IT developers as they consider certification of their health IT and providers as they consider what certified health IT to purchase.

- Computerized Provider Order Entry - Medications

2015 Edition Health IT Certification Criterion § 170.315(a)(1) (Computerized provider order entry - medications)

We proposed to adopt a 2015 Edition CPOE certification criterion specific to medication ordering that was unchanged in comparison to the 2014 Edition CPOE – medications criterion adopted at § 170.314(a)(18) as well as § 170.314(a)(1)(i). The proposed criterion does not reference any standards or implementation specifications.

Comments. Commenters overwhelmingly recommended that this criterion remain unchanged. A few commenters requested clarifications regarding the designation of authorized CPOE users and the proper counting of CPOE orders for the purposes of meeting the associated meaningful use objective and measure.

Response. We thank commenters for their support and have adopted this criterion as unchanged. As noted above, we have, however, adopted the "reason for order" data element as

an optional provision within this criterion. For questions related to the EHR Incentive Programs (i.e., the designation of authorized CPOE users and the proper counting of CPOE order for the purposes of meeting the associated meaningful use objective and measure), we refer readers to CMS and the EHR Incentive Programs Stage 3 and Modifications final rule published elsewhere in this issue of the **Federal Register**.

- Computerized Provider Order Entry - Laboratory

2015 Edition Health IT Certification Criterion § 170.315(a)(2) (Computerized provider order entry - laboratory)

We proposed to adopt a 2015 Edition CPOE certification criterion specific to laboratory ordering that was revised in comparison to the CPOE – laboratory criterion adopted at § 170.314(a)(19) as well as § 170.314(a)(1)(ii). For the ambulatory setting, we proposed that this criterion would include the HL7 Version 2.5.1 Implementation Guide: S&I Framework Laboratory Orders (LOI) from EHR, Draft Standard for Trial Use, Release 2 – US Realm ("Release 2"). We proposed to adopt the most recent version of the HL7 Version 2.5.1 Implementation Guide: S&I Framework Laboratory Test Compendium Framework, Release 2, (also referred to as the "electronic Directory of Services (eDOS) IG") for certification to all health care settings. We also proposed to require that a Health IT Module use, at a minimum, version 2.50 of Logical Observation Identifiers Names and Codes (LOINC®) as the vocabulary standard for laboratory orders.

Comments. Commenters stated that the LOIs and eDOS IGs were not ready for implementations, but acknowledged the significant progress being made in developing standards for laboratory ordering and the harmonizing of laboratory- related IGs.

Response. With consideration of comments, we have determined not to adopt any standards for this certification criterion. We have, however, adopted the "reason for order" data

element as an optional provision within this criterion. We have made the determination to keep this criterion "functional" at this time based on a number of factors, including (among other aspects) that the best versions of the IGs that could be associated with this criterion were not sufficiently ready. That being said, we believe that the LOI and eDOS IGs show great promise in improving laboratory interoperability and could potentially result in significant cost savings to the industry at large. Accordingly, we remain committed to continued collaboration with stakeholders to support the widespread adoption of these IGs, including the development of testing tools and pilots where necessary and feasible.

- Computerized Provider Order Entry – Diagnostic Imaging

2015 Edition Health IT Certification Criterion § 170.315(a)(3) (Computerized provider order entry – diagnostic imaging)

We proposed to adopt a 2015 Edition CPOE certification criterion specific to diagnostic imaging ordering that was unchanged in comparison to the 2014 Edition CPOE – diagnostic imaging criterion adopted at § 170.314(a)(20) as well as § 170.314(a)(1)(iii). The proposed criterion does not reference any standards or implementation specifications. We also proposed to adopt the title of "diagnostic imaging," which is the title we gave to the 2014 Edition version of this certification criterion in the 2014 Edition Release 2 final rule (79 FR 54436).

Comments. Commenters overwhelmingly recommended that this criterion remain unchanged. A few commenters recommended we add functionality to this criterion, including the required use of a standard such as Digital Imaging and Communications in Medicine (DICOM) to support radiology.

Response. We thank commenters for their support and have adopted this criterion as unchanged. As noted above, we have, however, adopted the "reason for order" data element as an optional provision within this criterion. While we appreciate comments suggesting the

inclusion of additional functionality, the recommended functionality is outside the scope of the proposed criterion. Therefore, we have not adopted the recommended functionality in this criterion. We also refer readers to our previous discussion of DICOM (77 FR 54173).

- Drug-Drug, Drug-Allergy Interaction Checks for CPOE

2015 Edition Health IT Certification Criterion § 170.315(a)(4) (Drug-drug, drug-allergy interaction checks for CPOE)

We proposed to adopt a revised 2014 Edition "drug-drug, drug-allergy interaction checks" criterion (§ 170.314(a)(2)) to clarify that the capabilities included in this criterion are focused on CPOE. We proposed that a Health IT Module must record at least one action taken and by whom, and must generate either a human readable display or human readable report of actions taken and by whom in response to drug-drug or drug-allergy interaction checks (DD/DAI). We explained that the benefits of recording user actions for DD/DAI interventions that assist with quality improvement and patient safety outweigh the development burden associated with this functionality. However, to address development concerns, we proposed that a Health IT Module must only record, at a minimum, one user action for DD/DAI checks; and asked for comment on focusing the requirement to record at least one user action taken for DD/DAI interventions on a subset of DD/DAI interventions and what sources we should consider for defining this subset. We further noted that the proposed criterion does not establish the uses for the "user action" information, who should be able to view the information, or who could adjust the capability. We also sought comment on requiring functionality that would inform a user of new or updated DD/DAI when the medication or medication allergy lists are updated.

Comments. We received a few comments supporting our proposed clarification that this criterion focused on CPOE, but also suggestions that this functionality could support other use cases, such as when medications are reviewed or medication or medication allergy lists are

updated. We received mixed comments in response to the proposed additional "recording user response" functionality for this criterion. While many commenters supported the overall goal of interaction checking for quality improvement and patient safety, including functionality that would inform a user of new or updated DD/DAI, many commenters stated that current systems already provide a wide range of functionality to enable providers to document decisions concerning interaction warnings. These commenters stated that the proposed "recording user response" is not necessary for certification or for providers to satisfy objectives of the EHR Incentive Programs. Commenters requested the criterion remain eligible for gap certification. A few expressed overall agreement with the other functionality specified in this criterion, including the ability to adjust the severity level of interventions (e.g., alerts) for drug-drug interaction checks.

Response. We have determined, based on public comments, to focus this certification criterion on CPOE and to not adopt the "recording user response" functionality. This approach is responsive to comments and will permit health IT developers to focus their efforts on functionality and requirements that support the goals outlined in the Executive Summary, including supporting the interoperability of health IT. To note, this criterion is eligible for gap certification.

- Demographics

2015 Edition Health IT Certification Criterion § 170.315(a)(5) (Demographics)

We proposed to adopt a revised 2015 Edition "demographics" certification criterion in comparison to the 2014 Edition certification criterion (§ 170.314(a)(3)). We received comments that focused on each of the specific data elements in the certification criterion. We have categorized and responded to these comments in a similar manner.

Sex

We proposed the requirement to record sex in accordance with HL7 Version 3 ("AdministrativeGender") and a nullFlavor value attributed as follows: male (M); female (F); and unknown (UNK), and noted that HL7 Version 3 for recording sex would be required under the "Common Clinical Data Set" definition for certification to the 2015 Edition. In the Proposed Rule's section III.B.3 ("Common Clinical Data Set"), we stated that this approach would become the method for capturing sex under the "Common Clinical Data Set" definition for certification to the 2015 Edition.

Comments. Commenters were generally supportive of recording sex in a structured manner. A few commenters suggested that we used other values, such as U or UN for undifferentiated. A few commenters also requested clarification on the proposed use of two different value sets (HL7 AdministrativeGender and NullFlavor).

Response. We appreciate the support for our proposal. We have adopted the requirement for recording sex as proposed. We clarify that this coding is intended to present birth sex. Therefore, we believe the use of the specified values and value sets is the most appropriate approach. It is also an approach that we believe poses the least burden and most health IT developers are using these values and value sets.

Race and Ethnicity

We proposed the requirement to record each one of a patient's races and ethnicities in accordance with, at a minimum, the "Race & Ethnicity – CDC" code system in the PHIN Vocabulary Access and Distribution System (VADS), Release 3.3.9[18] and aggregate each one of a patient's races and ethnicities to the categories in the OMB standard for race and ethnicity. We

[18] https://phinvads.cdc.gov/vads/ViewCodeSystem.action?id=2.16.840.1.113883.6.238#

explained that a Health IT Module must be able to record each one of a patient's races and ethnicities using any of the 900 plus concepts in the "Race & Ethnicity – CDC" code system, and noted that health IT developers and health care providers could determine the appropriate user interface implementation in a given setting. The Proposed Rule section III.A.2.d ("Minimum Standards" Code Sets) discussed the adoption of the "Race & Ethnicity – CDC" code system in PHIN VADS as a minimum standards code set and Release 3.3.9, or potentially a newer version if released before this final rule, as the baseline for certification to the 2015 Edition. To note, the Proposed Rule section III.B.3 "Common Clinical Data Set" also discussed adopting the Race & Ethnicity – CDC" code system in PHIN VADS (at a minimum, Release 3.3.9) and the OMB standard as the race and ethnicity standards under the "Common Clinical Data Set" definition for certification to the 2015 Edition.

Comments. A majority of commenters supported our proposal to require a Health IT Module to be able to capture granular patient race and ethnicity data. Some commenters questioned the necessity for such granular race and ethnicity capture because it was not required for the EHR Incentive Programs or another identified purpose, with one commenter recommending that this be a future certification requirement. Commenters expressed concerns about user interfaces in relation to the over 900 concepts for race and ethnicity in PHIN VADS, including concern over how many concepts should be displayed for users. Similarly, commenters suggested that testing and certification should not be to all 900 concepts. A few commenters requested clarification on whether a health IT Module must be able to capture multiple races or ethnicities for a patient and the appropriate method for capturing when a patient declines to provide race or ethnicity information.

Response. We thank commenters for their support. We have adopted the race and ethnicity requirements as proposed, including the use of both the OMB and the CDC Race and Ethnicity standards. We believe that the structured granular recording of race and ethnicity can both improve patient care and support the elimination of health disparities whether or not currently required by the EHR Incentives Programs or another HHS program. By adopting these requirements, we ensure certified health IT has these capabilities and can make them available to providers. We clarify four points in response to comments. First, as mentioned in the Proposed Rule, a health IT developer and provider can best determine how the user interface is designed, including how many race and ethnicity values are displayed. Second, as mentioned above and in the Proposed Rule, a Health IT Module must be able to record each one of a patient's races and ethnicities using any of the 900 plus concepts. For testing and certification, a Health IT Module would be tested to any of the 900 plus concepts at the discretion of the testing body. Third, a Health IT Module would need to be capable of recording multiple races and/or ethnicities for a patient. This approach is consistent with the OMB standard. Fourth, a Health IT Module must be able to demonstrate that it can record whether a patient declined to provide information for all data specified in this certification criterion. We do not, however, specify for the purposes of certification how that data is specifically captured.

Preferred Language

In the Proposed Rule, we proposed to require the use of the Internet Engineering Task Force (IETF) Request for Comments (RFC) 5646[19] standard for preferred language. We stated that RFC 5646 entitled "Tags for Identifying Languages, September 2009" is the coding system that is commonly used to encode languages on the web. We also noted that this standard is

[19] http://www.rfc-editor.org/info/rfc5646

compatible with the C-CDA Release 2.0 (and C-CDA Release 2.1) and that other preferred language standards in use today can be efficiently mapped to it, such as ISO 639-1, 639-2, and 639-3. The Proposed Rule explained that the standard does not determine the way in which health care providers use the capability to record preferred language or the preferred language values they are presented with to select a patient's preferred language. In the Proposed Rule's section III.B.3 ("Common Clinical Data Set"), we stated that RFC 5646 would also become the preferred language standard under the "Common Clinical Data Set" definition for certification to the 2015 Edition.

Comments. Commenters were generally supportive of the adoption of the RFC 5646 standard. Some commenters (health IT developers) expressed opposition to the recording of preferred language in RFC 5646 due to the new burden it would create versus the perceived minimal value. One commenter suggested adopting ISO 639-3 instead of RFC 5646.

Response. We have adopted RFC 5646 as the preferred language standard for this criterion. As extensively discussed in the Proposed Rule (80 FR 16817), we believe this is the most appropriate standard for capturing a patient's preferred language. It is compatible with the C-CDA Release 2.1 and other preferred language standards can be efficiently mapped to it, including IS0 639-1, 639-2, and 639-3. As mentioned in the Proposed Rule and clarified for other demographics data, a health IT developer and provider can best determine how the user interface is designed, including how many preferred languages are displayed.

Preliminary Cause of Death and Date of Death

In the Proposed Rule, we proposed that, for the inpatient setting, a Health IT Module must include the functionality to record, change, and access the "date of death." We stated that this functionality would be in addition to the requirement to enable a user to electronically

record, change, and access "preliminary cause of death" in case of mortality, as is included in the 2014 Edition "demographics" certification criterion.

Comments. The majority of commenters supported this requirement. A few commenters requested clarification as to whether the preliminary cause of death was to be recorded consistent with either the SNOMED CT® or ICD-10-CM standards.

Response. We thank commenters for their support and have adopted this requirement as proposed. We clarify that the preliminary cause of death is not required to be recorded in accordance with a standard for the purposes of certification to this criterion as we did not propose such a requirement nor have we adopted one.

Sexual Orientation and Gender Identity (SO/GI)

We did not propose to include a requirement to capture a patient's sexual orientation or gender identity as part of this criterion. Rather, we proposed the capture of SO/GI data as part of the proposed "social, psychological, and behavioral data" certification criterion.

Comments. We received a significant number of comments from providers, consumers/individuals, and health care coalitions strongly recommending that we consider including sexual orientation and gender identify as a component of the Base EHR definition (e.g., in the demographics certification criterion) or Common Clinical Data Set definition. These commenters suggested that there are mature vocabulary standards for representing SO/GI and there is strong clinical value in having this data to inform decisions about health care and treatment. Commenters indicated that by including SO/GI in the Base EHR or Common Clinical Data Set definitions, providers would be required to possess this functionality for participation in the EHR Incentive Programs, which could have a large impact for evaluating the quality of care provided to lesbian, gay, bisexual, and transgender (LGBT) communities.

Response. We thank commenters for their feedback. Given this feedback, the clinical relevance of capturing SO/GI, and the readiness of the values and vocabulary codes for representing this information in a structured way, we require that Health IT Modules enable a user to record, change, and access SO/GI to be certified to the 2015 Edition "demographics" certification criterion. By doing so, SO/GI is now included in the 2015 Edition Base EHR definition. The 2015 Edition Base EHR definition is part of the CEHRT definition under the EHR Incentive Programs. Therefore, providers participating in the EHR Incentive Programs will need to have certified health IT with the capability to capture SO/GI to meet the CEHRT definition in 2018 and subsequent years.

We note that like all information in the "demographics" criterion, certification does not require that a provider collect this information, only that certified Health IT Modules enable a user to do so. We believe including SO/GI in the "demographics" criterion represents a crucial first step forward to improving care for LGBT communities.

We have not included it in the Common Clinical Data Set at this time. We refer readers to section III.B.3 of this preamble for further discussion of the Common Clinical Data Set.

Comments. We received comments from a health care coalition that has partnered with and coordinated industry-development of the appropriate terminology to capture SO/GI for health care settings. The commenters suggested that we revise the proposed terminology for collecting SO/GI to use more appropriate language that reflects up-to-date, non-offensive terminology that will facilitate the goal of providing welcoming and affirming health care to LGBT individuals. As such, the commenters recommended that we retain the proposed SNOMED CT® and HL7 V3 codes but revise the description of some codes to use synonyms which reflect more appropriate language. The commenters noted that they have already

submitted revisions to SNOMED CT® to include the synonyms for these terms. The commenters also noted that the core concepts of the codes remain the same.

Response. We thank the commenters for the suggestion and are proceeding with the recommendation to include use the revised terminology for collecting SO/GI. We refer readers to § 170.207(o)(1) and § 170.207(o)(2) for a full list of the code descriptors and codes for SO/GI, respectively.

Comments. One commenter recommended we consider including structured and coded questions for soliciting SO/GI information as part of certification.

Response. While we thank the commenter for providing this recommendation, we do not believe that the suggested questions have not yet been scientifically validated for use in health care settings and, thus, have not adopted them. We do, however, believe that these questions are being used today in health care settings as "best practices," and would suggest that health care providers and institutions decide whether to include these questions in the collection of SO/GI information. These "best practice" questions and the answers we have adopted are:

- Do you think of yourself as:
    - Straight or heterosexual;
    - Lesbian, gay, or homosexual;
    - Bisexual;
    - Something else, please describe.
    - Don't know.
- What is your current gender identity? (Check all that apply.)
    - Male;
    - Female;

- Transgender male/Trans man/Female-to-male;
- Transgender female/Trans woman/Male-to-female;
- Genderqueer, neither exclusively male nor female;
- Additional gender category/(or other), please specify.
- Decline to answer.

Comments. One commenter recommended that we add another question and set of answers to collect assigned birth sex.

Response. We have not adopted this recommendation to collect assigned birth sex as suggested because we already require the capturing of birth sex as described under the "sex" section above.

- Problem List

2015 Edition Health IT Certification Criterion § 170.315(a)(6) (Problem list)

We proposed to adopt a 2015 Edition "problem list" certification criterion that was revised as compared to the 2014 Edition "problem list" certification criterion (§ 170.314(a)(5)) by requiring the September 2014 Release of the U.S. Edition of SNOMED CT® as the baseline version permitted for certification to this criterion. The Proposed Rule's section III.A.2.d ("Minimum Standards" Code Sets) discussed our adoption of SNOMED CT® as a minimum standards code set and the adoption of the September 2014 Release (U.S. Edition), or potentially a newer version if released before this final rule, as the baseline for certification to the 2015 Edition.

Comments. The majority of commenters supported the proposed certification criterion. A commenter suggested that instead of the full SNOMED CT® code system, the reference should be explicit to a concept and its value set relevant to this criterion, such as the "core" problem list.

A commenter recommended requiring certification to the most current version of SNOMED CT®. Some commenters recommended that we require the use of the ICD-10-CM code set. These commenters noted that the code set is used for billing purposes and the required use of SNOMED CT® adds burden on providers and their staff due to the required use of two different systems.

A couple of commenters stated that the problem list should not be limited to the duration of a hospitalization because it may be needed when the patient is out of the hospital, suggesting "for the duration of an entire hospitalization" be struck from the criterion. Another commenter suggested that the distinction between inpatient and ambulatory records should be dropped in favor of a "patient" record stating that several major healthcare systems have dropped the distinction and are focusing on a patient problem list where one or more problems on the problem list are addressed in a particular encounter (outpatient visit or inpatient stay).

Commenters suggested that if this criterion was adopted as proposed that health IT developers should have the ability to attest that their health IT previously certified to the 2014 Edition "problem list" criterion meets the newer baseline version of SNOMED CT® for the purposes of testing and certification to this criterion.

Response. We have adopted this certification criterion as proposed, except that we have adopted a newer baseline version SNOMED CT® (September 2015 Release of the U.S. Edition) for the purposes of certification. We refer readers to section III.A.2.c ("Minimum Standards" Code Sets) for a more detailed discussion of our adoption of the September 2015 Release of the U.S. Edition of SNOMED CT® and for our reasons why we always adopt a baseline version of a vocabulary code set for certification instead of specifying certification must be to the "most current" version. As with the 2014 Edition, testing and certification will focus on a Health IT

Module's ability to enable a user to record, change, and access a patient's problem list in accordance with SNOMED CT®. This will enable a provider to choose any available and appropriate code in SNOMED CT® for a patient's problems.

We did not propose as part of this criterion to test and certify a Health IT Module's ability to enable a user to record, change, and access a patient's active problem list and problem history across health care settings as this criterion is focused on the ambulatory and inpatient settings in support of the EHR Incentive Programs. We believe the use of "for the duration of an entire hospitalization" is appropriate for this criterion and refer readers to our detailed discussed of this determination in the 2014 Edition final rule (77 FR 54211-54212).

We agree with commenters that efficient testing and certification processes should be available to Health IT Modules previously certified to the 2014 Edition "problem list" criterion for certification to this criterion. Accordingly, we will consider such options, such as attestation, in developing the test procedure for this criterion and in issuing guidance to the ONC-AA and ONC-ACBs.

- Medication List

2015 Edition Health IT Certification Criterion § 170.315(a)(7) (Medication list)

We proposed to adopt a 2015 Edition "medication list" certification criterion that was unchanged as compared to the 2014 Edition "medication list" certification criterion (§ 170.314(a)(6)). To note, the proposed criterion does not reference any standards or implementation specifications.

Comments. The majority of commenters expressed support for this certification criterion as proposed. A few commenters suggested additional functionalities for this criterion. These suggestions included functionality to designate or mark medications as confidential or sensitive

and include patient-generated data. One commenter recommended requiring that medications be recorded in accordance with RxNorm. A couple of commenters requested clarification and expansion of the medication list to include over-the-counter medications, herbal supplements, medical cannabis, and oxygen. In general, a few commenters suggested that the medication list should be available across encounters and there should not be a distinction between inpatient and ambulatory records. One of these commenters noted that healthcare systems have dropped the distinction and are focusing on a patient medication list. Another commenter stated that the Food and Drug Administration (FDA) is currently working to implement requirements from the Drug Supply Chain Security Act (DSCSA) regarding standards for the interoperable exchange of information for tracing human, finished and/or prescription drugs. The commenter recommended that we be aware of these efforts and align current and future certification requirements with any future FDA requirements for standards-based identification of prescription drugs.

Response. We thank commenters for their support and have adopted this criterion as proposed. The other comments summarized above are outside the scope of the proposed criterion. We did not propose additional functionality for this criterion, including structured capture in accordance with RxNorm. We also did not propose as part of this criterion to test and certify a Health IT Module's ability to enable a user to record, change, and access a patient's active medication list and medication history across health care settings as this criterion is focused on the ambulatory and inpatient settings in support of the EHR Incentive Programs (please also see our response to comments for the "problem list" certification criterion above). Further, we do not define "medications" for the purpose of testing and certifying a Health IT Module's ability to enable a user to record, change, and access a patient's active medication list and medication history. We thank the commenter for the information related to FDA's work and

will take steps to ensure our work aligns with the relevant work of the FDA.

- Medication Allergy List

2015 Edition Health IT Certification Criterion § 170.315(a)(8) (Medication allergy list)

We proposed to adopt a 2015 Edition "medication allergy list" certification criterion that was unchanged as compared to the 2014 Edition "medication allergy list" certification criterion (§ 170.314(a)(7)).

Comments. The majority of commenters supported this criterion as proposed. Multiple commenters recommended adding functionality to support food and environmental allergies as well as other types of allergens, noting that most providers are already recording this information and that such functionality would support patient safety. Some of these same commenters recommended the structured capture of this information in various standards, including RxNorm, UNII, SNOMED CT®, and LOINC®. A couple of commenters recommended additional functionalities such as including time and date for medication allergies entered, edited, and deleted. In general, a few commenters suggested that the medication allergy list should be available across encounters and there should not be a distinction between inpatient and ambulatory records. One of these commenters noted that healthcare systems have dropped the distinction and are focusing on a patient medication allergy list. Another commenter stated that the FDA is currently working to implement requirements from the Drug Supply Chain Security Act (DSCSA) regarding standards for the interoperable exchange of information for tracing human, finished and/or prescription drugs. The commenter recommended that we be aware of these efforts and align current and future certification requirements with any future FDA requirements for standards-based identification of prescription drugs.

Response. We thank commenters for their support and have adopted this criterion as proposed. The other comments summarized above are outside the scope of the proposed criterion. We did not propose additional functionality for this criterion, including additional allergens and the structured capture of medication allergies. As we noted in the Proposed Rule (80 FR 16820), there are a number of vocabularies and code sets that could support food and environmental allergies as well as medications, but our view is that there is no ready solution for using multiple vocabularies to code allergies that could be adopted for the purposes of certification at this time. We also did not propose as part of this criterion to test and certify a Health IT Module's ability to enable a user to record, change, and access a patient's active medication allergy list and medication allergy history across health care settings as this criterion is focused on the ambulatory and inpatient settings in support of the EHR Incentive Programs (please also see our response to comments for the "problem list" certification criterion above). As noted in our response under the "medication list" certification criterion, we will take steps to ensure our work aligns with the relevant work of the FDA.

- Clinical Decision Support

2015 Edition Health IT Certification Criterion § 170.315(a)(9) (Clinical decision support)

We proposed to adopt a 2015 Edition "clinical decision support" (CDS) certification criterion that was revised in comparison to the 2014 Edition "CDS" criterion (§ 170.314(a)(8)). We proposed to require a Health IT Module to follow the updated Infobutton standard (Release 2, June 2014)[20] and one of two updated associated IGs: HL7 Implementation Guide: Service-Oriented Architecture Implementations of the Context-aware Knowledge Retrieval (Infobutton)

[20] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=208

Domain, Release 1, August 2013 ("SOA Release 1 IG"),[21] the updated Infobutton URL-based IG (HL7 Version 3 Implementation Guide: Context-Aware Knowledge Retrieval (Infobutton), Release 4, June 2014) ("URL-based Release 4 IG")[22]. We proposed to require certification only to the Infobutton standard (and an associated IG) for identifying diagnostic or therapeutic reference information, as we stated this is the best consensus-based standard available to support the use case. We requested comment on requiring that a Health IT Module be able to request patient-specific education resources identified using Infobutton standards based on a patient's preferred language. We proposed to require that a Health IT Module presented for certification to this criterion be able to record at least one action taken and by whom when a CDS intervention is provided to a user, and that a Health IT Module must generate either a human readable display or human readable report of the responses and actions taken and by whom when a CDS intervention is provided. We clarified that the 2015 Edition CDS certification criterion does not use the terms "automatically" and "trigger" as related to CDS interventions so as to reiterate the intent to encompass all types of CDS interventions without being prescriptive on how the interventions are deployed. We proposed cross-reference corrections to the 2014 Edition CDS criterion.

Infobutton Standard and Related IGs

Comments. A majority of commenters supported the inclusion of the updated Infobutton standard and related IGs. Multiple commenters recommended that there should be more options besides Infobutton for identifying diagnostic or therapeutic reference information. A commenter recommended a requirement for Infobutton to be connected to a reference resource at the end user's choice in cases of inability to use the Infobutton functionality due to contractual relationships to reference resources. Multiple commenters voiced a need for materials to be

[21] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=283
[22] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=22

tested and vetted to ensure the accuracy and appropriate literacy level of material, in addition to providers being able to provide educational resources from other sources in case the most appropriate material deemed by the physician cannot be identified or is limited by the health IT.

Response. We thank commenters for their support and have adopted the proposed Infobutton standard and supporting IGs. We clarify for commenters that our certification approach only focuses on capabilities that must be certified to meet this criterion. A health IT developer's product could include other means for identifying diagnostic or therapeutic reference information. Our approach actually reduces burden on health IT developers in that they do not have to have any other means tested and certified. In regard to comments suggesting the certification of the connection to a reference resource and diagnostic or therapeutic reference information obtained, these comments are beyond the scope of our proposal and we have not adopted them.

Preferred Language Request for Comment

Comments. Commenters expressed support for the capability to identify for a user diagnostic and therapeutic reference information based on a patient's preferred language with the use of Infobutton. Commenters stated that this would support reducing racial and ethnic health disparities by improving literacy and addressing language barriers. Some commenters contended that including such as requirement would increase burden for limited value because resources are often not available in other languages with the exception of three or four of the most commonly spoken languages.

Response. We appreciate the comments received in response to this request for comment, including those supporting the inclusion of preferred language. We have, however, not included preferred language functionality in this criterion. While this functionality many support reducing

health disparities, we believe that when weighing all proposed policies and the accumulated burden they present, this functionality would not provide as much impact in relation to other proposals such as the structured recording of a patient's preferred language and specific race and ethnicity information under the "demographics" criterion. By not adopting this functionality, health IT developers will be able to focus more of their efforts on other adopted functionality and requirements, including those that support the interoperability of health IT.

CDS Intervention Response Documentation

Comments. We received mixed comments in response to the proposed additional "recording user response" functionality for this criterion. While many commenters supported the overall goal of interaction checking for quality improvement and patient safety, many commenters stated that current systems already provide a wide range of functionality to enable providers to document decisions concerning CDS interventions. These commenters stated that the proposed "recording user response" is not necessary for certification or for providers to satisfy objectives of the EHR Incentive Programs.

Response. We have not adopted the "recording user response" functionality. This approach is responsive to comments suggesting that this functionality is already included in health IT and is unnecessary to support providers participating in the EHR Incentive Programs. Further, by not adopting this functionality, health IT developers will be able to focus more of their efforts on other adopted functionality and requirements, including those that support the interoperability of health IT.

Clarifying "Automatically" and "Triggered" Regulatory Text

Comments. Commenters expressed agreement with our proposal to not use the terms "automatically" and "trigger" in the 2015 Edition CDS criterion and that CDS interventions should be limited by how they are deployed.

Response. We thank commenters for their support. We have not included these terms in the certification criterion to clarify our intent to encompass all types of CDS interventions without being prescriptive on how the interventions are deployed.

Clinical Decision Support Configuration - Laboratory Tests and Values/Results

Comments. We received a comment seeking clarification on the criterion's reference to laboratory tests and values/results for CDS configuration capabilities related to the incorporation of a transition of care/referral summary. The commenter stated that we should remove reference to laboratory tests and values/results for CDS configuration in relation to the incorporation of a transition of care/referral summary because the proposed 2015 Edition "clinical information reconciliation and incorporation" criterion does not include reconciling laboratory tests and values/results.

Response. We have removed the references to laboratory tests and values/results from the criterion. The commenter is correct in that the 2015 Edition "clinical information reconciliation and incorporation" criterion does not include reconciling laboratory tests and values/results. Therefore, this data would not necessarily be available for CDS when a patient record is incorporated.

Reordering of Provisions/Regulation Text

We have reordered the provisions of the criterion/regulation text to better align with testing procedures. We have moved the CDS intervention interaction provision to the beginning, followed by the CDS configuration, evidence-based decision support interventions, linked

referential CDS, and source attributes. This reordering does not alter the requirements of the criterion in any way.

2014 Edition "Clinical Decision Support" Certification Criterion – Corrections

We received no comments on our proposal to revise the cross-reference in § 170.314(a)(8)(iii)(B)(2) (CDS configuration) to more specifically cross-reference the 2014 "transitions of care" ("ToC") criterion (§ 170.314(b)(1)(iii)(B)). Accordingly, we have adopted this proposed revision.

- Drug-Formulary and Preferred Drug List Checks

2015 Edition Health IT Certification Criterion § 170.315(a)(10) (Drug-formulary and preferred drug list checks)

In the Proposed Rule, we proposed to adopt a 2015 Edition "drug formulary checks and preferred drug list" certification criterion that was split based on drug formularies and preferred drug lists. We proposed that a Health IT Module must 1) automatically check whether a drug formulary exists for a given patient and medication and 2) receive and incorporate a formulary and benefit file according to the National Council for Prescription Drug Programs (NCPDP) Formulary and Benefit Standard v3.0 ("v3.0"). We proposed that a Health IT Module must automatically check whether a preferred drug list exists for a given patient and medication. For drug formularies and preferred drug lists, we proposed that a Health IT Module be capable of indicating the last update of a drug formulary or preferred drug list as part of certification to this criterion. We requested comment on more recent versions of the NCPDP Formulary and Benefit Standard to support functionality for receiving and incorporating a formulary and benefit file and sought to understand associated potential development burdens. In addition, we sought comment on a standard for individual-level, real-time formulary benefit checking to address the patient co-pay use case, whether we should offer health IT certification to the standard for this use case, and

if this functionality should be a separate criterion from the 2015 Edition "drug formulary and preferred drug list checks" certification criterion.

Comments. Commenters were supportive of splitting the drug-formulary checks functionality from the preferred drug list functionality. A number of commenters stated that the NCPDP Formulary and Benefit Standard provides static, group-level formulary pricing information that does not indicate individual-level, real-time prescription pricing information. A few commenters stated that these static, group-level formularies are not useful for informing discussions with patients about what medications to prescribe because they do not provide information about the patient's co-pay for a particular drug. Many commenters also suggested that it was not necessary for ONC to offer certification to this functionality because most health IT systems already support NCPDP's Formulary and Benefit Standard v3.0 due to the Medicare Part D e-prescribing requirements under the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA). Some of these commenters even indicated that they test and certify through Surescripts' certification program to the standard. In terms of a version of the NCPDP Formulary and Benefit Standard, stakeholders preferred ONC adopt v3.0 rather than any subsequent version to align with the Medicare Part D requirements. Commenters also contended that the industry has widely adopted v3.0 and that newer versions are less stable.

Many commenters stated that there is not an industry-wide accepted standard for real-time individual patient-level formulary checking, but recommended ONC adopt certification to a standard once the industry moves to an agreed-upon standard. A few commenters noted that an NCPDP task group is analyzing use cases to support a real-time prescription benefit inquiry and is planning to make recommendations to the NCPDP membership on the creation of a new transaction and/or standard or modification of existing transactions or standards.

Response. We appreciate the detailed feedback commenters provided. We have determined that it is most appropriate to not adopt a specific standard for this criterion. We agree with commenters that the NCPDP Formulary and Benefit Standard v3.0 is widely implemented today in support of Medicare Part D requirements and that certification to this standard would add unnecessary burden to health IT developers and providers who are already adhering to the standard.

We believe that certification for individual-level, real-time prescription pricing information will provide the most value to inform provider prescribing decisions and discussions between providers and patients on the most appropriate medication options for the patient. However, at this time, there is no real-time patient-level standard with consensus stakeholder support that would be appropriate for certification. Based on the comments received, we strongly urge the industry to accelerate its work on identifying the need to create a new transaction and/or standard or modify existing transactions or standards for real-time prescription benefit inquiries. We intend to continue our participation in this area and will consider proposing certification functionalities for real-time prescription benefit inquiries in future rulemaking.

With consideration of comments supporting our proposed split of functionality between drug formularies and preferred drug lists, we have adopted a 2015 Edition "drug-formulary and preferred drug list checks" criterion that simply separates drug formulary and preferred drug list functionality, but does not require any standards or functionality beyond that included in the 2014 Edition "drug-formulary checks" criterion. As such, this certification criterion is eligible for gap certification.

- Smoking Status

2015 Edition Health IT Certification Criterion
§ 170.315(a)(11) (Smoking status)

We proposed to adopt a 2015 Edition "smoking status" certification criterion that was revised in comparison to the 2014 Edition "smoking status" criterion (§ 170.314(a)(11)) and to include the 2015 Edition certification criterion in the 2015 Edition Base EHR definition. To be certified, we proposed that a Health IT Module must record, change, and access smoking status to any of the September 2014 Release of the U.S. Edition of SNOMED CT® available codes for smoking status, at a minimum. We noted that a Health IT Module certified to certification criteria that reference the Common Clinical Data Set (i.e., the "transitions of care" ("ToC"), "data export" (previously "data portability"), "view, download, and transmit to 3rd party" (VDT), "Consolidated CDA creation performance," and "application access to the Common Clinical Data Set" certification criteria) would need to be able to code smoking status in only the 8 smoking status codes, [23] which may mean mapping other smoking status codes to the 8 codes. We explained that we expect Health IT developers to work with health care providers to include the appropriate implementation of smoking status codes in a user interface.

Comments. Some commenters stated that health IT should not be required to support the full set of smoking status codes within SNOMED CT® as it would cause unnecessary development burden and potential workflow issues for providers. Multiple commenters also expressed concern with the proper mapping all of the available smoking status codes within SNOMED CT® to the specified 8 SNOMED CT® smoking codes in the Common Clinical Data Set and used for exchange of patient health information. We also received comments requesting the inclusion of other substances and routes of administration, including the use of chewing tobacco.

[23] These 8 codes are: current every day smoker, 449868002; current some day smoker, 428041000124106; former smoker, 8517006; never smoker, 266919005; smoker – current status unknown, 77176002; unknown if ever smoked, 266927001; heavy tobacco smoker, 428071000124103; and light tobacco smoker, 428061000124105.

Response. We have adopted a "smoking status" certification criterion that does not reference a standard. As stated in the Proposed Rule (80 FR 16870), the capture of a patient's smoking status has significant value in assisting providers with addressing the number one cause of preventable death and disease in the United States. We have also included this criterion in the Base EHR definition so that this functionality is available to all providers participating in the EHR Incentive Programs. In consideration of the concerns expressed by commenters regarding development burden and the proper mapping of all available smoking status codes within SNOMED CT® to the specified 8 SNOMED CT® for exchange, we believe that the best path forward is the adoption of a "smoking status" criterion that would simply require a Health IT Module to demonstrate that it can enable a user to record, change, and access a patient's smoking status. In regard to comments suggesting the inclusion of other substances and routes of administration, these comments are beyond the scope of our proposal and we have not adopted them. In sum, this certification criterion is "unchanged" as compared to the 2014 Edition "smoking status" criterion and is eligible for gap certification.

As discussed in more detail under section III.B.3 of this preamble, we have adopted the 8 specified SNOMED CT® smoking codes as part of the Common Clinical Data Set (and for purposes of exchange). This is a continuation of our approach first adopted with the 2014 Edition.

- Family Health History

2015 Edition Health IT Certification Criterion
§ 170.315(a)(12) (Family health history)

We proposed to adopt a 2015 Edition "family health history" (FHH) certification criterion that was revised in comparison to the 2014 Edition FHH certification criterion adopted at § 170.314(a)(13). In particular, we proposed to require a Health IT Module to enable a user to

record, change, and access a patient's FHH electronically according to, at a minimum, the concepts or expressions for familial conditions included in the September 2014 Release of the U.S. Edition of SNOMED CT®, which would be a newer baseline version of SNOMED CT® than adopted for the 2014 Edition FHH criterion. The proposed rule's section III.A.2.d ("Minimum Standards" Code Sets) discussed our adoption of SNOMED CT® as a minimum standards code set and the adoption of the September 2014 Release (U.S. Edition), or potentially a newer version if released before a this final rule, as the baseline for certification to the 2015 Edition.

Comments. Commenters generally supported this certification criterion. Some commenters suggested not adopting this criterion because it does not support a specific meaningful use objective of the proposed EHR Incentive Programs Stage 3. A couple of commenters suggested the recording of FHH is more valuable when it is actually exchanged, with one commenter recommending that we require FFH data be sent using the C-CDA FHH Section with Entries or, minimally, the C-CDA FHH Organizer Entry. Another commenter suggested that the FHH be stored in a question/answer format (LOINC® for "questions" (observations) and SNOMED CT® for "answers" (observation values)), which would also better support electronic exchange of the information. Some commenters suggested that if this criterion was adopted as proposed that health IT developers should have the ability to attest that their Health IT previously certified to the 2014 Edition FHH criterion meets the newer baseline version of SNOMED CT® for the purposes of testing and certification to this criterion.

Response. We have adopted this certification criterion as proposed, except that we have adopted a newer baseline version SNOMED CT® (September 2015 Release of the U.S. Edition) for the purposes of certification. We refer readers to section III.A.2.c ("Minimum Standards"

Code Sets) for a more detailed discussion of our adoption of the September 2015 Release of the U.S. Edition of SNOMED CT®. While not supporting a specific meaningful use objective of Stage 3 of the EHR Incentive Programs, this functionality is included in the CEHRT definition. Furthermore, we believe that the FHH functionality is a functionality that should be available to providers for more comprehensive patient care.

We note that our intent is not to limit the use of LOINC® for associated FHH "questions" or the specific SNOMED CT® code that is used to label FHH. Rather, the intent is to capture this information in SNOMED CT® instead of billing terminologies like ICD-10-CM. We also do not intend to prohibit the exchange of this information using the C-CDA 2.1. As we have noted in this and prior rulemakings, certification serves as a baseline. This baseline can be built upon through future regulation or simply through a decision by a health IT developer and/or its customer to include functionality that goes beyond the baseline. As present, we have set the certification baseline for FHH information at recording it in SNOMED CT®.

We agree with commenters that efficient testing and certification processes should be available to Health IT Modules previously certified to the 2014 Edition FHH criterion for certification to this criterion. Accordingly, we will consider such options, such as attestation, in developing the test procedure for this criterion and in issuing guidance to the ONC-AA and ONC-ACBs.

- Patient-Specific Education Resources

2015 Edition Health IT Certification Criterion § 170.315(a)(13) (Patient-specific education resources)

In the Proposed Rule, we proposed to adopt a 2015 Edition "patient-specific education resources" certification criterion that was revised in comparison to the 2014 Edition "patient-specific education resources" certification criterion (§ 170.314(a)(15)). We proposed that

certification would only focus on the use of Infobutton for this certification criterion instead of Infobutton and any means other than Infobutton as required by the 2014 Edition criterion. We stated that there is diminished value in continuing to frame the 2015 Edition certification criterion similarly to the 2014 Edition criterion.

We proposed to adopt the updated Infobutton standard (Release 2 and the associated updated IGs (SOA-based IG and URL-based IG)). We also noted that we would not include a requirement that health IT be capable of electronically identifying patient-specific education resources based on "laboratory values/results" because the Infobutton standard cannot fully support this level of data specificity.

We proposed that a Health IT Module be able to request patient-specific education resources based on a patient's preferred language as this would assist providers in addressing and mitigating certain health disparities. More specifically, we proposed that a Health IT Module must be able to request that patient-specific education resources be identified (using Infobutton) in accordance with RFC 5646. We noted that Infobutton only supports a value set of ISO 639-1 for preferred language and, therefore, stated that testing and certification of preferred language for this certification criterion would not go beyond the value set of ISO 639-1. We further noted testing and certification would focus only on the ability of a Health IT Module to make a request using a preferred language and Infobutton because the language of patient education resources returned through Infobutton is dependent on what the source can support.

Comments. Multiple commenters supported the inclusion of the updated Infobutton standard and supporting IGs. A few commenters expressed concern about limiting certification to only Infobutton and suggested there are other viable options for requesting patient-specific education resources. A commenter requested clarification as to whether providers must only use

certified health IT for requesting patient-specific education resources for the purposes of participating in the EHR Incentive Programs.

Response. We thank commenters for their support and have adopted the proposed Infobutton standard and supporting IGs. We continue to believe that the Infobutton capability is important to be available to providers to have and use to identify patient-specific education resources. We clarify for commenters that our certification approach only focuses on capabilities that must be certified to meet this criterion. A health IT developer's product could include other means for requesting patient-specific education resources. Our approach actually reduces burden on health IT developers in that they do not have to have any other means tested and certified. For questions related to the EHR Incentive Programs, we refer readers to CMS and the EHR Incentive Programs Stage 3 and Modifications final rule published elsewhere in this issue of the **Federal Register**.

Comments. We received a few comments supporting our approach for "laboratory values/results."

Response. We have not included "laboratory values/results" as patient data that must be used to identify patient-specific education resources.

Comments. Commenters expressed strong support for the capability to request patient-specific education materials based on a patient's preferred language with the use of Infobutton. Commenters stated that this would support reducing racial and ethnic health disparities by improving literacy and addressing language barriers. Commenters also expressed a need for materials to be tested and vetted to ensure the accuracy and appropriate literacy level of the materials. Some commenters contended that this requirement would increase burden for limited

value because educational resources are often not available in other languages with the exception of three or four of the most commonly spoken languages.

Response. We thank commenters for their support and feedback. With consideration of the mixed feedback, we have determined to designate the use of preferred language as an optional provision within this criterion. As optional, health IT developers have flexibility to pursue certification if they deem it advantages. With our new open data CHPL (see section IV.D.3 of this preamble), information on whether a Health IT Module was certified to this functionality would be readily available for consumers.

- Implantable Device List

2015 Edition Health IT Certification Criterion § 170.315(a)(14) (Implantable device list)

In the Proposed Rule, we proposed to adopt a new 2015 Edition certification criterion focused on the ability of health IT to exchange, record, and allow a user to access a list of Unique Device Identifiers (UDIs)[24] associated with a patient's implantable devices. Health IT certified to the proposed criterion would be able to "parse" a UDI into its constituent components (or "identifiers") and make those accessible to the user. Separately, the health IT would be able to retrieve and provide a user with access to, if available, the optional "Device Description" attribute associated with a UDI in the FDA's Global Unique Device Identification Database (GUDID). Further, to facilitate the exchange of UDIs and increase their availability and reliability in certified health IT, we proposed to include the proposed 2015 Edition implantable

[24] A UDI is a unique numeric or alphanumeric code that consists of two parts: (1) a device identifier (DI), a mandatory, fixed portion of a UDI that identifies the labeler and the specific version or model of a device, and (2) a production identifier (PI), a conditional, variable portion of a UDI that identifies one or more of the following when included on the label of a device: the lot or batch number within which a device was manufactured; the serial number of a specific device; the expiration date of a specific device; the date a specific device was manufactured; the distinct identification code required by 21 CFR 1271.290(c) for a human cell, tissue, or cellular and tissue-based product (HCT/P) regulated as a device. 21 CFR 801.3. See also http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/UniqueDeviceIdentification/.

device list certification criterion in the 2015 Edition Base EHR definition and to include a patient's UDIs as data within the CCDS definition for certification to the 2015 Edition. We also proposed to modify § 170.102 to include new definitions for "Device Identifier," "Implantable Device," "Global Unique Device Identification Database (GUDID)," "Production Identifier," and "Unique Device Identifier."

We explained that the purpose of the proposed implantable device list certification criterion was to enable the baseline functionality necessary to support the exchange and use of UDIs in certified health IT. The need to exchange and have access to this information wherever patients seek care is broadly relevant to all clinical users of health IT, regardless of setting or specialty, so that they may know what devices their patients are using (or have used) and thereby prevent device-related adverse events and deliver safe and effective care.[25] This need is most acute for implantable devices, which by their nature are difficult to detect and identify in the absence of reliable clinical documentation.

We acknowledged in the Proposed Rule that fully implementing UDIs in health IT will take time and require addressing a number of challenges. Nevertheless, we noted that substantial progress has been made. In particular, we summarized the FDA's regulatory activities and timeline for implementing the Unique Device Identification System and extensive work by public and private sector stakeholders to advance standards and specifications in support of UDI use cases. On the basis of these developments and our own ongoing consideration of these and other issues,[26] we recognized that while "the path to full implementation is complex, there are

[25] In addition, as UDIs become ubiquitous, UDI capabilities in health IT will support other important benefits, including better surveillance and evaluation of device performance and more effective preventative and corrective action in response to device recalls.

[26] As further context for our proposal, we described our previous consideration of these and other issues related to UDI adoption in a previous rulemaking. 79 FR 10894.

relatively straightforward steps" that we could take now to support the electronic exchange and use of UDIs, beginning with UDIs for implantable devices. Our proposed certification criterion focused narrowly on implementing these first steps.

In light of the foregoing and with the revisions discussed below in our analysis of the comments on this proposal, we have finalized a 2015 Edition "implantable device list" certification criterion. We have also finalized our proposals to include this certification criterion in the 2015 Base EHR definition and to include a patient's UDIs as data within the 2015 Common Clinical Data Set definition. Discussion of those proposals can be found elsewhere in this final rule.

Comments. Most commenters agreed with the central premise of our proposal, that enabling the exchange and use of UDIs in certified health IT is a key initial step towards realizing the substantial patient safety, public health, and other benefits of UDIs and the Unique Device Identification System. Many commenters strongly supported the proposed criterion, including its focus on implantable devices. Commenters stated that the ability to exchange and access identifying information about patients' implantable devices wherever patients seek care would enable clinicians to prevent device-related medical errors and improve the quality of care provided to patients. Commenters also stated that the need to access accurate information about patients' implantable devices is broadly applicable to primary care physicians, specialists, and other providers to support care coordination and ensure that providers have a complete medical history of their patients.

Many commenters supported the proposed criterion in full and recommended that we finalize it without any substantial revision. A significant number of commenters also urged to expand the scope of this criterion to include additional UDI-related capabilities. In contrast, a

significant number of commenters stated that we should not finalize this criterion or should make all or part of it an optional certification criterion for the 2015 Edition. Commenters also offered a variety of suggested revisions and refinements with respect to the capabilities we proposed.

Response. We have adopted this certification criterion substantially as proposed, subject to certain revisions and clarifications discussed further below in response to the comments we received. We thank commenters for their detailed and thoughtful feedback on our proposal. We reiterate that this certification criterion represents a first step towards enabling the widespread exchange and use of UDIs and related capabilities in certified health IT, beginning with implantable devices. Because we recognize that fully implementing UDIs in health IT will take time and require addressing a number of challenges, the certification criterion focuses narrowly on baseline health IT capabilities that developers can feasibly implement today. These capabilities will provide the foundation for broader adoption and more advanced capabilities and use cases. We believe that this approach minimizes the potential burden while maximizing the impact of this criterion for all stakeholders.

Comments. A significant number of commenters who supported our proposed implantable device list certification criterion also recommended that we adopt additional UDI-related capabilities, either as part of this criterion (which we proposed to reference in the 2015 Edition Base EHR definition) or as a separate, optional certification criterion. Many commenters urged us to include requirements for Automatic Identification and Data Capture (AIDC) of UDIs. Commenters stated that such a requirement would facilitate the accurate and efficient capture of UDIs and align this criterion with the UDI final rule, which requires UDIs to support one or more forms of AIDC. Some commenters also stated that if we did not require—or at least provide the option for—AIDC, users may be forced to manually enter

UDIs. They stated that this could discourage them from capturing UDIs, which could lead to incomplete or inaccurate information about patients' implantable devices. Separate from AIDC, several commenters suggested that we adopt other UDI-related capabilities, such as the ability to generate lists of patients with a particular device; to generate notifications to patients in the event of a device recall; and to record and track information about non-implantable devices and medical and surgical supplies that are not regulated as a device.

Response. We have not adopted any AIDC requirements for UDIs as part of this final rule. While we unequivocally agree with commenters that UDIs should be captured using AIDC and should rarely if ever be manually entered; and while for this reason we strongly urge health IT developers and heath care organizations to implement AIDC capabilities in all settings and systems in which UDIs may be captured; yet for the reasons elaborated below, we believe at this time that certification is neither an effective nor appropriate means to further these policies. As we explained in the Proposed Rule, this criterion is not intended to provide the capability to enter or "capture" UDIs for implantable device, such as during the course of a procedure. The reason for this is that the capture of UDIs currently occurs in a wide variety of "upstream" IT systems and settings that are beyond the scope of the current ONC Health IT Certification Program. Rather than ineffectually trying to address these "upstream" use cases, we have chosen to focus this certification criterion on the baseline functionality necessary to ensure that, once recorded in a patient's electronic health record, UDIs can be exchanged among "downstream" health IT systems (the overwhelming majority of which we do certify) and accessed by clinicians wherever patients seek care.

Some commenters understood our rationale for not requiring AIDC capabilities for all certified health IT and instead recommended we adopt a separate optional AIDC certification

criterion that could be leveraged by certified health IT designed for operating rooms and other surgical settings in which devices are implanted or removed. While we appreciate the suggestion, such a certification criterion would be applicable to only a small subset of certified health IT, which in turn represents only a small subset of IT systems used to capture UDIs for implantable devices. Moreover, prescribing specific AIDC requirements for certified health IT may also be unnecessary. Given the obvious convenience, accuracy, and other advantages of AIDC, we anticipate that users of certified health IT designed for surgical settings will expect developers to include AIDC capabilities as a necessary complement to the baseline implantable device list functionality required by this criterion. Allowing developers and their customers to design and implement the most appropriate AIDC solutions for their individual needs is consistent with FDA's policy of permitting flexibility in the use of these technologies and avoids imposing unnecessary requirements and costs on developers, providers, and our testing and certification bodies.

Contrary to the suggestions of some commenters, our decision not to adopt a particular AIDC requirement for implantable devices does not mean that users of certified health IT systems will be forced to manually record UDIs. Again, for the reasons we have stated, this criterion has no bearing on how UDIs are entered or captured in upstream IT systems during a procedure or operation. It is tailored solely to bringing and providing capabilities for UDIs to downstream EHR and health IT systems used in physicians' offices, hospitals, and other places where patients with implantable devices seek care.

Similarly, at this time we believe that it would be premature to include other capabilities suggested by commenters. Some of those capabilities—such as the ability to record information about non-implantable devices—are beyond the scope of the proposal. For other capabilities,

greater adoption and use of UDIs in certified health IT is needed before the capabilities will be useful to most health IT users. For example, we recognize that being able to generate a list of patients with a particular device will be necessary to respond to device recalls and analyze device performance and other characteristics. But those benefits cannot materialize until UDIs are more broadly and more readily accessible through interoperable health IT and health information exchange. Likewise, achieving these benefits will first require implementing other baseline functionality included in this criterion, such as the ability to retrieve key device attributes from the GUDID. We think that focusing the requirements of this criterion—and thus the efforts of developers and users of certified health IT—on these essential baseline functionalities is the quickest path to the adoption of UDIs in health IT and thus to creating demand and opportunities for the more advanced capabilities commenters envision.

Comments. Some commenters requested clarification as to what constitutes an "implantable device" for purposes of this certification criterion.

Response. We have adopted new definitions in § 172.102 for "Implantable Device" and several other terms by cross-referencing the definitions for those terms already provided at 21 CFR 801.3. We believe adopting these definitions in our final rule will prevent any interpretative ambiguity and ensure that each phrase's specific meaning reflects the same meaning given to it in the Unique Device Identification System final rule. For further discussion of these new definitions, we refer readers to section III.B.4 of this preamble.

Comment. A commenter recommended that we use the term "identifier" instead of the term "data element" to refer to the following identifying information that composes the Production Identifier portion of a UDI:

- the lot or batch within which a device was manufactured;

- the serial number of a specific device;
- the expiration date of a specific device;
- the date a specific device was manufactured; and
- for an HCT/P regulated as a device, the distinct identification code required by 21 CFR § 1271.290(c).

To avoid confusion and align our terminology with the UDI final rule, the commenter recommended we refer to these "data elements" as "identifiers" or "production identifiers."

Response. We agree that our use of the term "data elements" was imprecise and could lead to unnecessary confusion. Accordingly, we have revised our terminology as follows to align more closely with the UDI final rule.

In our proposal, we used the term "data elements" to describe two distinct types of information associated with UDIs. First, we said that a Health IT Module certified to our proposed criterion would have to be able to parse certain "data elements from a UDI" and make these accessible to a user. 80 FR 16825. In that context, we were referring to what the UDI final rule describes as the "production identifiers that appear on the label of the device." 21 CFR 830.310(b)(1). These are the identifiers listed above that compose and are required to be included in the Production Identifier when required to be included on the label of a device. 21 CFR 801.3. Because these identifiers are part of the UDI, health IT should be able to parse these identifiers from the UDI using the issuing agency's specifications. There is no need to query an external database or source, such as the GUDID.

Second, we also used the same term, "data element," to refer to certain information not included in the UDI itself but that is associated with the UDI and can be retrieved using the GUDID. Specifically, we proposed that health IT be able to retrieve and make accessible the

optional "Device Description" attribute associated with the Device Identifier portion of the UDI (assuming the attribute has been populated in the GUDID).

To distinguish these separate concepts and for consistency with the UDI final rule, this preamble and the corresponding regulation at § 170.315(a)(14) use the terms "identifier" and "attribute" to refer to the two distinct types of information described above.

Comments. Many commenters, including some health IT developers, supported the requirement to parse a UDI and allow a user to access the identifiers that compose the UDI. Other commenters stated that requiring this functionality would be burdensome because UDIs may be issued by different issuing agencies and in different formats. Some commenters suggested we withdraw this proposed requirement until a canonical format is established to harmonize and streamline the process of parsing UDIs issued by different FDA-accredited issuing agencies and in different formats.

A number of commenters pointed out that we had omitted from this requirement the Distinct Identification Code required by 21 CFR 1271.290(c), which is one of the five identifiers that make up the Production Identifier and applies to human cells, tissues, or cellular and tissue-based products (HCT/P) regulated as a device, including certain kinds of implantable devices (e.g., skin grafts and bone matrixes). To ensure the exchange of UDIs for all implantable devices and to avoid misalignment with the UDI final rule, we were urged to include the Distinct Identification Code among the identifiers that technology must be able to parse and make accessible to a user under this criterion.

Response. The requirement to parse a UDI is reasonable despite the existence of multiple issuing agencies and formats. We disagree that this requirement is burdensome and note that it was supported by several health IT developers. This criterion would require health IT to be able

to parse UDIs issued by FDA-accredited issuing agencies. There are currently three FDA-accredited issuing agencies (GS1, HIBCC, and ICCBBA)[27] and each issuing agency has only one approved UDI format. All three formats are unique and can thus be readily distinguished by health IT and parsed according to the correct format. The formats themselves are described in detail in a single five-page reference document available on the FDA website.[28] Each format has been approved by the FDA, and no changes can be made unless the FDA similarly approves of the changes prior to implementation.

We disagree that the requirement to parse a UDI should be postponed until the emergence of a single canonical UDI format. It is unclear at this time when or if such a canonical format will be developed and whether it would support the functionality we are requiring. It is also unclear whether implementing a canonical format would reduce or increase the overall technical complexity and burden of implementing these capabilities for multiple UDI formats. Meanwhile, postponing these capabilities would frustrate the purpose of this certification criterion. Without the ability to parse a UDI, health IT would be unable to provide users with useful information identifying and safety-related information about a device, such as the device's expiration date (which will be parsed from the Production Identifier) or a description of the device (which will be retrieved by parsing and looking up the Device Identifier in the GUDID).

The omission of "Distinct Identification Code required by 21 CFR 1271.290(c)" among the identifiers that health IT must be able to parse was an oversight, and we thank commenters

---

[27] http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/UniqueDeviceIdentification/UDIIssuingAgencies/default.htm.

[28] FDA, UDI Formats by FDA-Accredited Issuing Agency (May 7, 2014), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/UniqueDeviceIdentification/GlobalUDIDatabaseGUDID/UCM396595.doc. The reference document is one of two technical documents made available by the FDA to assist labelers and other persons to comply with the GUDID Guidance. See http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/UniqueDeviceIdentification/GlobalUDIDatabaseGUDID/ucm416106.htm.

for bringing it to our attention. We agree that to avoid misalignment with the UDI final rule, health IT should be required to parse this identifier and make it accessible in the same manner required for the other identifiers that compose the Production Identifier, as referenced in the Proposed Rule. We therefore include it with those identifiers at §170.315(a)(14)(ii). For similar alignment and consistency, we also include the Production Identifier itself in the list of identifiers at §170.315(a)(14)(ii).

Comments. Several commenters objected to the proposed requirement that health IT be able to query a UDI against the GUDID and retrieve the associated "Device Description" attribute (when that attribute has been populated and is available). Some commenters stated that it was unreasonable to expect developers to implement GUDID capabilities before all of the planned GUDID functionality is available. At the time of the Proposed Rule, the GUDID was available as a downloadable file, which was and continues to be updated daily. A web interface and web services were also planned but had not yet been implemented. Although we explained that the daily downloadable version of GUDID could be used to satisfy the proposed criterion, some commenters insisted that we should not require any GUDID retrieval capabilities until web services are in place to enable GUDID attributes to be easily retrieved "on demand." Several commenters requested that we clarify FDA's timeline for implementing web services.

Response. FDA has partnered with the National Library of Medicine (NLM) to implement the GUDID. The GUDID is now available via a web interface called AccessGUDID.[29] In addition, FDA has confirmed that web services will be available via the AccessGUDID website by October 31, 2015. These web services are being implemented to

[29] See http://accessgudid.nlm.nih.gov/. A list of APIs currently in development is available at http://accessgudid.nlm.nih.gov/docs.

support health IT developers to meet this implantable device list certification criterion. For any valid UDI, the web services will return the following GUDID attributes:

- "GMDN PT Name";
- "Brand Name";
- "Version or Model";
- "Company Name";
- "What MRI safety information does the labeling contain?"; and
- "Device required to be labeled as containing natural rubber latex or dry natural rubber (21 CFR 801.437)."

In addition to these GUDID attributes, and for the convenience of health IT developers, the web services will also return the "SNOMED CT® Identifier" and the "SNOMED CT® Description" mapped to the GMDN code set.[30]

As commenters acknowledged, including many who objected to this requirement, the availability of dedicated web services for retrieving the attributes associated with a UDI from the GUDID will significantly streamline and reduce the costs of including this functionality in certified health IT. We take the commenters at their word and believe that the availability of these dedicated web services—which will be specifically designed for health IT developers and aligned with this certification criterion—will substantially mitigate the concerns raised by developers and other commenters regarding the potential burden or technical challenges of implementing GUDID functionality.

[30] Under a Cooperative Agreement between the Global Medical Device Nomenclature Agency and the International Health Terminology Standards Development Organization (IHTSDO), GMDN will be used as the basis for the medical device component of SNOMED CT®. See http://www.ihtsdo.org/resource/resource/84.

Comments. Several commenters were puzzled by our proposal to require retrieval only of the "Device Description" attribute. They pointed out that submission of this attribute to the GUDID is optional and is not standardized. The proposed requirement would therefore be unlikely to serve our goal of providing clinicians and patients with accurate and accessible information about implantable devices. Some commenters suggested that the "Global Medical Device Nomenclature (GMDN) PT Name" attribute would better suit our purpose and noted that this attribute, unlike "Device Description," is a required attribute and a recognized international standard for medical device nomenclature.

Several commenters also urged us to require retrieval of additional GUDID attributes. Several commenters noted that certain safety-related attributes—specifically "What MRI safety information does the labeling contain?" and "Device required to be labeled as containing natural rubber latex or dry natural rubber (21 CFR 801.437)"—are required to be submitted to the GUDID, are already available, and would significantly further the patient safety aims outlined in our proposal. Along the same lines, other commenters identified additional GUDID attributes that would enable identification of the manufacturer or labeler (i.e., company name), brand, and specific version or model of a device.

Response. We believed that retrieving the "Device Description" attribute would be a good starting point for GUDID functionality under this criterion and would make the implantable device list more useful to clinicians by displaying the familiar name of each device in the list next to the device's UDI. Based on the comments, we accept that the "GMDN PT Name" attribute is more suitable for our purposes because it is a recognized international standard for medical devices and, unlike the "Device Description" attribute, is required and therefore much more likely to in fact be populated in the GUDID. We are therefore revising §170.315(a)(14)(iii)

to require the "GMDN PT Name" attribute instead of "Device Description." Relatedly, we have also revised §170.315(a)(14)(iii) to permit health IT developers who meet this requirement using the GUDID web services to do so in either of two ways. They may either retrieve the "GMDN PT Name" attribute or, alternatively, the "SNOMED CT® Description" associated with a UDI. Pursuant to a cooperative agreement between the relevant standards developing organizations, the SNOMED CT® code set is being mapped to GMDN PT and thus the description of a device will be identical under both terminologies. However, we expect that many developers will prefer to use the SNOMED CT® code set because they already do so and because they can retrieve the computable "SNOMED CT® Identifier," which will also be available via the web services and will enable developers to more easily deploy CDS and other functionality for implantable devices. Thus allowing developers the flexibility to retrieve the "SNOMED CT® Description" in lieu of the identical mapped "GMDN PT Name" attribute will avoid requiring them to support multiple and duplicative code sets for medical devices and may also encourage them to incorporate more advanced capabilities for implantable devices, consistent with the goals of this criterion.

As discussed above, the GUDID web interface is now available via the NLM AccessGUDID website, which will soon be augmented with dedicated web services designed to support health IT certified to this criterion. With this increased readiness of the GUDID, health IT should be able to retrieve additional GUDID attributes with little additional effort. Therefore, we are also including the following attributes among those that must be retrieved and made accessible to users of health IT certified to this criterion:

- "Brand Name";
- "Version or Model";

- "Company Name";
- "What MRI safety information does the labeling contain?"; and
- "Device required to be labeled as containing natural rubber latex or dry natural rubber (21 CFR 801.437)."[31]

For the reasons that commenters identified, these particular attributes will further the core goals of this criterion by significantly enhancing the ability of clinicians to identify and access important safety-related information about their patients' implantable devices.

Comment. A commenter noted that this criterion would require health IT to retrieve UDI attributes exclusively from the GUDID. The commenter recommended we consult with FDA to ensure that the GUDID will be able to support the potentially large volume of requests that could result from this requirement.

Response. As discussed above, FDA and NLM are implementing web services specifically to support health IT developers to meet this implantable device list certification criterion. FDA has signed an interagency agreement with NLM to provide public access to AccessGUDID, including web services. NLM has experience with large volume requests and will be able to meet any demands generated by developers and users as a result of this criterion.

Comments. Some commenters noted that UDI attributes are not exclusive to the GUDID and are commonly stored in providers' enterprise resource planning systems (ERPS), materials management information systems (MMIS), and other "systems of record." Thus, instead of requiring health IT to always retrieve the UDI attributes from the GUDID, it was suggested that we permit attributes to be retrieved from these and other appropriate sources, thereby giving

[31] Current GUDID attributes are derived from the UDI final rule and are specified in the FDA GUDID Data Elements Reference Table (May 1, 2015), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/UniqueDeviceIdentification/GlobalUDIDatabaseGUDID/UCM396592.xls

providers and developers (who may have different database and technical infrastructures) the flexibility to select the most appropriate source of this information.

Response. As we stated in the Proposed Rule, the requirement to retrieve attributes from the GUDID can be accomplished using the GUDID's web interface, web services, downloadable module, or any other method of retrieval permitted under FDA's GUDID guidance. Thus GUDID attributes could be retrieved from a local system, provided the information in that system is up to date and is based upon the data downloaded from the GUDID. That said, we encourage the use of the AccessGUDID web services, which as discussed above are being designed specifically to support health IT developers to meet this implantable device list certification criterion.

Comments. Commenters overwhelmingly supported our proposal to require that health IT enable a user to change a UDI in a patient's implantable device list and, in appropriate circumstances, "delete" erroneous, duplicative, or outdated information about a patient's implantable devices. However, several commenters took issue with our use of the term "delete," which could imply that a user should be able to completely remove a UDI and associated information from a patient's implantable device list and from the patient's electronic health record altogether. Commenters stated that information about a patient's implantable devices should be retained for historical accuracy and context. One commenter noted that allowing users to delete this information could violate record retention laws. Several commenters suggested that we clarify that a user should be able to "flag" or otherwise annotate a UDI as no longer active while still retaining the UDI and associated information.

The comments on this aspect of our proposal suggest some confusion surrounding the concept of an "implantable device list" contemplated in the Proposed Rule. Different commenters used the term "implantable device list" to refer to at least three distinct constructs:

(1) the list of UDIs that would be recorded and exchanged as structured data; (2) the presumably more detailed list of information about a patient's implantable devices that would subsist separately and locally in EHR systems; and (3) the list of UDIs and other information that would be formatted and presented to users of an EHR system. Some commenters recognized this ambiguity and asked us to be more precise. But several commenters oscillated between these different constructs and imputed them to different parts of our proposal, depending on the context. As a result, some of these commenters perceived in our proposal elements that had not been proposed, such as the ability to enable a user to manually record a UDI or to exchange certain kinds of information about implantable devices.

Response. We appreciate commenters' feedback on this aspect of our proposal. We agree that a user should not be able to permanently "delete" UDIs recorded for a patient. Therefore, we are adopting the approach suggested by most commenters that would allow a user to change the status of a UDI but would require that UDI itself not be deleted and still be accessible to a user. Specifically, health IT certified to this criterion must enable a user to change the status of a UDI recorded for a patient to indicate that the UDI is inactive. We also expect that developers will implement this functionality in a manner that allows users to indicate the reason that the UDI's status was changed to inactive. Consistent with the policy that UDIs should not be deleted from the implantable device list or from a patient's electronic health record, a UDI that has been designated inactive must still be accessible to the user so that users can access information about the device, even if it was explanted or recorded in error. We expect that both the status and other appropriate metadata will be recorded in a manner consistent with the C-CDA, where applicable, and will be exchanged with the UDI according to that standard.

As noted above, the comments on this aspect of our proposal suggest the need for greater precision regarding the concept of an "implantable device list." In this final rule, we use the term "implantable device list" to refer to the visible list that is displayed to the user of health IT certified to this criterion and that must show, at a minimum: (1) a patient's active UDIs, meaning all UDIs recorded for the patient that have not been designated inactive; (2) the corresponding description of each UDI in the list (which, as discussed above, may be either the GUDID attribute "GMDN PT Name" or the "SNOMED CT® Description" mapped to that attribute); and (3) if one or more inactive UDIs are not included in the list, a method of accessing those UDIs and their associated information from within the list. The implantable device list may but need not also include the identifiers and attributes associated with each UDI that the health IT must be able to retrieve and make accessible to a user. If the implantable device list does not contain these identifiers and attributes, then the health IT would need to enable a user to access them (for example, by presenting them when a user clicks on an item in the implantable device list). Similarly, the implantable device list may but need not include inactive UDIs, so long as these UDIs are accessible from within the list. For example, the implantable device list could display only active UDIs so long as it also contained a link or other obvious way for a user to access all other UDIs recorded for the patient.

The discussion above should make clear that we are using the term "implantable device list" to refer to the UDIs and other information that must be presented and made accessible to a user in the manner described above. This information is distinct from the information not visible to a user that must be recorded and exchanged by health IT certified to this criterion. That information is not an "implantable device list" but rather a list of UDIs recorded for a patient and the associated metadata that must be recorded and exchanged in accordance with the

requirements of the CCDS definition, the 2015 Base EHR definition, and the C-CDA standard. We discuss this data separately below in response to comments regarding the exchange of contextual information about a patient's implantable devices. To avoid any ambiguity or misinterpretation, we have structured § 170.315(a)(14) to more precisely codify the concepts explained above.

Comments. In the Proposed Rule, we stated that this certification criterion would not require health IT to be able to exchange or use contextual information about a device (such as a procedure note). We requested comment on whether we had overlooked the need for or feasibility of requiring this functionality. Many of the comments we received emphasized the importance of recording and exchanging contextual information about implantable devices. Some commenters expressed concerns that exchanging UDIs without their proper context could lead to interoperability, patient safety, or other implementation challenges. Some commenters also urged us to specify precisely how contextual information associated with an implantable device should be recorded and exchanged among health IT certified to this criterion. These commenters did not identify any specific standards or implementation specifications. Several other commenters explained that current standards and implementation guides do not specify a consistent approach to documenting this information.

Response. We recognize the importance of contextual information about patients' implantable devices. As described elsewhere in this rule, we have included the Unique Device Identifier in the CCDS definition with the intent of capturing and sharing UDIs associated with implantable devices in both internal EHR records as well as exchangeable documents. We clarify that, where the UDI is present and represents an Implantable Device, the UDI should be sent in accordance with the C-CDA, which specifies its inclusion in the Procedure Activity section of

exchangeable documents. We also expected that appropriate associated metadata, such as the date and site of the implant, will be included with the UDI where available as specified in the standard.[32]

Beyond these basic parameters, we believe it is premature to prescribe the exact content and form of contextual information associated with UDIs. The comments confirm our observation in the Proposed Rule that additional standards and use cases will be needed to support this functionality.

Comments. Some commenters insisted that the proposed criterion lacked relevance to the majority of providers who do not practice in surgical or certain kinds of inpatient settings. For this reason, they suggested that we remove some or all of the criterion from the 2015 Base EHR definition or from the final rule.

Some commenters who otherwise supported our proposal felt that we should not include this certification criterion in the Base EHR or should make some of the proposed requirements optional in the 2015 Edition. Similarly, some commenters objected to the inclusion of a patient's Unique Device Identifiers in the CCDS definition. Some of these commenters objected in principle to including any requirements that are not correlated with a meaningful use objective or measure, while others objected on the basis that this certification criterion would be unduly costly and burdensome for developers and could place significant and unnecessary burdens on providers.

Several commenters claimed that this criterion was not ripe and there were a lack of available standards for certain aspects of our proposal. Commenters also cited potential

[32] The UDI for implantable devices is encoded and exchanged in the Procedure Activity Procedure (V2) section of C-CDA, which contains a Product Instance template that can accommodate the UDI the implantable device, the implant date, and the target site. Although not required by the standard, this information should be sent if available, as with all of the CCDS content.

implementation challenges, especially the fact that UDIs and other information about implantable devices are often captured in IT systems that are not part of certified health IT. Because bridging these systems will be challenging without more mature standards or customized interfaces, the information in these systems may not be recorded in certified health IT.

Response. Again, we reiterate that this criterion is not aimed at surgical specialties, settings, or systems. It is aimed at delivering information to all clinicians so that they can know what devices their patients have and use that information to deliver safer and more effective care. We take seriously the concerns raised by some commenters regarding the potential costs and burdens of the proposed criterion. We have addressed those concerns above in our responses to comments on the specific aspects of our proposal to which those concerns pertain. We note that for many of these aspects, health IT developers often contradicted one another as to the relative costs and difficulty of implementing the UDI-related capabilities we proposed. As just one illustration, several EHR developers stated that the requirement that health IT be able to parse a UDI was infeasible or would be unduly burdensome. In contradistinction, a different EHR developer objected to other aspects of the proposal but specifically endorsed the capability to parse UDIs; and yet another EHR developer supported all of the capabilities we proposed. In short, health IT developers' comments regarding cost and burden often pointed in different directions, which suggests that many of their concerns are idiosyncratic to particular developers, not generalizable to all developers or the health IT industry. We submit that competition in the marketplace is the more appropriate vehicle for mediating such differences, not our regulations.[33]

[33] In this connection we refer readers to the discussion of the new transparency and disclosure requirements for health IT developers finalized elsewhere in this rule.

Because all providers should have access to information about their patients' implantable devices, we are including a patient's Unique Device Identifiers in the CCDS definition. To ensure that all certified health IT has the basic ability to exchange, record, and make this information available, we are including this certification criterion in the 2015 Base EHR definition. These definitions are not limited to the EHR Incentive Programs and must support other programs as well as the broader needs of health IT users throughout the health care system. We refer commenters to our discussion of these definitions elsewhere in this final rule.

We decline to postpone this criterion until the Unique Device Identification System is fully implemented for all devices and across the entire medical device industry, or until additional standards are fully developed and harmonized for additional use cases. While this work is ongoing, UDIs are required to be available for all implantable devices by September 2015. Similarly, standards already exist for recording and exchanging UDIs for implantable devices as structured data in patients' electronic health records. These standards have been refined since the last time we proposed to adopt a certification criterion for implantable devices. And, as noted above, the GUDID is now available via the NLM's AccessGUDID website and will support web services for this certification criterion. While full implementation of the Unique Device Identification System will take several years, and while the development of standards is an ongoing process, UDIs for implantable devices can begin to be incorporated in health IT and will support and help accelerate these other efforts.

Commenters concerns regarding potential "upstream" implementation challenges are valid, but we have addressed those concerns by focusing this certification criterion only on the baseline functionality necessary to ensure that, once recorded in a patient's electronic health

record, UDIs can be exchanged among certified health IT and accessed by users of certified health IT wherever the patient seeks care.

- Social, Psychological, and Behavioral Data

2015 Edition Health IT Certification Criterion § 170.315(a)(15) (Social, psychological, and behavioral data)

We proposed to adopt a new 2015 Edition "social, psychological, and behavioral data" certification criterion that would require a Health IT Module to be capable of enabling a user to record, change, and access a patient's social, psychological, and behavioral data based on SNOMED CT® and LOINC® codes, including sexual orientation and gender identity and the ability to record a patient's decision not to provide information. As the Proposed Rule explained, the proposed certification criterion is designed to advance the collection and use of such patient data, to transform health delivery, to reduce health disparities, and to achieve the overarching goals of the National Quality Strategy. We proposed that social, psychological, and behavioral data be coded in accordance with, at a minimum, version 2.50 of LOINC®, and we explained that LOINC® codes will be established in a newer version of LOINC® for the question-answer sets that do not currently have a LOINC® code in place, prior to the publication of the final rule. We proposed that sexual orientation be coded in accordance with, at a minimum, the September 2014 Release of the U.S. Edition of SNOMED CT® and HL7 Version 3 that gender identity be coded in accordance with, at a minimum, the September 2014 Release of the U.S. Edition of SNOMED CT® and HL7 Version 3, as enumerated in tables in the Proposed Rule. We sought comment on inclusion of the appropriate social, psychological, and behavioral data measures, on standardized questions for collection of sexual orientation and gender identity data, on a minimum number of data measures for certification, on combining and separating the measures in certification criteria, and on inclusion of additional data and available standards.

Comments. Many commenters were in support of our proposal to include a new certification criterion for the capture of social, psychological, and behavioral data. Commenters recommended that we consider including security and privacy safeguards for this information and additional measures relevant to other settings (e.g., oral health measures, behavioral health diagnosis history, expansion of violence measures, and expansion of measure applicability to parents of pediatric patients). Commenters also recommended that we verify proposed LOINC® codes that were listed as pending in the Proposed Rule.

Some commenters were against certification for this data. These commenters cited lack of uses cases for the data, overburdening providers with data collection, and lack of maturity of data standards. A few commenters were not supportive of additional certification for criteria that are not proposed to specifically support Stage 3 of the EHR Incentive Programs.

Response. We thank commenters for their feedback. We have adopted a 2015 Edition "social, psychological, and behavioral data" certification criterion that is described in more detail below. As stated in Proposed Rule (80 FR 16826), we continue to believe that offering certification to enable a user to record, change, and access a patient's social, psychological, and behavioral data will assist a wide array of stakeholders in better understanding how this data may adversely affect health and ultimately lead to better outcomes for patients. We also believe that this data has use cases beyond the EHR Incentive Programs, including supporting the Precision Medicine Initiative[34] and delivery system reform. In addition, the Federal Health IT Strategic Plan aims to enhance routine medical care through the incorporation of more information into the health care process for care coordination and a more complete view of health, including social

[34] http://www.nih.gov/precisionmedicine/

supports and community resources.[35] We believe the collection of the information in certified Health IT Modules through this criterion can better inform links to social supports and community resources.

In regard to comments expressing privacy and security concerns, we first note that the functionality in this criterion is focused on capture and not privacy and security. Second, we have established a privacy and security certification framework for all Health IT Modules that are certified to the 2015 Edition (please see section IV.C.1 of this preamble). Third, we recommend that institutions develop and maintain policies for the collection and dissemination of this data that is consistent with applicable federal and state laws.

We appreciate comments on additional data to consider for inclusion in this criterion. We have, however, determined that the proposed list presents an appropriate first step for the standardized collection of social, behavioral, and psychological data. We note, based on feedback from commenters, we have included the capture of sexual orientation and gender identity (SO/GI) data in the 2015 Edition "demographics" certification criterion. We will continue to consider whether this list should be expanded through future rulemaking.

We have verified the LOINC® codes that were proposed and obtained the codes for those listed as pending in the Proposed Rule, and have provided the proper codes and answer list IDs for all eight domains we are adopting in this criterion (please refer to § 170.207(p)) for the full list of LOINC® codes).

Comments. There were mixed comments on whether we should adopt all proposed domains in one criterion or adopt a separate criterion for each proposed domain. We also received mixed feedback on whether certification would be to all domains, a select number, or at

[35] http://www.healthit.gov/sites/default/files/9-5-federalhealthitstratplanfinal_0.pdf

least one. Commenters in favor of one criterion with all domains stated that the proposed domains are interrelated and together provide a total health system perspective that can facilitate care management and coordination.

Response. We thank commenters and agree that these eight domains can together provide a more comprehensive picture of the patient that can facilitate care management and coordination. We also believe that there will not be a significant increase in development burden to meet all the proposed domains because there will be developmental synergies in meeting all domains using the required LOINC® code set. Accordingly, we have adopted one criterion that requires certification to all eight proposed domains (not including SO/GI).

- Transitions of Care

2015 Edition Health IT Certification Criterion § 170.315(b)(1) (Transitions of care)

We proposed to adopt a 2015 Edition certification criterion for "transitions of care" ("ToC") that is a continuation and extension of the "ToC" certification criterion adopted as part of the 2014 Edition Release 2 final rule at § 170.314(b)(8). We proposed the following revisions and additions.

Updated C-CDA Standard

We proposed to adopt C-CDA Release 2.0 at § 170.205(a)(4) and noted that compliance with the C-CDA Release 2.0 cannot include the use of the "unstructured document" document-level template for certification to this criterion. To address "bilateral asynchronous cutover," we proposed that the 2015 Edition "ToC" certification criterion reference both the C-CDA Release 1.1 and Release 2.0 standards and that a Health IT Module presented for certification to this criterion would need to demonstrate its conformance and capability to create and parse both versions (Release 1.1 and 2.0) of the C-CDA standards. While we recognized that this proposal

was not ideal, we proposed this more conservative approach as a way to mitigate the potential that there would be interoperability challenges for transitions of care as different health care providers adopted Health IT Modules certified to the 2015 Edition criterion (including CCDA Release 2.0 capabilities) at different times. We requested comment on an alternative approach related to the creation of C-CDA-formatted documents. We noted that the adoption of C-CDA Release 2.0 would be applicable to all of the other certification criteria in which the C-CDA is referenced and that, unless C-CDA Release 2.0 is explicitly indicated as the sole standard in a certification criterion, we would reference both C-CDA versions in each of these criteria.

Comments. Commenters agreed that C-CDA Release 2.0 offered improvements compared to Release 1.1 for unifying summary care record requirements and better enabling exchange of structured data between providers across disparate settings than previous versions. Commenters did not support requiring that Health IT Modules presented for certification would need to demonstrate its conformance and capability to send, receive, and parse both versions Release 1.1 and 2.0 of the C-CDA standards. Commenters stated that this proposed requirement would be too resource intensive, expressed concerns about the storage needed to store two versions of the C-CDA document, and would require systems to establish complex rules about handling content that is present in one version but not in the other. The majority of commenters instead recommended that we adopt a single version of the C-CDA standard that would ensure systems can correctly process both Releases 1.1 and 2.0, with many commenters specifically recommending Release 2.1 of C-CDA (HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use

Release 2.1, August 2015)[36] which the industry has developed, balloted, and published. Release 2.1 provides compatibility between Releases 2.0 and 1.1 by applying industry agreed-upon compatibility principles.[37] Release 2.1 also contains all the new document templates included in Release 2.0. Commenters also recommended an alternate pathway if we did not adopt Release 2.1 that would require:

- A 2015 Edition certified Health IT Module to be able to send documents conformant to C-CDA Release 2.0;
- A 2015 Edition certified Health IT Module to be able to parse both a C-CDA Release 1.1 and 2.0 document;
- A 2014 Edition certified Health IT Module to be able to parse a C-CDA Release 1.1 document, and display but not parse a document conformant to C-CDA Release 2.0.

A few commenters requested clarification on the different kinds of null values and guidance on what constitutes an "indication of none" since blank values will not meet the requirements of the corresponding measure for transitions of care for Stage 3 of the EHR Incentive Programs.

Response. We thank commenters for their suggestions to adopt Release 2.1 rather than require adherence to both versions Release 1.1 and Release 2.0. We agree that Release 2.1 largely provides compatibility with Release 1.1 while maintaining many of the improvements and new templates in Release 2.0. While we thank commenters for the alternate suggested pathway regarding 2014 Edition certified health IT, this would require a revision to the existing

---

36 http://www.hl7.org/documentcenter/public/standards/dstu/CDAR2_IG_CCDA_CLINNOTES_R1_DSTUR2.1_2015AUG.zip

37 http://wiki.hl7.org/index.php?title=Consolidated_CDA_R2.1_DSTU_Update

2014 Edition "ToC" certification criteria (§ 170.314(b)(1), § 170.314(b)(2), and § 170.314(b)(8)) that would require technology to be able to display a C-CDA document conformant with C-CDA Release 2.0. We did not propose this approach for public comment. Further, it would also be impractical and burdensome to implement as it would require forcing all health IT developers to bring back health IT certified to the 2014 Edition to update each product's certification.

We believe that adopting Release 2.1 largely achieves the goal to ensure systems can send, receive, and parse both C-CDA documents formatted according to Release 1.1 or 2.0 and minimizes the burden raised by commenters. However, we are aware that a system developed strictly to Release 2.1 might not automatically support receiving Release 1.1 C-CDAs without additional development (e.g., additional generation and import effort since different vocabulary requirements apply in several places when comparing the two versions of the C-CDA). Therefore, we have adopted C-CDA Release 2.1 (both Volumes 1 and 2) as a requirement for the 2015 Edition "ToC" criterion at § 170.314(b)(1), and have also adopted the requirement that a Health IT Module must demonstrate its ability to receive, validate, parse, display, and identify errors to C-CDA Release 1.1 documents to ensure compatibility and interoperability. Note that for consistency, all 2015 Edition certification criteria that reference C-CDA creation (e.g., clinical information reconciliation and incorporation; view, download, and transmit to 3rd party) require conformance to Release 2.1. 2015 Edition certification criteria that include a "receipt" of C-CDA documents function (e.g., clinical information reconciliation and incorporation) will also require testing to correctly process C-CDA Release 1.1 documents for the reasons described above. This pathway ensures maximum interoperability while balancing the development burden.

Regarding the questions of clarification on the use of null values and what constitutes an "indication of none" for the purposes of meeting the EHR Incentive Program Stage 3 measure, this issue concerns the information needed to fulfill the "automated numerator recording" and "automated measure calculation" functions proposed at § § 170.315(g)(1) and (g)(2), respectively. This issue concerns the draft test procedure for § § 170.315(g)(1) and (g)(2) as related to transitions of care, and we intend to update the test procedures to include guidance on how C-CDA R2.1 null values (including "indication of none") are appropriately expressed by applying guidance from the HL7 Examples Task Force.

We also highly recommend that health IT developers and providers follow the guidance provided in the HL7 Implementation Guide: S&I Framework Transitions of Care Companion Guide to Consolidated-CDA for Meaningful Use Stage 2, Release 1 – US Realm[38] that includes industry "best practices" guidance for consistent implementation of the C-CDA Release 1.1 standard, including for mapping Common MU Data Set elements into the C-CDA standard. It is our understanding that the industry is developing an update to this "companion guide" to provide guidance on implementing the C-CDA Release 2.1 standard. We encourage health IT developers to use the update to develop their products to the 2015 Edition criteria that reference C-CDA Release 2.1 when it becomes available.

C-CDA Document Template Types

We proposed to require that all certified Health IT Modules be able to parse C-CDA Release 2.0 documents formatted according to the following document templates:

- Continuity of Care Document (CCD);
- Consultation Note;

[38] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=374

- History and Physical;
- Progress Note;
- Care Plan;
- Transfer Summary;
- Referral Note; and
- Discharge Summary.

These document templates include clarifications and enhancements relative to Release 1.1, as well as new document templates (i.e., Care Plan, Referral Note, and Transfer Summary). We also proposed to prohibit the use of the unstructured document template.

Comments. Commenters were supportive of the new and clarified document templates for more specific use cases where a CCD may contain more information than is necessary. However, a number of commenters were concerned about the burden to certify all document templates, and noted that not all document templates were applicable to all settings. As such, commenters suggested we require only the CCD, Referral Note, and (for inpatient settings only) Discharge Summary and allow health IT developers to determine which additional templates would be appropriate to offer for the settings and providers intended to be served by the product. A few commenters suggested that we not prohibit the use of the unstructured document template as it could be a stepping stone to help providers begin using the C-CDA standard and can be used to provide reports with images or scanned forms.

Response. We thank commenters for the comments, and acknowledge that some of the proposed C-CDA document templates may not be applicable to all settings. Therefore, we have required that certified Health IT Modules be able to parse C-CDA Release 1.1 and C-CDA Release 2.1 CCD, Referral Note, and (for inpatient settings only) Discharge Summary document

templates for certification to this criterion. We encourage health IT developers and providers to work together to determine if additional C-CDA templates would be better suited for certain settings. For example, the CCD may contain more information than is necessary for some care transitions and other C-CDA document templates may provide a more succinct and/or targeted summary of a patient's clinical information for certain settings. We note that C-CDA Release 2.1 includes the same document templates included in Release 2.0.

Regarding the use of the unstructured document template, we believe that it limits interoperability as data is not exchanged in a structured and standardized (e.g., to certain vocabulary standards) manner. For the purposes of certification to this certification criterion, Health IT Modules cannot include the use of the unstructured document template.

Valid/Invalid C-CDA System Performance and Display

We proposed that Health IT Modules would need to demonstrate the ability to detect valid and invalid C-CDA documents, including document, section, and entry level templates for data elements specified in 2014 and 2015 Editions. Specifically, that this would include the ability to detect invalid C-CDA documents, to identify valid C-CDA document templates, to detect invalid vocabularies and codes not specified in either the C-CDA 1.1 or 2.0 standards or required by this regulation, and to correctly interpret empty sections and nullFlavor combinations per the C-CDA 1.1 or 2.0 standards. Last, we proposed that technology must be able to display in human readable format the data included in a transition of care/referral summary document. We explained that we expected that Health IT Modules to have some mechanism to track errors encountered when assessing received C-CDA documents and we proposed that health IT be able to track the errors encountered and allow for a user to be notified of errors or review the errors produced. We stated these functionalities are an important and necessary technical prerequisite in

order to ensure that as data in the system is parsed from a C-CDA for incorporation as part of the "clinical information reconciliation and incorporation" certification criterion the user can be assured that the system has appropriately interpreted the C-CDA it received.

Comments. There was overall support from commenters on the proposal to require Health IT Modules detect valid and invalid C-CDA documents. However, similar to the comments above, commenters did not support the proposal to require validation of both C-CDA Releases 1.1 and 2.0 because of the burden and complexity of processing two versions of the same standard. A few commenters were concerned with the proposed requirement for the receiving system to manage an incorrectly formatted C-CDA document, and requested that this burden should be on the sending system. A few commenters also requested clarification on whether the receiver is required to notify the sender of the C-CDA document of errors. Commenters also requested clarification on how validation and display would be tested as it would be unrealistic for health IT to accept every single code in a system. Last, some commenters were concerned about the "alert fatigue" a user could encounter if notified of every C-CDA error detected by the certified system.

Response. We thank commenters for their support of the proposal. As noted above, systems would be required to support validation and display for both Releases 1.1 and Release 2.1 to ensure compatibility and interoperability. We reiterate as noted above that systems will be tested to perform the validation and display functions for only the CCD, Referral Note, and (inpatient settings only) Discharge Summary templates.

Regarding the burden to the receiving system to process incorrectly formatted C-CDA errors, we note that all Health IT Modules certified to a 2015 Edition criterion that includes the functionality to create a C-CDA are also required to be certified to the "C-CDA Creation

Performance" certification criterion at § 170.315(g)(6). This certification criterion requires that systems are able to create C-CDA documents in accordance with a gold standard that we provide, thereby reducing the potential for errors in a C-CDA sent by an outgoing system (please refer to the "C-CDA creation performance" criterion in the preamble for further details).

However, we recognize that there may still be errors in created C-CDA documents from a sending system and therefore continue to believe in the value of the receiving system to process and validate C-CDA documents, including notifying the user of errors. We clarify that the error notification should be available to the receiving user. Regarding error notification, systems would be required to demonstrate its ability to notify the user of errors or allow the user to review the errors for the purposes of certification. Per commenters' concerns about "alert fatigue," we note there is no explicit requirement that the user be interrupted regarding the availability of errors. Rather, that the user needed to be able to access such errors. We anticipate that validation and display would be tested through visual inspection that test data in the form of C-CDA documents with and without errors can be correctly parsed and errors correctly identified.

We have finalized the requirement as part of this criterion that Health IT Modules must be able to detect valid and invalid transition of care/referral summaries received and formatted in accordance with C-CDA Release 1.1 and Release 2.1 for the CCD, Referral Note, and (inpatient settings only) Discharge Summary document templates, including detection of invalid vocabulary standards and codes, correct interpretation of empty sections and null combinations, recording of errors/notification of errors to the user, and the ability to display a human readable formatted C-CDA (for both Releases 1.1 and 2.1). We discuss additional clarifications regarding the display of C-CDA sections below.

Clinical Relevance of Summary Care Record Information

We have received feedback from providers expressing difficulty finding or locating the pertinent and relevant clinical information on a patient from a transition of care/referral summary received as a C-CDA document. Commenters have indicated that data included in a transition of care/referral summary document may be rendered and displayed as a long, multi-page document, which makes it challenging for a provider to quickly find the clinical information they seek to make a care decision.

We note that CMS has finalized in the EHR Incentive Programs Stage 3 and Modifications final rule guidance that permits a provider and organization (i.e., the "sender") to define the "clinical relevance" of information sent in a summary care record depending on the circumstances, as best fits the organizational needs, and as relevant for the patient population.[39] CMS notes, however, that the sending provider has to have the ability to send all clinical notes or laboratory results in a summary care document if that level of detail is requested by the receiving provider.

While the guidance in the EHR Incentive Programs Stage 3 and Modifications final rule does address "clinical relevance" from the sending side and could result in a reduction in the quantity of data potentially viewed by a recipient as "unnecessary" or not useful, we recognize that certain patients, such as those with complex and/or chronic conditions may have a transition of care/referral summary sent to receiving providers with large quantities of data included. In that respect, we included as part of the 2014 Edition Final Rule a specific "section views" capability in the "transitions of care" certification criterion (adopted at 45 CFR 170.314(b)(1)(iii)(C)), which we described as having been added to the certification criterion in

[39] Please see the EHR Incentive Programs Stage 3 and Modifications final rule published elsewhere in this issue of the **Federal Register.**

order to make sure that health IT would be able to extract and allow for individual display each additional section or sections (and the accompanying document header information (i.e., metadata)) that were included in a transition of care/referral summary received and formatted in accordance with the Consolidated CDA (77 FR 54219).

We indicated that this functionality would be useful in situations when a user wanted to be able to review other sections of the transition of care/referral summary that were not incorporated (as required by this certification criterion at 45 CFR 170.314(b)(1)), such as a patient's procedures and smoking status, and that the technology would need to provide the user with a mechanism to select and just view those sections without having to navigate through what could be a lengthy document.

The section views capability remains as part of the 2015 Edition version of this criterion. Additionally, to address comments that raised concerns and requested that we act to address a C-CDA's "length" and users' ability to more easily navigate to particular data within the C-CDA, we have included more precise requirements in this portion of the certification criterion. Specifically, the 2015 Edition version includes that a user must be able to: 1) directly display only the data within a particular section, 2) set a preference for the display order of specific sections, and 3) set the initial quantity of sections to be displayed. We also clarify that the sole use of the CDA.xsl style sheet provided by HL7 to illustrate how to generate an HTML document from a CDA document will not be acceptable to meet these requirements. We believe these clarifications will help address stakeholder concerns regarding the difficulty finding or locating the pertinent and relevant clinical information on a patient from a ToC/referral summary received as a C-CDA document. We intend to ensure that the test procedure for this criterion thoroughly tests these aspects consistent with the certification criterion's requirements. We also

strongly urge the health IT industry to dedicate additional focus toward improving the rendering of data when it is received. Putting such data to use in ways that enable providers to quickly view and locate the information they deem necessary can help improve patient care and prevent important information from being inadvertently missed. We further note that standards experts are aware of the stakeholder concerns discussed above, and that the HL7 Structured Documents Work Group is working on contributing positive momentum to this issue.[40] The HL7 Structured Documents Work Group's work involves developing guidance on the "relevant" data that should be sent by the sender. We encourage health IT developers to participate in this process and implement the industry principles arising out of this project.

Edge Protocols

We proposed to "carry-over" a requirement from the 2014 Edition Release 2 "transitions of care" criterion at § 170.314(b)(8) that would require a certified Health IT Module be able to send and receive transition of care/referral summaries through a method that conforms to the ONC Implementation Guide for Direct Edge Protocols, Version 1.1 at § 170.202(d).

Comments. Commenters were generally in support of requiring one of the four Edge Protocols designated in the ONC IG for Direct Edge Protocols. One commenter was concerned that the edge protocols offer no additional value for those that have already implemented Direct.

Response. As stated in the 2014 Edition Release 2 final rule, we believe that adoption of the ONC IG for Direct Edge Protocols can improve the market availability of electronic health information exchange services for transitions of care by separating content from transport related to transitions of care. We believe that certification to the Direct Edge Protocols IG can also enable greater certainty and assurance to health IT developers that products certified to this IG

[40] http://www.hl7.org/special/Committees/projman/searchableProjectIndex.cfm?action=edit&ProjectNumber=1183

have implemented the IG's edge protocols in a consistent manner (79 FR 54437). As such, we have finalized the requirement that a certified Health IT Module be able to send and receive transition of care/referral summaries through a method that conforms to the ONC Implementation Guide for Direct Edge Protocols, Version 1.1.

We note that we inadvertently left out a provision of the proposed regulation text related to Edge Protocol requirements. As noted above and in the Proposed Rule, we intended to "carry over" the Edge Protocol requirements included in § 170.314(b)(8) for this criterion. Therefore, we have added to the provision in § 170.315(b)(1)(i)(A) about sending transition of care/referral summaries through a method that conforms with the Edge Protocol and a requirement that it must also lead to the summaries being processed by a service that has implemented Direct. This addition parallels the Direct Edge Protocol "receiving" requirements we proposed and have finalized. It also clarifies a consistent set of technical capabilities for sending the Edge Protocol and technologies interacting with services that have implemented Direct, which again are the exact same requirements included in § 170.314 (b)(8) that we intended to duplicate in this 2015 Edition criterion.

<u>XDM Package Processing</u>

We proposed to include a specific capability in this certification criterion that would require a Health IT Module presented for certification that is also being certified to the SMTP-based edge to demonstrate its ability to accept and process an XDM package it receives, which would include extracting relevant metadata and document(s). We explained that this additional requirement only applies to a Health IT Module presented for certification with an SMTP-based edge implementation and not an XDR edge implementation. Because we expect XDM packaging to be created in accordance with the specifications included in IHE IT Infrastructure Technical

Framework Volume 2b, Transactions Part B – Sections 3.29 – 2.43, Revision 7.0, August 10, 2010 (ITI TF-2b),[41] we proposed to adopt this as the standard at § 170.205(p)(1) for assessing whether the XDM package was successfully processed.

Comments. Commenters were supportive of the proposal to demonstrate XDM package processing. Many commenters recommended that processing on receipt depends on metadata in the XDM package that should be aligned with the general metadata in Appendix B of the IHE Data Access Framework Document Metadata Based Access Implementation Guide that was published for public comment on June 1, 2015.[42] One commenter recommended that the certification criterion point specifically to section 3.32.4.1.4 of ITI TF-2b.

Response. We thank commenters for their support of the proposal and have finalized this requirement that Health IT Modules certified to an SMTP-based edge protocol be able to receive and make available the contents of an XDM package formatted in accordance with ITI TF-2b, which we have adopted at § 170.205(p)(1). We note that the ONC Implementation Guide for Direct Edge Protocols adopted at § 170.202(d) and required for this criterion as discussed above references the guidance in the ONC XDR and XDM for Direct Messaging Specification for proper use of metadata that is aligned with the IHE Data Access Framework Document Metadata Based Access IG. Therefore, we do not believe it is necessary to reference the IHE IG as these metadata requirements are already referenced and required for this criterion. Similarly, our requirement to adhere to the ITI TF-2b would include any specific section required in the standard, and thus we do not need to reference a specific section.

---

[41] http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Rev7-0_Vol2b_FT_2010-08-10.pdf
[42] http://ihe.net/uploadedFiles/Documents/PCC/IHE_PCC_IG_DAF_National%20Extension_Rev1.0_PC_2015-06-01.pdf

SMTP-based transport systems use standard Multi-Purpose Internet Mail Extension (MIME) to identify email attachments and to enable receiving computer systems to process attachments seamlessly. For example, a MIME type of "text/html" identifies text styled in HTML format. C-CDA documents are commonly identified using "text/xml" and "application/xml" MIME types. In addition, XDM packages are commonly identified with "application/zip" and "application/octet-stream" MIME types. However, these MIME types have not been standardized by the community for transporting C-CDA and XDM files. Systems could potentially use other valid MIME types to send the documents. While these standard MIME types provide sufficient information for receiving systems to render content, they do not provide a way to distinguish the C-CDA and XDM documents from all the other documents that could be sent using the same MIME types. Until an appropriate set of MIME types are developed that can uniquely identify C-CDA and XDM, there is widespread acknowledgement that the receiving systems should accept all common MIME types, and use the information within the actual documents, to process C-CDA and XDM accordingly. Hence, in order to facilitate interoperability, we expect Health IT Modules to be able to support all commonly used MIME types when receiving C-CDA and XDM packages. We intend to update the test procedure to include guidance on specific MIME types that we expect Health IT Modules to support, at a minimum.

Common Clinical Data Set

We proposed to require Health IT Modules to enable a user to create a transition of care/referral summary that includes, at a minimum, the Common Clinical Data Set for the 2015 Edition that includes references to new and updated vocabulary standards code sets.

Comments. Commenters were supportive of this proposal overall. A few commenters were concerned about specific data elements in the proposed 2015 Edition Common Clinical Data Set definition.

Response. We thank commenters for their support and have adopted the requirement that Health IT Modules enable a user to create a transition of care/referral summary that includes the 2015 Edition Common Clinical Data Set at a minimum. We address the specific data elements in the 2015 Edition Common Clinical Data Set definition in under section III.B.3 of this final rule.

Encounter Diagnoses

We proposed to continue the requirement from the 2014 Edition "ToC" certification criterion that a Health IT Module must enable a user to create a transition of care/referral summary that also includes encounter diagnoses using either SNOMED CT® (September 2014 Release of the U.S. Edition as a baseline for the 2015 Edition) or ICD-10-CM codes.

Comments. One commenter recommended solely the use of ICD-10-CM for encounter diagnoses and certification. Another commenter requested clarification on whether the encounter diagnoses are meant to be "billing diagnoses" and whether the health IT would need to include all billing diagnoses for encounters or just the primary encounter, and how primary would be determined.

Response. As stated in our 2014 Edition final rule (77 FR 54178 and 54220), we believe that SNOMED CT® is the more appropriate vocabulary for clinical purposes and provides greater clinical accuracy. However, it may be beneficial for inpatient Health IT Modules to be certified to and support the use of ICD-10-CM to represent diagnoses, and finalized the 2014 Edition "transitions of care – create and transmit" criterion at § 170.314(b)(1) to allow for either ICD-10-CM or SNOMED CT®. We continue this policy and have finalized the requirement for

this 2015 Edition "ToC" certification criterion that a Health IT Module enable a user to create a transition of care/referral summary that includes encounter diagnoses using either SNOMED CT® (September 2015 Release of the U.S. Edition as a baseline for the 2015 Edition[43]) or ICD-10-CM codes.

We note that our certification requirement does not dictate what encounter diagnoses providers would include in a transitions of care document, only that certified Health IT Modules can enable a provider to include encounter diagnoses using SNOMED CT® or ICD-10-CM.

"Create" and Patient Matching Data Quality

As a part of the "Create" portion of the "ToC" criterion in the 2015 Edition, we proposed to require a Health IT Module to be able to create a transition of care/referral summary that included a limited set of standardized data in order to improve the quality of the data that could potential be used for patient matching by a receiving system. The proposed standardized data included: first name, last name, maiden name, middle name (including middle initial), suffix, date of birth, place of birth, current address, historical address, phone number, and sex, with constrained specifications for some of the proposed standardized data.

Comments. There was general support for requiring the proposed data elements to be exchanged in order to improve patient matching. Some commenters were concerned with conflicts between the proposed approach and existing systems' algorithms and patient matching protocols. A few commenters recommended that we wait until there is a consensus-based patient matching standard before adopting requirements for certification. A few commenters also noted that the proposal does not address data quality.

[43] We refer readers to section III.A.2.c ("Minimum Standards" Code Sets) for further discussion of our adoption of SNOMED CT® as a minimum standards code set and our decision to adopt this version.

Response. We note that systems can continue to use their existing algorithms and patient matching protocols and that our proposed approach was not intended to conflict with any existing practice. We reiterate that the proposed data elements stem from the HITPC's and HITSC's recommendations and findings from the 2013 ONC initiative on patient matching as described in the Proposed Rule (80 FR 16833-16834). We continue to believe these recommendations represent a first step forward that is consensus-based. We agree that the proposal did not address data quality in the sense that it would improve the "source's" practices and procedures to collect highly accurate and precise data. However, we believe that including standards for the exchange of certain data elements could improve interoperability and provides an overall level of consistency around how the data are represented. We encourage ongoing stakeholder efforts focused on improving patient matching through better data quality processes and will continue to monitor and participate in these activities.

Comments. Commenters recommended that we ensure alignment between the proposed data elements and corresponding standards with those in the C-CDA standard.

Response. We have performed an analysis of the proposed data elements and standards with those in C-CDA Release 2.1 and have made some revisions as described below. In some cases, the ONC method may be more constrained than what is in C-CDA Release 2.1 and we believe there will be no conflict. Rather the additional constraint is intended to promote patient matching and interoperability. We also address standards for specific elements below.

Comments. Commenters suggested that we should not reference the CAQH Phase II Core 258: Eligibility and Benefits 270/271 Normalizing Patient Last Name Rule version 2.1.0 for suffix as it puts JR, SR, I, II, III, IV, and V in the same field as RN, MD, PHD, and ESQ. Commenters felt that these suffixes should be kept separate as it could be confusing if a patient

has more than one suffix (e.g., JR and MD). Individuals may also not use both suffixes in all circumstances, so it may be difficult to match records using both.

Response. We agree with the comments and have not adopted the constraint for suffix to adhere to the CAQH standard. We recommend that health IT developers and providers follow the guidance for suffix in C-CDA Release 2.1 for exchange, which allows for an additional qualifier for any suffix provided with the last name field.

Comments. One commenter noted that the CAQH Phase II Core 258: Eligibility and Benefits 270/271 Normalizing Patient Last Name Rule version 2.1.0 is intended for normalization of information upon receipt rather than at the point of sending. Pre-normalization can lead to data loss and detract from patient matching. Therefore the commenter recommended ONC not require the CAQH Phase II Core 258: Eligibility and Benefits 270/271 Normalizing Patient Last Name Rule version 2.1.0 for normalizing last name in the sending of transition of care/referral summary documents and rather point to it as guidance for receiving systems.

Response. We agree with the commenter, and have not adopted the constraint for last name normalization in accordance with the CAQH standard. We recommend that health IT developers and providers follow the guidance for last name in C-CDA Release 2.1 for exchange of transition of care/referral summary documents.

Comments. A few commenters suggested that the concept of "maiden name" is not used in all cultures and is also gender-specific. Some commenters noted that some nationalities, cultures, or ethnic groups do not use this term and, in other cases, an individual may adopt more than one family name during marriage. There are other cases where the last name or family name has been legally changed for other situations. Most commenters recommended we instead use

another term that broadly captures these situations and allows for aliases that a patient may use in these circumstances.

Response. We thank commenters for the feedback and have revised "maiden name" to "previous name" to accommodate for any other aliases including the situations described above by the commenters. We note that the C-CDA Release 2.1 contains a field for "birth name" that can accommodate this information.

Comments. A number of commenters were concerned about including place of birth in the list of data elements as there is a lack of standards on representing the place of birth. Some systems include city, county, state, and country, while other systems may only include some of these elements. Therefore, these commenters stated that it would be difficult to standardize on place of birth as proposed and it would offer no additional value for improving patient matching.

Response. We agree with commenters that the lack of standards for representing place of birth would not improve patient matching at this time and, therefore, have not finalized this data element requirement.

Comments. A few commenters noted concerns about including the hour, minute, and second of the date of birth, and suggested that the time zone is needed to correctly match records.

Response. We note that as proposed in the 2015 Edition, the hour, minute, and second of the date of birth were optional or conditional fields based on whether they were included. Since we have not finalized the proposed requirement to include place of birth, we have revised the requirement as follows. We clarify that for the purposes of certification that the hour, minute, and second for a date of birth are optional for certification. If a product is presented for certification to this optional provision, the technology must demonstrate that the correct time zone offset is included.

Comments. One commenter supported the proposal to include phone number in the list of patient match elements. Another commenter recommended we specify a standard for representing phone number.

Response. We clarify that we proposed that the phone number must be represented in the ITU format specified in the International Telecommunication Union (ITU)'s ITU-T E.123[44] and ITU-T E.164 standards.[45] These are the best available industry standards for representing phone number and we have adopted them for representing phone number in this certification criterion.

Comments. As stated above, commenters suggested we perform an analysis of the standards required by the C-CDA standard and resolve any inconsistencies with our proposal.

Response. In our analysis of the proposed data elements with the C-CDA Release 2.1 standard as suggested by commenters, we found that the C-CDA Release 2.1 standard is not able to distinguish between historical and current address as proposed. Because of the discrepancy between our proposal and what the C-CDA Release 2.1 can accommodate, we have revised the requirement to "address" (not specified as historical or current). We note that C-CDA Release 2.1 can accommodate more than one address. It is our understanding that the underlying parent C-CDA standard (i.e., CDA) included the ability to send a useable period with the address to specify different addresses for different times of the year or to refer to historical addresses. However, this useable period was removed from C-CDA as it did not have enough use. We intend to work with stakeholders going forward in assessing whether the useable period should be included in future versions of the C-CDA standard or whether there are other methods for distinguishing historical or current address for consideration in future rulemaking.

---

[44] http://www.itu.int/rec/T-REC-E.123-200102-I/e
[45] http://www.itu.int/rec/T-REC-E.164-201011-I/en

Comments. A number of commenters recommended ONC adopt the US Postal Service (USPS) standard for representing address. Commenters noted that the standard is widely supported by health care organizations today, and that it is recommended by the American Health Information Management Association.[46] Another commenter recommended we consider adoption of the GS1 Global Location Number standard.

Response. We thank commenters for the input. At this point in time and since this patient matching requirement focuses on the use and representation of address in the C-CDA standard, we believe that use of the C-CDA standard's built-in requirements is the best, most incremental path forward. We note the C-CDA Release 2.1 standard references the HL7 postal format. Additionally, testing and validation to the HL7 postal format in the C-CDA standard is already available as part of 2014 Edition "transitions of care" testing to C-CDA Release 1.1. We see a need for continued industry work to determine the appropriateness of existing standards and tools for normalizing postal address for health care use cases such as matching of electronic patient health records, and intend to work with stakeholders in this space. Thus, we look forward to continuing to work with stakeholders to analyze the USPS address standard[47] and other industry standards with respect to any future updates to the C-CDA to bring about industry-wide consistency. We anticipate the C-CDA validation tool for 2015 Edition "transitions of care" testing will carry over the 2014 Edition testing and suggest that health IT developers and implementers adhere to the guidance in C-CDA Release 2.1 on the use of the HL7 postal format.

Comments. A few commenters suggested we consider the addition of data elements to the proposed list, such as a social security number or the last four digits of a social security number.

---

[46] http://perspectives.ahima.org/wp-content/uploads/2014/12/PatientMatchingAppendixA.pdf
[47] http://pe.usps.gov/cpim/ftp/pubs/Pub28/pub28.pdf

Response. We thank commenters for the suggestions but do not agree and have not accepted these suggestions. We have evaluated the list proposed in the Proposed Rule[48] and continue to believe that it represents a good first step toward improving patient matching in line with the HITSC, HITPC, and ONC 2013 patient matching initiative recommendations. We intend to continue our work in developing patient matching best practices and standards, including evaluating the feasibility, efficacy, and, in some cases, the legality of specifying other data elements for patient matching. We may propose to expand this list or adopt a more sophisticated patient match policy in future rulemaking as standards mature.

Comments. A few commenters noted that a 100% patient match is impossible to achieve in every instance.

Response. We note that our proposal only concerns the ability of a certified Health IT Module to create a transition of care/referral summary document that contains the proposed data elements in accordance with the specified standards/constraints. The proposal would not require a system to demonstrate how it performs patient matching with these data for certification. As noted above, we believe the algorithms and patient matching protocols are best left to health IT systems and providers to determine at this point in time. While the HITPC recommended[49] that we should develop, promote, and disseminate best practices, there is not an industry-wide standard for patient matching protocols that is ready to require as a condition of certification. We intend to continue working with the industry to develop these best practices, and will evaluate at a later point if certification would confer additional benefit for improving patient matching. Until

[48] First name, last name, maiden name, middle name (including middle initial), suffix, date of birth, place of birth, current address, historical address, phone number, and sex, with constrained specifications for some of the proposed standardized data.

[49] http://www.healthit.gov/FACAS/sites/default/files/standards-certification/8_17_2011Transmittal_HITSC_Patient_Matching.pdf

such protocols are established and mature, our requirement addresses the HITPC's first recommendation, which is to provide standardized formats for demographic data fields.

In consideration of public comments, we have finalized the requirement that Health IT Modules must be able of creating a transition of care/referral summary in accordance with just C-CDA Release 2.1 as part of this certification criterion that includes the following data formatted to the associated standards/constraints where applicable:

- First name;
- Last name;
- Previous name;
- Middle name (including middle initial);
- Suffix;
- Date of birth – The year, month, and day of birth are required fields. Hour, minute, and second are optional fields; however, if hour, minute, and second are provided then the time zone offset must be included. If date of birth is unknown, the field should be marked as null;
- Address;
- Phone number – Represent phone number (home, business, cell) in the ITU format specified in ITU-T E.123[50] and ITU-T E.164[51] which we are adopting at § 170.207(q)(1). If multiple phone numbers are present, all should be included; and
- Sex in accordance with the standard we are adopting at § 170.207(n)(1).

[50] http://www.itu.int/rec/T-REC-E.123-200102-I/e
[51] http://www.itu.int/rec/T-REC-E.164-201011-I/en

We note that we corrected the date of birth requirements to specify the year, month, and day of birth as the required fields. We previously inadvertently listed "date" instead of "day."

Direct Best Practices

Given feedback from stakeholders regarding health IT developers limiting the transmission or receipt of different file types via Direct, we reminded all stakeholders in the Proposed Rule of the following best practices for the sharing of information and enabling the broadest participation in information exchange with Direct: http://wiki.directproject.org/Best+Practices+for+Content+and+Workflow. We did not include a proposal or request for comment related to this guidance.

Comments. One commenter recommended we review the challenges and solutions recommended by the DirectTrust in Chapter 2, Chapter 7 and Chapter 8 of the white paper, "A Report on Direct Trust Interoperability Testing and Recommendations to Improve Direct Exchange.[52]

Response. As we did not include a proposal or request for comment, we thank the commenter for the recommendation and will review the recommended material.

Certification Criterion for C-CDA and Common Clinical Data Set Certification

We noted that no proposed 2015 Edition certification criterion includes just the C-CDA Release 2.0 and/or the Common Clinical Data Set, particularly with the 2015 Edition not including a proposed "clinical summary" certification criterion as discussed in the 2015 Edition Proposed Rule (80 FR 16850). We requested comment on whether we should adopt a separate 2015 Edition certification criterion for the voluntary testing and certification of health IT to the

---

52 http://static1.1.sqspcdn.com/static/f/1340919/26054983/1426686689687/Report+on+DirectTrust+Interoperability+Testing.pdf?token=A0DNBiAqjJ2YzuhUTn4vnBMrtVI%3D

capability to create a summary record formatted to the C-CDA Release 2.0 with or without the ability to meet the requirements of the Common Clinical Data Set definition.

Comments. We received comments in favor of adopting a new 2015 Edition criterion that includes just the ability of a Health IT Module to enable a user to create a transition of care/summary care record in accordance with C-CDA Release 2.0 and with the ability to meet the requirements of the Common Clinical Data Set.

Response. We have adopted two new 2015 Edition certification criteria (with no relation to the EHR Incentive Programs) that include just the ability of a Health IT Module to enable a user to create (one criterion) and receive (one criterion) a transition of care/referral summary in accordance with C-CDA Release 2.1 (create) and both C-CDA Releases 1.1 and 2.1 (receive) and with the ability to meet the requirements of the Common Clinical Data Set at § 170.315(b)(4) and § 170.315(b)(5), respectively. For the certification criterion adopted to "create" a transition of care/referral summary at § 170.315(b)(4), we have also, for consistency, include the same patient matching data as referenced by the "ToC" certification criterion. We refer readers to the "Common Clinical Data Set summary record – create" and "Common Clinical Data Set summary record – receive" certification criteria in this section of the preamble for a more detailed description of the rationale and specific requirements of the new certification criteria.

C-CDA Data Provenance Request for Comment

We requested comment on the maturity and appropriateness of the HL7 IG for CDA Release 2: Data Provenance, Release 1 (US Realm) (DSTU)[53] for the tagging of health information with provenance metadata in connection with the C-CDA, as well as the usefulness

[53] http://wiki.hl7.org/index.php?title=HL7_Data_Provenance_Project_Space and http://gforge.hl7.org/gf/project/cbcc/frs/?action=FrsReleaseBrowse&frs_package_id=240

of this IG in connection with certification criteria, such as "ToC" and "VDT" certification criteria.

Comments. Although commenters were supportive of the usefulness of data provenance, the majority of commenters did not think the HL7 Data Provenance standard was mature for adoption at this point in time.

Response. We thank commenters for their input and will continue to monitor the industry uptake and maturity of the HL7 Data Provenance standard in consideration of future rulemaking.

- Clinical Information Reconciliation and Incorporation

2015 Edition Health IT Certification Criterion § 170.315(b)(2) (Clinical information reconciliation and incorporation)

We proposed to adopt a 2015 Edition "clinical information reconciliation and incorporation" certification criterion that is a revised (but largely similar to the 2014 Edition Release 2) version of the "clinical information reconciliation and incorporation" criterion adopted at § 170.314(b)(9). First, we proposed that Health IT Modules must be able to incorporate and reconcile information upon receipt of C-CDA's formatted to both Release 1.1 and Release 2.0 for similar reasons (e.g., for compatibility with Release 1.1) as proposed for the "ToC" criterion described above.

Comments. Commenters were generally supportive of the proposal to adopt a criterion for "clinical information reconciliation and incorporation" for interoperability.

Response. We thank commenters for their support and have adopted a 2015 Edition criterion for "clinical information reconciliation and incorporation" with the following changes and clarifications as discussed below.

Comments. Similar to the comments we received for the "ToC" criterion, commenters were not in favor of the proposed requirement to support both versions of C-CDA Release 1.1 and 2.0 because of the burden to receive and process two versions of the same standard.

Response. As discussed in the preamble of the "ToC" criterion above, we have adopted a requirement that systems must be able to receive and correctly process documents formatted to both C-CDA Releases 1.1 and 2.1. While C-CDA Release 2.1 largely addresses compatibility issues with Release 1.1 and reduces the burden for systems receiving both versions, we are aware that a system developed strictly to Release 2.1 might not automatically support receiving Release 1.1 C-CDAs without additional development. Therefore, this criterion will focus on functionalities to receive, incorporate, and reconcile information from a C-CDA formatted to Releases 1.1 and 2.1.

C-CDA Document Templates and Reconciliation

We proposed that a certified Health IT Module be able to receive, reconcile, and incorporate information from the C-CDA Release 2.0 CCD, Discharge Summary, and Referral Note document templates at a minimum. Note that we incorrectly referenced the "Referral Summary" document template. There is no "Referral Summary" document template and we intended the "Referral Note" document template.

Comments. We did not receive specific comments regarding the C-CDA document templates proposed for this criterion.

Response. Although we did not receive comments regarding the C-CDA document templates for this certification criterion, we maintain the consistency decision discussed in the "ToC" criterion to require incorporation and reconciliation of information from the C-CDA Releases 1.1 and 2.1 CCD, Referral Note, and (for inpatient settings only) Discharge Summary

document templates. We believe this will provide consistency between the minimum certification requirements for systems creating and sending C-CDA documents for transitions of care and this criterion for the receipt, incorporation, and reconciliation of C-CDA information.

Data for Reconciliation

We proposed that a Health IT Module must be able to reconcile and incorporate, at a minimum: problems, medications, and medication allergies from multiple C-CDAs, with testing for this specific system performance to verify the ability to incorporate valid C-CDAs with variations of data elements to be reconciled (e.g., documents with no medications, documents having variations of medication timing data). We also proposed that problems be incorporated in accordance with the September 2014 Release of the U.S. Edition of SNOMED CT® and that medications and medication allergies be incorporated in accordance with the February 2, 2015 monthly version of RxNorm as a baseline and in accordance with our "minimum standards code sets" policy.

Comments. A few commenters suggested we include additional data for incorporation and reconciliation, such as food allergies and intolerances, labs, and immunizations.

Response. As stated in the 2014 Edition final rule, we continue to believe that problems, medications, and medication allergies are the minimum data that should be reconciled and incorporated from a C-CDA (77 FR 54223). We note that this minimum requirement for certification would not prohibit health IT developers from including functionality to reconcile and incorporate a broader set of information from a C-CDA, which is something we encourage developers to pursue.

Comments. One commenter suggested that a provider may use different functionality for the reconciliation of medications distinct from the medication allergies and/or problems, and

recommended that that certification criterion should allow for distinct or combined reconciliation approaches.

Response. We clarify that the certification criterion would allow for distinct (individual) or combined reconciliation functions for medications, medication allergies, and problems to be implemented so long as all the functions can be demonstrated.

Comments. Commenters were supportive of testing for this criterion to verify a Health IT Module's ability to incorporate valid C-CDAs with variations in the data elements to be reconciled. Commenters believed this would reasonably test the real-world variation that may be found in C-CDA documents.

Response. We thank commenters for their support and intend for testing to verify a certified Health IT Module's ability to incorporate valid C-CDAs with variations in the data elements.

C-CDA Creation for Validation of Accurate Reconciliation

We proposed to require that a C-CDA be created based on the reconciliation and incorporation process in order to validate the incorporation results. We expected that the generated C-CDA would be verified using test tools for conformance and can be checked against the information that was provided to incorporate.

Comments. We received mixed feedback on this proposal. Some commenters were concerned that this requirement would not provide added benefit for Health IT Module users or patients. Other commenters noted that this requirement would be adding in a "create" function to this criterion, which they thought contradicted the modularity we previously introduced in the 2014 Edition Release 2 final rule when we made modifications to the 2014 Edition "transitions of care" and "clinical information reconciliation" criteria.

Response. We believe that the creation of a C-CDA based on the reconciliation and incorporation process will improve and automate the testing and verification process. While there are other methods of verifying reconciliation, such as queries and list displays, an automated verification through the use of test tools provides the most assurance that the information was reconciled and incorporated correctly. We do not believe this requirement will add unnecessary burden as it is our understanding that systems that receive, incorporate, and reconcile C-CDA information can also create a C-CDA. Furthermore, the purpose of this additional portion of the certification criterion is to increase provider assurance that the incorporation performed by a system post-reconciliation is accurate and complete.

With respect to the comments that mentioned an apparent contradiction with the requirement for "creating" a C-CDA as part of this certification criterion, we disagree, and remind commenters that the changes we made in the 2014 Edition Release 2 final rule were to better position the "incorporation" functionality in the right certification criterion (79 FR 54438-54439). Therefore, we have adopted the requirement that Health IT Modules be able to create a C-CDA Release 2.1 based on the reconciliation and incorporation process that will be verified during testing and certification. Note that this requirement applies to the ability to create a C-CDA formatted to the C-CDA Release 2.1 CCD document template only.

Comments. One commenter asked for clarification on whether the proposed regulation text "technology must be able to demonstrate that the transition of care/referral summary received is or can be properly matched to the correct patient" means that Health IT Modules must be able to auto-match to the correct patient. Commenters noted that many systems allow for manual match, and that an auto-match may not be the most appropriate method to match patient records.

Response. We clarify that it was not our intention to prescribe how patient match is performed for this criterion. We have revised the regulation text to reflect that the technology must demonstrate that the received transition of care/referral summary document can be properly matched to the correct patient. We leave the flexibility to the health IT developer and provider to determine the best method for patient match.

Comments. A few commenters were concerned with the proposed requirement that for each list type (i.e., medications, medication allergies, or problems) the Health IT Module must simultaneously display the data from at least two sources. Commenters noted that there would not be two sources if the patient is new to the receiving system.

Response. We reiterate that for the purposes of testing and certification, Health IT Modules must demonstrate the ability to simultaneously display the data from at least two sources. While the commenters' point is fair it is not within scope for the purposes of testing and certification, which focuses on when there is data to reconcile. In other words, the purpose of this certification criterion is, in part, to assess technology's capability to reconcile data from two sources. Testing and certification is focused on ensuring that that functionality exists and performs correctly. Additionally, the criterion does not address the totality of capabilities that may be present in the technology. In cases where a new patient presents this specific functionality may not be applicable or used at all.

- Electronic Prescribing

2015 Edition Health IT Certification Criterion § 170.315(b)(3) (Electronic prescribing)

We proposed to adopt a 2015 Edition certification criterion for e-prescribing that is revised in comparison to the 2014 Edition "e-prescribing" criterion (§ 170.314(b)(3)).

First, we proposed to require a Health IT Module certified to this criterion be able to receive and respond to additional National Council for Prescription Drug Programs (NCPDP) SCRIPT Standard Implementation Guide Version 10.6 (v10.6) transactions or segments in addition to the New Prescription transaction, namely Change Prescription, Refill Prescription, Cancel Prescription, Fill Status, and Medication History. We proposed to require that a Health IT Module be able to send and receive end-to-end prescriber-to-receiver/sender-to-prescriber transactions (bidirectional transactions). The proposed transactions and reasons for inclusion for testing and certification are outlined in Table 5 below.

Table 5. Proposed Additional[54] NCPDP SCRIPT v10.6 Transactions for Testing and Certification to e-Prescribing Certification Criterion

NCPDP SCRIPT v10.6 Transaction or Segment	**Use Case(s)**	**Problem Addressed/ Value in Testing for Certification**
Change Prescription (RXCHG, CHGRES)	• Allows a pharmacist to request a change of a new prescription or a "fillable" prescription. • Allows a prescriber to respond to pharmacy requests to change a prescription.	Facilitates more efficient, standardized electronic communication between prescribers and pharmacists for changing prescriptions.
Cancel Prescription (CANRX, CANRES)	• Notifies the pharmacist that a previously sent prescription should be canceled and not filled. • Sends the prescriber the results of a prescription cancellation request.	Facilitates more efficient, standardized electronic communication between prescribers and pharmacists for cancelling prescriptions.
Refill Prescription (REFREQ, REFRES)	• Allows the pharmacist to request approval for additional refills of a prescription beyond those originally prescribed. • Allows the prescriber to grant the pharmacist permission to provide a patient with additional refills or decline to do so.	Facilitates more efficient, standardized electronic communication between prescribers and pharmacists for refilling prescriptions.
Fill Status (RXFILL)	Allows the pharmacist to notify the prescriber about the status of a prescription in three cases: 1) to notify the prescriber of a dispensed prescription, 2) to notify the prescriber of a partially dispensed prescription, and 3) to notify a prescriber of	Allows the prescriber to know whether a patient has picked up a prescription, and if so, whether in full or in part. This information can inform assessments of medication adherence.

[54] We proposed to keep the "New Prescription" transaction for testing and certification.

	a prescription not dispensed.	
Medication History (RXHREQ, RXHRES)	• Allows a requesting entity to generate a patient-specific medication history request. • The responding entity can respond, as information is available, with a patient's medication history, including source, fill number, follow-up contact, date range.	Allows a requesting entity to receive the medication history of a patient. A prescriber may use this information to perform medication utilization review, medication reconciliation, or other medication management to promote patient safety.

We solicited comment on other NCPDP SCRIPT v10.6 transactions that should be considered for testing and certification, and for what use cases/value, and the factors to consider for end-to-end prescriber-to-receiver testing.

Second, we proposed to require that a Health IT Module certified to this criterion enable a user to enter, receive, and transmit codified Sig instructions in a structured format in accordance with NCPDP Structured and Codified Sig Format Implementation Guide v1.2 which is embedded within NCPDP SCRIPT v10.6 for certification to the e-prescribing criterion in the 2015 Edition.[55] We proposed this because we believe standardizing and codifying the majority of routinely prescribed directions for use can promote patient safety, as well as reduce disruptions to prescriber workflow by reducing the number of necessary pharmacy call-backs. We proposed that this requirement apply to the New Prescription, Change Prescription, Refill Prescription, Cancel Prescription, Fill Status, and Medication History prescription transactions or segments as we understood that the NCPDP Structured and Codified Sig Format can be used for all NCPDP SCRIPT v10.6 prescription transactions that include directions for medication use. We also proposed to require that a Health IT Module include all structured Sig segment components enumerated in NCPDP SCRIPT v10.6 (i.e., Repeating Sig, Code System, Sig Free Text String,

[55] NCPDP's Structured and Codified Sig Format Implementation Guide v1.2 is within the NCPDP SCRIPT v10.6 standard. https://www.ncpdp.org/NCPDP/media/pdf/StandardsMatrix.pdf

Dose, Dose Calculation, Vehicle, Route of Administration, Site of Administration, Sig Timing, Duration, Maximum Dose Restriction, Indication and Stop composites).

We solicited comment on whether we should require testing and certification to a subset of the structured and codified Sig format component composites that represent the most common Sig instructions rather than the full NCPDP Structured and Codified Sig Format Implementation Guide v1.2. NCPDP published recommendations for implementation of the structured and Codified Sig format for a subset of component composites that represent the most common Sig segments in the NCPDP SCRIPT Implementation Recommendations Version 1.29.[56]

Third, we proposed that a Health IT Module certified to this criterion be capable of limiting a user's ability to electronically prescribe all medications only in the metric standard, and be capable of always inserting leading zeroes before the decimal point for amounts less than one when a user electronically prescribes medications. We also proposed that the Health IT Module not allow trailing zeroes after a decimal point. We stated our intent for proposing these requirements was to support more precise prescription doses in order to reduce dosing errors and improve patient safety.

Last, we proposed to adopt and include the February 2, 2015 monthly version of RxNorm in this criterion as the baseline version minimum standards code set for coding medications.

Comments. Many commenters suggested reducing the scope of this proposed criterion to either divide out the requirements into separate certification criteria or to only require the minimum functionalities needed to achieve the corresponding proposed e-prescribing objective for Stage 3 of the EHR Incentive Programs (80 FR 16747).

Response. In finalizing the e-prescribing criterion, we considered whether the proposed

[56] http://www.ncpdp.org/NCPDP/media/pdf/SCRIPTImplementationRecommendationsV1-29.pdf

functionality would help achieve interoperability between health IT systems and would align with the goals and objectives described in the "Federal Health IT Strategic Plan."[57] The reasons for the finalized e-prescribing criterion and its included functionality are described below in response to comments.

Comments. A number of commenters supported the additional NCPDP SCRIPT v10.6 transactions we proposed to require for testing and certification to this criterion, and believed the additional requirement would facilitate bidirectional prescriber-pharmacist communications and comprehensive medication management. A number of commenters were concerned about the variable adoption and use of the additional NDPCP SCRIPT v10.6 transactions that were proposed. A few commenters were concerned with the interruptive nature of real-time messaging alerts and suggested that they be batch-processed to a team rather than a single provider for viewing. One commenter suggested that we verify the correct official names of the proposed NCPDP SCRIPT v10.6 transactions. Regarding the medication history transactions, a few commenters noted that many EHRs support additional means of retrieving medication history that can offer advantages to the NCPDP medication history transactions (e.g., HL7, proprietary third party integration, direct connection with third party payers).

Response. We thank commenters for their support of the proposal. Providers that prescribe or dispense Medicare Part D drugs using electronic transmission of prescriptions are required to comply with the standards that CMS has adopted under the Medicare Prescription Drug, Improvement, and Modernization Act (MMA) of 2003. CMS adopted NCPDP SCRIPT v10.6 for Part D e-prescribing in the 2013 Physician Fee Schedule final rule (77 FR 69330-69331) effective November 1, 2013, including the following transactions which we also

[57] http://www.healthit.gov/sites/default/files/9-5-federalhealthitstratplanfinal_0.pdf

proposed to require for 2015 Edition testing and certification:

- New prescription transaction;
- Prescription change request transaction;
- Prescription change response transaction;
- Refill prescription request transaction;
- Refill prescription response transaction;
- Cancel prescription request transaction;
- Cancel prescription response transaction; and
- Fill status notification.

We believe that providers that are e-prescribing under Part D should have already adopted NCPDP SCRIPT v10.6 for these transactions as required effective November 1, 2013. Further, by requiring these transactions as part of certification, we are supporting the use of additional NDPCP SCRIPT v10.6 transactions in a standardized way.

Comments. Some commenters also noted support for the medication history transaction request and response transactions, and other commenters noted that both pharmacy and EHR systems have widely adopted the medication history transactions.

Response. As stated in the Proposed Rule, we believe that all the above proposed transactions can facilitate prescriber and pharmacist communications that advance better care for patients and improve patient safety. Therefore, in support of these goals and to harmonize with CMS' Part D requirements, we have finalized our proposal to require that certified health IT systems enable a user to prescribe, send, and respond to the following NCPDP SCRIPT v10.6 transactions for certification to the 2015 Edition e-prescribing criterion:

- New prescription transaction (NEWRX);

- Prescription change request transaction (RXCHG);
- Prescription change response transaction (CHGRES);
- Refill prescription request transaction (REFREQ);
- Refill prescription response transaction (REFRES);
- Cancel prescription request transaction (CANRX);
- Cancel prescription response transaction (CANRES);
- Fill status notification (RXFILL);
- Medication history request transaction (RXHREQ); and
- Medication history response transaction (RXHRES).

We have confirmed the official name of these transactions with NCPDP. We note that the requirements we have finalized outline the capabilities that certified health IT must be able to support, and do not require providers to use these functionalities when e-prescribing. The requirements of providers and prescribers for e-prescribing are specified by other programs, such as the implementation of the Medicare Modernization Act and the EHR Incentive Programs. We also note that there are other standards and services available for requesting and receiving medication history information. Our adoption of the NCPDP SCRIPT v10.6 medication history request and response transactions is consistent with a standard that commenters agreed is widely used and—as above stated—has been adopted by the health care industry. Our adoption of these requirements does not preclude developers from incorporating and using technology standards or services not required by our regulation in their health IT products.

Regarding how message notifications are presented to health IT users, we believe this is a design feature that should be left to providers and health IT developers to determine, including whether batch notification is preferable to real-time messaging alerts.

Comments. Some commenters suggested that it was premature to require end-to-end bidirectional testing because they believed pharmacy systems may not support the transactions. Commenters also asked for clarification on how certified health IT would be tested to demonstrate end-to-end bidirectional messaging. A number of commenters suggested ONC consider deeming Surescripts certification to count towards meeting the requirements of ONC's Health IT Certification Program. A few commenters also were concerned about the differences between Surescripts and testing and certification requirements under the ONC Health IT Certification Program.

Response. ONC published a notice in the **Federal Register** (80 FR 32477) that restated our commitment to work with the health IT industry towards a more streamlined health IT testing and certification system. This notice addressed a flexibility included in the ONC Health IT Certification Program that allows the National Coordinator to approve test procedures, test tools, and test data developed by non-governmental entities for testing efficiencies in the ONC Health IT Certification Program. A person or entity may submit a test procedure or test tool (which includes test data) to the National Coordinator for Health IT to be considered for approval and use by NVLAP accredited testing laboratories. We strongly encourage persons or entities to submit such test procedures, test tools, and test data to us if they believe such procedures, tools, and data could be used to meet certification criteria and testing approval requirements, including those for e-prescribing functionalities. Given our policy that permits any person or entity to submit test procedures, test tools, and test data for approval and use under the ONC Health IT Certification Program, we encourage stakeholders to review the **Federal Register** notice and submit test procedures, test tools, and test data for approval by the National

Coordinator in accordance with the instructions outlined in the notice.[58]

We look forward to testing tools that allow pharmacy communications to either be simulated or sent by a pharmacy system that has agreed to participate in the ONC Health IT Certification Program as a pilot test system that is able to emulate real-life e-prescribing scenarios. We note that we intend to analyze any differences between our requirements for testing and certification to this certification criterion and other industry certification programs for e-prescribing to determine opportunities for alignment. However, we note that industry certification programs may address a different use case and potentially test more functionality than required by this certification criterion.

Comments. A number of commenters were concerned with the limitation of the NCPDP Structured and Codified Sig Format Implementation Guide v1.2 that limits the structured and codified Sig text element to 140 characters, and noted that it could hinder the ability to transmit complex dosing instructions (e.g., tapers). Commenters noted that a later version of the NCPDP SCRIPT Standard Implementation Guide expands this text element length to 1,000 characters, but recommended that we not adopt this version until CMS has adopted a later version as a requirement for part of Part D e-prescribing. Commenters were also concerned that the NCPDP Structured and Codified Sig Format v1.2 is not widely implemented and needs more testing. A number of commenters noted NCPDP is in the process of updating the NCPDP SCRIPT Implementation Recommendations to reflect updates in guidance on implementation of the most common Sig instructions. Some commenters also noted that there are newer versions to the NCPDP SCRIPT Implementation Recommendations than v1.29. These commenters were concerned that guidance on implementing the most common Sig instructions is still evolving and

[58] https://www.federalregister.gov/articles/2015/06/09/2015-13510/acceptance-and-approval-of-non-governmental-developed-test-procedures-test-tools-and-test-data-for

suggested that we wait until there is more implementation experience with using the NCPDP Structured and Codified Sig Format v1.2 and later versions before considering inclusion in a certification criterion. A number of commenters supported the Sig segment for the indication for the medication to be documented in SNOMED CT® to assist the pharmacist with medication counseling and care coordination, whether or not ONC were to adopt the full NCPDP Structured and Codified Sig Format v1.2.

Response. We thank commenters for their detailed comments and recommendations. We acknowledge the limitations of the 140 character structured and codified Sig, and the concerns with low implementation of the NCPDP SCRIPT Structured and Codified Sig Format v1.2 and later versions. In light of our decision to focus on interoperability and considerations about the maturity of standards, we have not finalized the proposal to require a Health IT Module certified to this criterion to enable a user to enter, receive, and transmit codified Sig instructions in a structured format. While we continue to believe that e-prescribed medication instructions should be transmitted in a structured format for improved patient safety and for clearer communication of the prescribing information as intended by the prescriber, we do not believe a standard is ready for adoption at this point in time. We will continue to monitor CMS's requirements for Part D e-prescribing, and may reconsider this stance for future rulemaking based on newer versions of the NCPDP SCRIPT Standard Implementation Guide that may provide implementation improvements.

While we are not adopting the NCPDP SCRIPT Structured and Codified Sig Format v1.2 in its entirety, we agree with commenters on the potential benefits of a field that captures the reason for the prescription. This information has value for care coordination between prescribers, pharmacists, and care team members. NCPDP SCRIPT v10.6 supports the exchange of the

reason for the prescription in a few ways, including 1) medication-associated diagnosis using diagnosis elements in the DRU (Drug Segment) and 2) medication indication using the indication elements in the SIG (Structured Sig Segment).

For the first method, NCPDP SCRIPT v10.6 supports use of ICD-9-CM codes or ICD-10-CM codes with an additional qualifier. However, the standard does not permit the medication-associated diagnosis to be exchanged using SNOMED CT® codes until version 2013011 and later. We continue to support SNOMED CT® as the vocabulary code set for clinical diagnoses. Despite the limitation of NCPDP SCRIPT v10.6 regarding exchange of SNOMED CT® codes for medication-associated diagnoses, e-prescribing transactions that include the reason for the prescription support patient safety and align with initiatives underway at HHS.[59] While the use of ICD-10-CM for medication-associated diagnoses is not ideal, the value of requiring a field for medication-associated diagnoses in accordance with NCPDP SCRIPT v10.6 outweighs the limitations of that version of the standard. We will consider requiring certification for the medication-associated diagnosis using SNOMED CT® codes in a future version of this certification criterion if we adopt a version of NCPDP SCRIPT that can support medication-associated diagnoses using SNOMED CT® codes.

The second method described above (medication indication using indication elements in the SIG) does support the use of SNOMED CT® vocabulary. In order to implement the indication elements in the SIG, developers would need to implement at least a subset of the structured and codified Sig format component composites that represent the most common Sig instructions as described in the SCRIPT Implementation Recommendations Version 1.29[60] and later. As we have not adopted the proposal to require a Health IT Module certified to this

[59] http://chainonline.org/research-tools/improving-hit-prescribing-safety/
[60] http://www.ncpdp.org/NCPDP/media/pdf/SCRIPTImplementationRecommendationsV1-29.pdf

criterion to enable a user to enter, receive, and transmit codified Sig instructions in a structured format, implementation of this second method would depend on whether the developer voluntarily chooses to implement Structured and Codified Sig Format v1.2.

Given the options discussed above, we have finalized a requirement that requires a Health IT Module to enable a user to receive and transmit the reason for the prescription using the diagnosis elements in the DRU Segment. This requirement would apply to the new, change request and response, cancel request and response, refill request and response, fill status, and medication history request and response NCPDP SCRIPT v10.6 transactions that we have required in this criterion (see discussion above). Again, we note that this requirement would only apply to the capability that a certified Health IT Module certified to this criterion has to demonstrate, not that a provider is required to populate the field for reason for the prescription when e-prescribing. For the first method described above, we note that with compliance deadline of October 1, 2015, for use of ICD-10-CM and the effective date of this final rule, we intend to test compliance with ICD-10-CM for the purposes of testing and certification under the ONC Health IT Certification Program.

We are also including an optional provision that would test a Health IT Module's ability to enable a user to receive and transmit the reason for the prescription using the indication elements in the SIG Segment for those developers that may have voluntarily chosen to implement the Structured and Codified Sig Format v1.2.

Comments. Commenters were generally supportive of improving patient safety through use of the metric standard for dosing, but recommended that this requirement only apply to oral liquid medications. A number of commenters noted that the dose quantity for non-oral, non-liquid medications may not be representable using metric units (e.g., number of puffs for

inhalers, number of drops for ear and eye drops, "thin film" for topic creams and ointments). There was some concern that pharmacies may translate metric prescribing instructions into more "patient friendly" instructions (such as translating from mL to "spoonfuls") that could lead to patient dosing concerns. Commenters were also supportive of the proposal to require the use of standard conventions for leading zeroes and decimals (i.e., a leading zero is always inserted before the decimal point for amounts less than one, as well as not allowing trailing zeroes after a decimal point).

Response. We thank commenters for their support of the proposal, and for clarifying the issue about non-metric dose quantities. Given this input and support, we have finalized the requirement that a Health IT Module be capable of limiting a user's ability to electronically prescribe oral, liquid medications in only metric standard units of mL (i.e., cc units will not be allowed for certification). A Health IT Module certified to this criterion would also be required to always insert leading zeroes before the decimal point for amounts less than one when a user electronically prescribes all medications, as well as not allow trailing zeroes after a decimal point. Stakeholder feedback has indicated that medication labels will contain dosing instructions in the metric standard if the prescriber doses in the metric standard. Along with federal partners (including the FDA and CDC),[61] we encourage pharmacies to ensure the labels maintain the metric standard for dosing instructions. Guidance already exists encouraging this as a best practice for medication labeling.[62] We understand that industry best practices also promote the provision of a metric dosing device along with oral liquid medications.[63] Last, for purposes of patient safety, we would also encourage health IT developers to implement industry

[61] http://www.cdc.gov/MedicationSafety/protect/protect_Initiative.html#MedicationErrors
[62] http://www.ncpdp.org/NCPDP/media/pdf/wp/DosingDesignations-OralLiquid-MedicationLabels.pdf
[63] http://www.ncpdp.org/NCPDP/media/pdf/wp/DosingDesignations-OralLiquid-MedicationLabels.pdf

recommendations around the use of "tall man lettering" to differentiate between drug names that are similar and commonly confused.[64]

Comments. Commenters were supportive of the proposal to adopt the February 2, 2015, monthly version of RxNorm. A few commenters suggested that we adopt this version at a minimum, but allow implementation of later versions.

Response. We thank commenters for their support and have adopted the September 8, 2015 monthly version of RxNorm.[65] As we finalized in the 2014 Edition final rule (77 FR 54170), we remind stakeholders that our policy for "minimum standards" code sets permits the adoption of newer versions of the adopted baseline version minimum standards code sets for purposes of certification unless the Secretary specifically prohibits the use of a newer version (see § 170.555 and 77 FR 54268). We agree with stakeholders that the adoption of newer versions of RxNorm can improve interoperability and health IT implementation.

Comments. A few commenters noted there is a need for standards for e-prescribing of controlled substances (EPCS). One commenter suggested that a standard for prior authorization (ePA) prescribing transactions is needed.

Response. We thank commenters for these suggestions, but note that these comments are outside the scope of this criterion as proposed.

- Common Clinical Data Set Summary Record – Create; and Common Clinical Data Set Summary Record – Receive

2015 Edition Health IT Certification Criterion
§ 170.315(b)(4) (Common Clinical Data Set summary record – create)

[64] http://www.ismp.org/Tools/tallmanletters.pdf

[65] We refer readers to section III.A.2.c ("Minimum Standards" Code Sets) for a more detailed discussion of our adoption of the September 8, 2015 monthly version of RxNorm.

2015 Edition Health IT Certification Criterion
§ 170.315(b)(5) (Common Clinical Data Set summary record – receive)

In the Proposed Rule under the proposed 2015 Edition "transitions of care" certification criterion, we solicited comment on whether we should adopt and make available for testing and certification a separate certification criterion focused on the capability to create a summary record formatted to the C-CDA Release 2.0 with or without the ability to meet the requirements of the Common Clinical Data Set definition.

Comments. Comments generally supported the proposal to adopt a separate certification criterion for the ability of a Health IT Module to create a summary care recorded formatted to the C-CDA standard. A few commenters suggested that this certification criterion would only be valuable if the Common Clinical Data Set was included as well. Similar to the comments received for the "ToC" criterion summarized previously in this section of the preamble, commenters were concerned that C-CDA documents formatted to Release 2.0 would not provide compatibility with C-CDA Release 1.1. These commenters recommended that this certification criterion should require creation of C-CDAs consistent with C-CDA Release 2.1.

Response. We agree with commenters that this criterion will be valuable if it includes the capability to create a C-CDA with the Common Clinical Data Set. This criterion may also be valuable and less burdensome for health IT developers that design technology for other programs and settings outside of the EHR Incentive Programs that would like to require or offer functionality for the creation of C-CDA documents without the other requirements of the 2015 Edition "transitions of care" criterion (e.g., transport requirements). These programs and settings may find value for providers to create a summary care record or transition of care document in accordance with the C-CDA standard and with the Common Clinical Data Set. For example, existing CMS programs point to the use of technology certified to create C-CDA documents with

the Common Clinical Data Set, including for chronic care management services in the CY 2016 Physician Fee Schedule final rule (80 FR 41796). CMS programs also encourage the use of certified health IT for various settings and purposes.[66] Accordingly, we have adopted a new 2015 Edition "Common Clinical Data Set summary record - create" certification criterion to support this and other use cases. We have also adopted a similar criterion that would support receipt of health information exchanged in accordance with this functionality (Common Clinical Data Set summary record – receive" certification criterion).

Common Clinical Data Set summary record – create

This new criterion would require a Health IT Module enable a user to create a transition of care/referral summary formatted in accordance with C-CDA Release 2.1 and that includes, at a minimum, the Common Clinical Data Set and patient matching data. For the same reasons described in the "ToC" certification criterion above, the patient match data represent a first step forward to improving the quality of data included in an outbound summary care record to improve patient matching. Please refer to our decision to adopt C-CDA Release 2.1 for all certification criteria that reference C-CDA standard creation in the 2015 Edition as described further in the preamble for the "ToC" certification criterion. Consistent with our decision for the "ToC," "clinical information reconciliation and incorporation," and "C-CDA creation performance" criteria described elsewhere in this section of the preamble, this certification criterion references the C-CDA Release 2.1 CCD, Referral Note, and (for inpatient settings only) Discharge Summary document templates for this certification criterion.

We have also included the encounter diagnoses (with either the September 2015 Release of the US Edition of SNOMED CT® or ICD-10 codes), cognitive status, functional status, reason

[66] We refer readers to section IV.B.4 ("Referencing the ONC Health IT Certification Program") of this preamble for discussion of these programs and associated rulemakings.

for referral (ambulatory only), referring or transitioning provider's name and office contact information (ambulatory only), and discharge instructions (inpatient only) which are contained in the "transitions of care" criterion. This data has value for providing additional context and information for providers to make care decisions when receiving and sending transition of care/referral summary documents. As noted above, certain CMS programs have required or encouraged that this data be transmitted between care settings. Inclusion of this data will promote consistency for transitions of care across care settings and highlight ongoing efforts to develop standards for representing this data electronically.

Common Clinical Data Set summary record – receive

In addition to adopting a new certification criterion for "Common Clinical Data Set summary record – create," we have also adopted a complementary certification criterion focused on the receipt and proper processing of a transition of care/referral summary formatted to C-CDA and with the Common Clinical Data Set. Our goal is to ensure that when a C-CDA document is created consistent with the "Common Clinical Data Set summary record – create" certification criterion that the receiving system can properly process the information for informing care coordination. This has value for stakeholders such as providers who may be participating in other programs that require the use of the "Common Clinical Data Set summary record – create" functionality as well as registries that may be recipients of this information. As stated in the Federal Health IT Strategic Plan, core technical standards form the foundation for interoperability, and systems that send and receive information in these common standards will help ensure the meaning of information is consistently understood.[67]

[67] http://www.healthit.gov/sites/default/files/9-5-federalhealthitstratplanfinal_0.pdf

In order to ensure the receiving system correctly processes the C-CDA document, we will test that a system can properly validate the information in accordance with the same requirements of the "ToC" criterion (e.g., parse, detect and notify users of errors, identify valid document templates and process data elements, and correctly interpret empty sections and null combinations and be able to display a human readable format that contains the information in the received C-CDA document in accordance with the C-CDA standard). These methods mirror those in the "ToC" criterion and will provide baseline assurance that a receiving system can properly process the C-CDA document as together they verify that the Health IT Module is correctly interpreting the received C-CDA document information.

Consistent with our decision for the "ToC" and "clinical information reconciliation and incorporation" certification criteria described above, we have required certification to the C-CDA Releases 1.1 and 2.1 CCD, Referral Note, and (for inpatient settings only) Discharge Summary document templates for this certification criterion. As previously discussed, while C-CDA Release 2.1 largely promotes compatibility with C-CDA Release 1.1, receiving systems may have to perform additional processing to ensure Release 1.1 conformance with Release 2.0. We have included a requirement that Health IT Modules be able to receive C-CDA documents with the encounter diagnoses (with either the September 2015 Release of the US Edition of SNOMED CT® or ICD-10-CM codes), cognitive status, functional status, reason for referral (ambulatory only), referring or transitioning provider's name and office contact information (ambulatory only), and discharge instructions (inpatient only) for the same reasons we have included these data in the "Common Clinical Data Set summary record – create" criterion described above.

We have also included the "section views" capability from the "ToC" certification criterion to ensure that Health IT Modules certified to this certification criterion will be able to extract and allow for individual display each section (and the accompanying document header information (i.e., metadata)) that was included in a transition of care/referral summary received and formatted in accordance with C-CDA Releases 1.1 and 2.1. This will allow a user to select and just view the relevant sections without having to navigate a potentially length C-CDA document.

- Data Export

2015 Edition Health IT Certification Criterion § 170.315(b)(6) (Data export)

We proposed to adopt a 2015 Edition "data portability" certification criterion that was revised in comparison to the 2014 Edition "data portability" certification criterion (§ 170.314(b)(7)). Similar to the 2014 Edition version, we proposed to include the 2015 Edition "data portability" criterion in the Base EHR definition (i.e., the 2015 Base EHR definition). To address feedback from health IT developers and providers on the 2014 Edition certification criterion, the proposed "data portability" certification criterion at § 170.315(b)(6) focused on specific capabilities that would give providers easy access and an easy ability to export clinical data about their patients for use in a different health information technology or a third party system for the purpose of their choosing. We emphasized that this capability would need to be user-focused and user-driven. We proposed to require that a user be able to configure a Health IT Module to create an export summary for a given patient or set of export summaries for as many patients selected and that these export summaries be able to be created according to certain document-template types included in the C-CDA Release 2.0. We proposed to require the Common Clinical Data Set as the minimum data that a Health IT Module must be capable of

including in an export summary, in addition to encounter diagnoses (according to the standard specified in § 170.207(i) (ICD-10-CM) or, at a minimum, the version of the standard at § 170.207(a)(4) (September 2014 Release of the U.S. Edition of SNOMED CT®), cognitive status, functional status, reason for referral and the referring or transitioning provider's name and office contact information, and discharge instructions for the inpatient setting. We proposed to require that a user would need to be able to be able to configure the technology to set the time period within which data would be used to create the export summary or summaries, and that this must include the ability to enter in a start and end date range as well as the ability to set a date at least three years into the past from the current date. We proposed to require that a user would need to be able to configure the technology to create an export summary or summaries based on specific user selected events listed in the Proposed Rule. We proposed to require that a user would need to able to configure and set the storage location to which the export summary or export summaries were intended to be saved.

Comments. Many commenters expressed support of the concept of "data portability." Many commenters also requested that we clarify the purpose of data portability and provide related use cases to distinguish "data portability" from the transition of care certification criterion. Some commenters also suggested renaming the criterion to better describe its intended use. One commenter noted the "ambulatory only" requirement included in the criterion seemed to be confusing data portability with transition of care.

Response. We appreciate commenters' support of the concept of data portability and the proposed certification criterion. To provide additional clarity, we have decided to simply name the adopted certification criterion in this final rule "data export."

This certification criterion's purpose is to enable a user to export clinical data from health IT for one patient, a set of patients, or a subset of that set of patients. The functionality included in the criterion is intended to support a range of uses determined by a user and it was not our intention to prescribe or imply particular uses for this functionality. We also note that this functionality is not intended to and may not be sufficient to accomplish a full migration from one product to another without additional intervention because of the scope of this criterion. Specifically, the data and document templates specified in this criterion would not likely support a full migration, which could include administrative data such as billing information. The criterion's functionality could, however, support the migration of clinical data between health IT systems and can play a role in expediting such an activity if so determined by the user.

The "inpatient only" and "ambulatory only" portions of the criterion that require referral and discharge information, respectively, were part of the scope of 2014 Edition "data portability" certification criterion, are part of the transition of care criterion, and are also referenced in by the "VDT" criterion. As such, we see no compelling reason to change this criterion's scope and have adopted the criterion with these distinctions and data.

Comments. Some commenters supported requiring all of the proposed C-CDA document templates. Other commenters stated that the number of document templates should be limited. Some commenters had recommendations on alternative vocabularies to include in the C-CDA.

Response. Consistent with other responses provided in this final rule, this certification criterion requires conformance to the C-CDA R2.1. In consideration of comments received on the Proposed Rule, we have limited the C-CDA document template scope for this criterion to the CCD document template. We note that the vocabularies used by the C-CDA R2.1 are defined through the Standards Developing Organization (SDO) process and we do not seek to change

that approach via this rulemaking (i.e., we adopt the C-CDA R2.1 as published). We note that we have adopted this criterion with the proposed inclusion of the Common Clinical Data Set and other specified data, including the updated minimum standards code sets we discuss in section III.A.2.c ("Minimum Standards" Code Sets) of this preamble.

Comments. One commenter stated that when a note is signed or an order is placed does not necessarily indicate that all relevant documentation is ready for export as the provider may enter more information in the record or a result could come back from a laboratory order. The commenter stated that this could result in incomplete data being exported. Another commenter stated that there should be an affirmative action by the user clearly indicating the intent to initiate a data export. A commenter suggested removal of the requirements related to event configuration, stating there was no clear use case. Commenters also stated that the dates in the "timeframe configuration" were unclear and sought clarification on whether it was an admission date, an encounter date, the date the data was entered in the system or some other date. One commenter recommended that providers should have access to the full set of data included in the certified health IT for the entire period covered by a provider's contract. The HITSC stated in written advice to the National Coordinator that the "trigger conditions" were not appropriate and went beyond what it believed the policy goals for this criterion.[68]

Response. In consideration of comments, we have not finalized the requirement to permit a user to configure a data export based on signing a note or placing an order. We believe that a time-based approach as the baseline scope for this certification criterion is the most appropriate, consistent with our policy goals, and helps balance user functionality required for the purposes of certification with developer burden. In that regard, by finalizing a time-based approach, we have

[68] https://www.healthit.gov/FACAS/sites/faca/files/HITSC_Certification_NPRM_TSSWG_Comments_2015-05-20.pdf

determined that this final certification criterion can be more simply described by combining the proposed "timeframe" and "event" configurations into one provision.

We have also not adopted the proposed time requirement that technology would need to include the ability to set a date at least three years into the past from the current date. We have determined that we could not properly test and certify to such a requirement. We acknowledge that some Health IT Modules presented for certification, particularly in 2016, will not have access to three or even one year's worth of patient health information that is conformant to the standards requirements of this criterion. A health IT developer's and Health IT Module's access to such health information, and the quality of such health information, will also likely vary considerably based on the customers (providers) it serves. This would further complicate testing and certification, and potentially place certain health IT developers and products at a disadvantage. Therefore, we have not adopted this proposed requirement.

We have finalized as part of this criterion a specific capability that expresses time-based configuration requirements. This first portion of this part of the criterion expresses that a user must be able to configure a time period within which data would be used to create export summaries, which must include the ability to express a start and end date range. The second portion of this part of the criterion expresses three time-based actions/configurations a user must be able to complete based on the date range they have specified. A user would need to be able to: 1) create export summaries in real-time (i.e., on demand); 2) configure technology to create such summaries based on a relative date and time (e.g., generate a set of export summaries from the prior month on the first of every month); and 3) configure technology to create such summaries based on a specific date and time (e.g., generate a set of export summaries with a date range between January 1, 2015 and March 31, 2015 on April 1, 2015 at 1:00AM EDT). We reiterate

that a Health IT Module will need to support the user's ability to select and configure those dates and times.

Comments. One commenter requested that the "file location" be a Direct address or an external location in an HIE or some other system.

Response. For the purposes of certification, we clarify that a Health IT Module must, at a minimum, permit a user to select a local or network storage location. We have intentionally left the specific transport method (e.g., sending to a Direct email address) or further product integration (e.g., routing the export to a web service, web service or integration engine) to the discretion of the health IT developer and its customers.

Comments. Commenters expressed concern that privacy and security issues may arise when data is exported. Some commenters suggested that the criterion should require an ability to limit the users that would be permitted to execute the data export functionality, contending that limiting the users could address potential performance issues that may result when executing this functionality as well as issues related to use access or misuse.

Response. We thank commenters for raising these issues and have modified this criterion in response. We agree that this certification criterion could benefit from requiring health IT to include a way to limit the (type of) users that would be able to access and initiate data export functions. Thus, consistent with other certification criteria that include functionality to place restrictions on the (type of) users that may execute this functionality, we have adopted corresponding language in this final criterion. However, we emphasize for stakeholders this additional "limiting" functionality on the type of users that may execute the data export functionality is intended to be used by and at the discretion of the provider organization implementing the technology. In other words, this functionality cannot be used by health IT

developers as an implicit way to thwart or moot the overarching user-driven aspect of this certification criterion.

- Data Segmentation for Privacy

2015 Edition Health IT Certification Criterion § 170.315(b)(7) (Data segmentation for privacy – send)

2015 Edition Health IT Certification Criterion § 170.315(b)(8) (Data segmentation for privacy – receive)

We proposed to adopt two new 2015 Edition certification criteria referred to as "data segmentation for privacy (DS4P)-send" and data segmentation for privacy (DS4P)-receive." These criteria were not proposed to be in scope for the EHR Incentive Programs. Rather, they were proposed to be available for health IT developers and other programs. The proposed certification criteria focused on technical capabilities to apply and recognize security labels (i.e., privacy metadata tags) to a patient's health record. We noted in the Proposed Rule that the technical capabilities to do so would enable a sending provider's technology to tag a patient's record such that recipient of such a record (if such recipient had also implemented the technology) would be able to recognize that the patient's record was "sensitive" and needed special protection under federal or state privacy law. For example, DS4P was piloted to support the exchange of health information covered by 42 CFR Part 2 ("Part 2"), which are federal regulations implementing the law protecting confidentiality of, and restricting access, to substance abuse related patient records.

We proposed to adopt the DS4P standard as outlined in the HL7 Version 3 Implementation Guide: DS4P, Release 1 (DS4P IG), Part 1: CDA R2 and Privacy Metadata[69].

[69] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=354 Completed Normative Ballot in January 2014 and was successfully reconciled in February 2014. HL7 approved the final standard for publication and ANSI approved in May 2014.

The standard describes the technical means to apply security labels to a health record and data may be tagged at the document-level, the section-level, or individual data element-level. The DS4P standard also provides a means to express obligations and disclosure restrictions that may exist for the data. The DS4P standard does not enforce privacy laws or alter privacy laws. A healthcare provider is still responsible for ensuring that use, access, or disclosure of the sensitive health information complies with relevant state and federal law. DS4P supports that compliance in an electronic health environment and is a means for providers to electronically flag certain pieces of data that may be subject to those laws. Importantly, the DS4P standard is "law-agnostic" and not restricted to Part 2 data. It may be implemented to support other data exchange environments in which compliance with state or federal legal frameworks require sensitive health information to be tagged and segmented.

Comments. In general, most commenters recognized the value in complying with laws that require protecting sensitive health information. However, we received comments both expressing support and opposition to adopting the proposed certification criteria at this time. Commenters in support of the DS4P certification criteria and proposed standard pointed out the standard was the best currently available option for protecting sensitive health information and allows behavioral health, substance abuse, and other data to be available at the point of care. Commenters cited teenagers, victims of intimate partner violence, and patients with behavioral health or substance abuse conditions as particularly vulnerable populations that would benefit from the ability to exchange sensitive health information electronically. Several commentators pointed out that, while we limited segmentation to document-level tagging in the Proposed Rule preamble, we did not do so in the proposed regulation text.

Commenters that expressed opposition to the DS4P certification criteria and proposed standard stated that the standard was immature and not widely adopted. The commenters expressed concern that segmentation can lead to incomplete records and that receiving systems may not know how to handle the DS4P tagged data, which could lead to incomplete records that may subsequently contribute to patient safety issues. Several comments stated that DS4P has only been piloted with Part 2 data. One commenter requested clarification on how a sending system will know if a receiving system supports DS4P. Commenters also requested guidance on how to visualize in the system that data may be incomplete or what workflows should be used when segmented data is received. Several commentators requested that we consider the Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework Volume 4 – National Extensions – Section 3.1 Data Segmentation for Privacy (DS4P)[70] as an alternative to the DS4P IG.

Response. We appreciate the thoughtful comments submitted on the proposed criteria. Notably, with respect to the comments we received that expressed opposition to the DS4P standard our analysis of the comments indicates that commenters were more concerned with the complexity of the privacy law landscape than they were about the technology itself. In this regard, the vast majority of comments focused on policy-related questions such as the likelihood that specialized privacy laws might create "holes" in the data. Additionally, we received no comments that provided substantive technical criticisms of the DS4P standard.

In reference to the DS4P standard's maturity, we note that it is considered a "normative" standard from the HL7 perspective–a status which requires substantially higher HL7 membership participation compared to a Draft Standard for Trial Use (DSTU) status. While we recognize that

[70] http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol4.pdf

to date the standard has not been widely adopted, it has been used with Part 2 data and other sensitive health information by the Substance Abuse and Mental Health Services Administration (SAMHSA), the U.S. Department of Veterans Affairs (VA), and private companies.

In consideration of the comments we received and several of HHS' overarching policy goals (enabling interoperability, supporting delivery system reform, reducing health disparities, and supporting privacy compliance), we have adopted the proposed DS4P criteria. We note that these criteria are not part of the 2015 Edition Base EHR definition, are not required in the certification program policies for health IT developers to seek certification to, and are not required for providers to participate in the EHR Incentive Programs. As we have stated, DS4P enables sensitive health information to be exchanged electronically and we strongly encourage health IT developers to include DS4P functionality and pursue certification of their products to these criteria in order to help support their users' compliance with relevant state and federal privacy laws that protect sensitive health information.

We agree with commenters that we should explicitly state that document-level tagging is the scope required for certification and have made this modification to criteria. We have also clearly indicated in the DS4P-receive criterion that the ability to receive a summary record in accordance with the C-CDA R2.1 is required. This was inadvertently omitted from the criterion's proposed regulation text, but was referenced in the DS4P-send criterion.

In response to the broader comments that were critical of the notion of DS4P, we reiterate that DS4P is a technical standard that helps healthcare providers comply the laws applicable to them. As such, healthcare providers should already have processes and workflows to address their existing compliance obligations. The DS4P standard does not itself create incomplete records. Under existing law patients already have the right to prevent re-disclosure of certain

types of data by withholding consent to its disclosure or to place restrictions on its re-disclosure. DS4P allows providers to tag data as sensitive and express re-disclosure restrictions and other obligations in an electronic form. DS4P does not determine whether a segmentation obligation exists legally or what that legal obligation means to the recipient. Instead, DS4P allows for tagging and exchange of health information that has already been determined to be sensitive and in need of special protections. In the absence of DS4P, this specially protected data may still be exchanged, if consent is given for disclosure, by fax or mail, but these methods may make the data unavailable in electronic form in the receiving provider's EHR.

We recognize that the current privacy law landscape is complex. Despite the complexities of the privacy law landscape, we believe now is the time to support a standard that allows for increased protection for individuals with sensitive health conditions and enables sensitive health information to flow more freely to authorized recipients. Over 43 million Americans ages 18 and up have some form of mental illness.[71] As stated before, providers already have workflows to care for individuals with these and other sensitive health conditions. DS4P allows providers the ability to move away from fax-and-paper information exchange into interoperable exchange of sensitive health information. Oftentimes, individuals with sensitive health conditions require coordinated care that is not possible if sensitive health data cannot be exchanged. Additionally, the technical ability to segment data supports the Precision Medicine Initiative[72] and delivery system reform[73] where those initiatives depend on making computable individual's choices about disclosure of their data.

---

[71] http://www.samhsa.gov/disorders
[72] https://www.whitehouse.gov/sites/default/files/docs/pmi_privacy_and_trust_principles_july_2015.pdf; see also https://www.whitehouse.gov/the-press-office/2015/01/30/fact-sheet-president-obama-s-precision-medicine-initiative
[73] http://www.hhs.gov/healthcare/facts/blog/2014/09/improving-health-care-delivery.html

The current DS4P standard does not have a service discovery mechanism to determine if a potential recipient is able to receive a tagged document. We expect that providers will have to determine the receiving capabilities of their exchange partners, similar to how they have to work with their exchange partners today when they are manually exchanging sensitive health information via fax. Additionally, the DS4P standard contains a human-readable text block that will render in the recipients system—putting the human healthcare user on notice that they are viewing sensitive health information, allowing them to take appropriate actions in their system manually.

We are not aware of implementations that have used the IHE National Extensions for Data Segmentation for Privacy and do not agree with permitting it as an alternative approach to DS4P for the purposes of certification at this time.

- Care Plan

2015 Edition Health IT Certification Criterion § 170.315(b)(9) (Care plan)

We proposed to adopt a new 2015 Edition certification criterion that would require a Health IT Module to enable a user to record, change, access, create and receive care plan information in accordance with the Care Plan document template in the HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes.[74] We explained that the C-CDA Release 2.0 contains a Care Plan document template that provides a structured format for documenting information such as the goals, health concerns, health status evaluations and outcomes, and interventions. We emphasized that the Care Plan document template is distinct from the "Plan of Care Section" in previous versions of the C-CDA, stating that the Care Plan document template represents the synthesis of multiple plans of care (for treatment) for a

[74] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=379

patient, whereas the Plan of Care Section represented one provider's plan of care (for treatment). The Proposed Rule noted that the C-CDA Release 2.0 had renamed the previous "Plan of Care Section" as the "Plan of Treatment Section (V2)" for clarity. We sought comment on whether we should require for certification to this criterion certain "Sections" that are currently deemed optional as part of the Care Plan document template for certification to this criterion, namely the "Health Status Evaluations and Outcomes Section" and "Interventions Section (V2)."

Comments. Commenters were supportive of the proposal to adopt a new voluntary "care plan" criterion. The commenters stated that the Care Plan document template supports broader information about the patient, including education, physical therapy/range of motion, and social interventions not commonly found in other parts of the C-CDA standard. A few commenters stated that the C-CDA Release 2.0 Care Plan document template only represents a "snapshot in time," rather than a dynamic, longitudinal shared care plan. Some commenters expressed concern that this document template is new to C-CDA Release 2.0 and suggested that there was no implementation experience. Other commenters stated that clinician input was factored into the development of the Care Plan document template and that there have been pilots through the S&I Framework Longitudinal Coordination of Care Initiative.[75] Commenters suggested that the inclusion of the Care Plan document template in certification would provide a glide path for adoption of EHRs by home health care and hospice providers.

Response. We thank commenters for their feedback. As stated in the Proposed Rule (80 FR 16842), we believe the Care Plan document template has value for improving coordination of care and provides a structured format for documenting information such as goals, health concerns, health status evaluations, and interventions. It represents a consensus-based approach

[75] http://wiki.siframework.org/LCC+Pilots+WG

and is the best standard available today for capturing and sharing care plan information. The document template has also been demonstrated through pilots in the S&I Framework. As such, we have adopted this criterion. To note, we have adopted the C-CDA Release 2.1 standard for this certification criterion for consistency with our approach to the C-CDA in this final rule and for the same substantive reasons discussed earlier in this preamble under the "ToC" certification criterion.

Comments. A few commenters suggested that it was not necessary to adopt this certification criterion because other proposed criteria also reference the C-CDA standard and Care Plan template.

Response. As described in more detail in this preamble for the other certification criteria we have adopted that reference the C-CDA standard (e.g., "ToC," "data export," and "Consolidated CDA creation performance"), we have adopted reduced requirements for C-CDA Release 2.1 document template conformance per the use case(s) served by each certification criterion. As such, the "ToC," "data export," "clinical information reconciliation," and "Consolidated CDA creation performance" criteria do not require the C-CDA Release 2.1 Care Plan document template. Therefore, we have adopted this criterion to support the care planning use cases recited above and in the Proposed Rule.

Comments. A commenter recommended that we be more specific about which optional (e.g., "MAY") items in the Health Concerns section of the C-CDA Care Plan document template should be required.

Response. As we stated in section III.A.2.b of this preamble regarding referenced standards for certification, if an element of a standard or IG is optional or permissive in any way, it will remain that way for testing and certification unless we specified otherwise in regulation.

To the commenter's question, we have not specified otherwise in regulation. We note, however, that we would expect that health IT developers and providers would work together to determine whether the optional items are relevant and useful for the provider and patients intended to be served by the Health IT Module.

Comments. Most commenters expressed support for requiring a Health IT Module to be certified to the optionally designated sections in the C-CDA Release 2.0 Care Plan document template to meet this criterion. Commenters noted the Health Status Evaluations and Outcomes Section incorporates patient-reported outcomes to improve care and assist with the long-term goal of a truly integrated care plan. Commenters also suggested the Interventions Section (V2) would be useful for patients and family caregivers.

Response. We thank commenters for their feedback. We agree with commenters that the Health Status Evaluations and Outcomes Section and Interventions Section (V2) of the C-CDA provide important information for incorporating the patient's perspective in an effort to improve outcomes and the long-term goal of a longitudinal, dynamic, shared care plan. Accordingly, we have specifically identified these sections as required to be met for certification to this criterion.

Comments. A few commenters suggested that this criterion should also include a requirement for the receiving system of a C-CDA Care Plan to be able to reconcile the care plan information with the patient's record in the receiving system.

Response. While reconciliation is important and may be appropriate for any future iteration of this certification criterion, this functionality is outside the scope of our proposal. Therefore, we have not included in this criterion. We note that the industry continues to improve and develop advanced care planning standards and tools, which may address the incorporation of

care planning information. As such, we will continue to monitor these developments for consideration in future rulemaking.

Comments. A few commenters suggested that we are conflating certain sections of the C-CDA Care Plan document template (e.g., Health Concerns and Goals) with items proposed in the Common Clinical Data Set.

Response. We refer readers to our response to this comment under the Common Clinical Data Set definition in section III.B.3 of this preamble.

- Clinical Quality Measures – Record and Export

2015 Edition Health IT Certification Criterion § 170.315(c)(1) (Clinical quality measures – record and export)

We proposed to adopt a 2015 Edition "clinical quality measures (CQM) – record and export" certification criterion that was revised in comparison to the 2014 Edition "CQM – capture and export" certification criterion (§ 170.314(c)(1)). In the Proposed Rule, we explained that we would align our use of the term "record" used in other 2014 and 2015 Edition certification criteria and proposed to call this certification criterion "CQM – record and export." We proposed to require that a system user be able to export CQM data formatted to the Quality Reporting Document Architecture (QRDA) Category I standard at any time the user chooses for one or multiple patients and without subsequent developer assistance to operate. We also proposed to require that this certification criterion be part of the set of criteria necessary to satisfy the "2015 Edition Base EHR" definition (see also section III.B.1 of this preamble for a discussion of the 2015 Edition Base EHR definition). We solicited comment on the standard, including versions of QRDA Category I, we should adopt for this certification criterion with consideration given to where the industry may be with adoption of CQM and CDS standards

over the next few years. In particular, we identified industry efforts to harmonize CQM and CDS standards. We asked for comment on the following version of QRDA or QRDA-like standards:

- HL7 Implementation Guide for CDA Release 2: Quality Reporting Document Architecture (QRDA), DSTU Release 2 (July 2012);
- HL7 Implementation Guide for CDA Release 2: Quality Reporting Document Architecture (QRDA), DSTU Release 2 (July 2012) and the September 2014 Errata; or
- A QRDA-like standard based on the anticipated Quality Improvement and Clinical Knowledge (QUICK) Fast Healthcare Interoperability Resources (FHIR)-based DSTU.

In asking for comment, we sought to understand the tradeoffs stakeholders perceive in adopting each standard considering that the EHR Incentive Programs Stage 3 proposed rule proposed that health IT certified to the 2015 Edition would not be required until January 1, 2018, but that EPs, eligible hospitals, and CAHs participating in the EHR Incentive Programs Stage 3 objectives and measures could upgrade to health IT certified to the 2015 Edition "CQM – record and export" certification criterion in 2017.

Comments. The majority of commenters recommended adopting the HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture – Category I (QRDA I); Release 1, DSTU Release 3, US Realm ("QRDA Category I Release 3 IG" or "Release 3").[76] Commenters noted that CMS is using the QRDA Category I Release 3 IG for the 2015 update eCQM measures and the 2016 reporting period and recommended that we adopt this version for program alignment.[77] Commenters indicated Release 3 addresses known issues, fixes errors, and adds missing content compared to earlier versions of the QRDA Category I standard.

[76] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=35
[77] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/eCQM_Library.html

Commenters also noted that Release 3 uses an incremental version of the underlying data model (the Quality Data Model 4.1.1) that is a step-wise approach toward harmonized CQM and CDS standards that stakeholders are developing.

While commenters were supportive of the work and direction on harmonized CQM and CDS standards to produce an anticipated QUICK FHIR-based DSTU, all commenters noted that no such standard is currently available and that it is premature to require any such standard for the 2015 Edition. Many commenters stated that stakeholders are still in the process of implementing QRDA and that we should adopt an incremental version of QRDA rather than pivot to the QUICK standard at this time.

Response. With consideration of commenters' feedback, we have adopted this criterion and the QRDA Category I Release 3 IG (both Volumes 1 and 2) for this criterion. In order to accommodate Release 3, we are amending the paragraph level at § 170.205(h) to move the standard that is required for the 2014 Edition "CQM – capture and export" criterion to § 170.205(h)(1), and adopting Release 3 at § 170.205(h)(2).

We agree with commenters that it is too early to adopt the QUICK CQM standards, but will continue to support the development and piloting of these harmonized CQM and CDS standards and reassess their appropriateness for certification at the time of a relevant future rulemaking.

Comments. Commenters expressed support for the proposal to permit users to export CQM data formatted to the QRDA Category I standard for one or multiple patients at any time the user chooses and without subsequent developer assistance to operate. Some commenters requested clarification on what constitutes "without subsequent developer assistance to operate" and noted that batch export could be disruptive to overall EHR functionality. A few commenters

asked for clarification of the use cases for export. Some commenters also requested clarification regarding who constitutes a "user," with a few commenters suggesting that the "user" should only be those individuals with specific administrative privileges.

Response. We thank commenters for their support of the proposal. We have included in this criterion a requirement that a user be able to export a data file formatted in accordance with Release 3 for one or multiple patients that includes all of the data captured for each CQM to which the health IT was certified. We believe that the ability to export CQM data would serve two purposes. First, this functionality will allow a provider or health system to view and verify their CQM results for quality improvement on a near real-time basis. Second, the export functionality gives providers the ability to export their results to multiple programs, such as those run by CMS, states, and private payers.

As we discussed in the 2015 Edition proposed rule (80 FR 16843), our intent is for users of certified health IT to be able to export CQM data formatted to the QRDA Category I standard for one or more patients without needing to request support from a developer. Stakeholders have noted that some health IT certified to the 2014 Edition "CQMs – capture and export" criterion do not provide users the ability to export QRDA Category I files "on demand" and that users must submit requests for the health IT developer to assist or perform the export function on their behalf. For testing and certification to the 2015 Edition "CQM – record and export" criterion, we would expect demonstration that the Health IT Module enables the user to export CQM data formatted to the QRDA Category I standard for one or more patients without needing additional developer support. We believe that providers and health systems should determine the protocols around when and how providers export CQM data, and we do not address this issue as part of certification as it is outside the scope of the ONC Health IT Certification Program.

We previously described a "user" in the 2014 Edition final rule (77 FR 54168) and continue to use the same description for the 2015 Edition. We expect the functionalities of this criterion to be available to any user, but the specification or limitation of types of users for this functionality is outside the scope of certification to this criterion. Providers have the discretion to determine the protocols for when and which users should use this functionality.

- Clinical Quality Measures – Import and Calculate

2015 Edition Health IT Certification Criterion § 170.315(c)(2) (Clinical quality measures – import and calculate)

We proposed to adopt a 2015 Edition "clinical quality measures (CQM) – import and calculate" certification criterion that was revised in comparison to the 2014 Edition "CQM – import and calculate" certification criterion (§ 170.314(c)(2)). We proposed to require that a system user be able to import CQM data formatted to the QRDA standard for one or multiple patients at any time the user chooses and without additional assistance to operate. We proposed to no longer include an exemption that would allow a Health IT Module presented for certification to § 170.315(c)(1), (c)(2), and (c)(3) to not demonstrate the data import capability. Rather, we proposed that a Health IT Module would be required to demonstrate that it could import data in order to be certified to this certification criterion even if it is also certified to provide "record and export" and "electronic submission/report" functions. We solicited comment on the version of QRDA or QRDA-like standards for individual patient-level CQM reports we should adopt for this certification criterion.

We stated that we intend testing to the 2015 Edition "CQM – import and calculate" certification criterion to include the import of a larger number of test records compared to testing for the 2014 Edition and to automatically de-duplicate records for accurate CQM calculation. We

requested comment on this intent and the number of test records we should consider testing a Health IT Module for performing import and calculate functions.

Comments. The majority of commenters recommended adopting the HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture – Category I (QRDA I); Release 1, DSTU Release 3, US Realm ("QRDA Category I Release 3 IG" or "Release 3"). These commenters cited the same reasons for adopting Release 3 as recited under the 2015 Edition "CQM – record and export" criterion summarized above, and to which we refer readers. A few commenters recommended that QRDA Category III (aggregate level CQM reports) should not be required for this criterion.

Response. With consideration of commenters' feedback, we have adopted this criterion and the QRDA Category I Release 3 IG (both Volumes 1 and 2) for this criterion. We note that we did not propose to require import of QRDA Category III files for this criterion and thus QRDA Category III is outside the scope of this criterion.

Comments. Commenters expressed support for the proposal to permit users to import CQM data formatted to the QRDA Category I standard for one or multiple patients at any time the user chooses and without subsequent developer assistance to operate. A few commenters asked for clarification of the use cases for import, and the justification for why all systems (even those previously considered "self-contained") must demonstrate import. These commenters noted that some systems export CQM data to a third-party data aggregator or warehouse for calculation, whereas other EHR systems perform the calculation function itself. In the latter case, some commenters suggested it was not necessary for the system to be able to import CQM data. A few commenters were not supportive of requiring import using the QRDA Category I standard. Rather, they suggested import should be allowed using whatever standard or data

structure is already being used by the system for import.

Response. We thank commenters for their support of the proposal and requests for additional clarifications. We have included in this criterion a requirement that a user be able to import a data file formatted in accordance with Release 3 for one or multiple patients that includes all of the data captured for each CQM to which the health IT was certified. We believe that the ability to import CQM data would serve two purposes. First, this functionality could streamline the testing and certification process by importing QRDA Category I files rather than systems needing to manually enter test patient data. Second, the import functionality can promote quality improvement and data sharing between systems by providing systems the ability to import CQM data from other systems in a standardized format. We note that ONC held a HITPC hearing on certification in 2014 and the HITPC recommended CQM certification as a top priority for providing value for quality improvement and delivery system reform.[78] While we are not prescribing how data is imported into a system (e.g., mapped to a backend database or viewable to a provider as part of the patient record), we believe that requiring the import functionality can facilitate these use cases.

As we discussed in the 2015 Edition proposed rule (80 FR 16843), our intent is for users of certified health IT to be able to import CQM data formatted to the QRDA Category I standard for one or more patients without needing to request support from a developer. Stakeholders have noted that some health IT certified to the 2014 Edition "CQMs – import and calculate" criterion do not provide users to import QRDA Category I files "on demand" and that users must submit requests for the developer to assist or perform the import function on their behalf. For testing and certification to the 2015 Edition "CQM – import and calculate" criterion, we would expect

[78] http://www.healthit.gov/facas/calendar/2014/05/07/policy-certification-hearing

demonstration that the Health IT Module enables the user to import CQM data formatted to the QRDA Category I standard for one or more patients without needing additional developer support. We believe that providers and health systems should determine the protocols around when and how providers import CQM data, and we do not address this issue as part of certification as it is outside the scope of the ONC Health IT Certification Program.

Comments. Commenters supported our intent to increase the number of test records used during the testing and certification process for this criterion. Most commenters recommended that rather than test to a certain number of records, testing should ensure that every pathway by which a patient can enter the numerator or denominator of the given measure is tested. Commenters were supportive of requiring health IT to demonstrate auto de-duplication of imported records during the testing process, but some commenters were concerned about how systems would be required to incorporate and reconcile imported data. Commenters requested clarification on whether duplicate records would be determined by a duplicate record ID number or by requiring the system to compare the data in two records and determine whether it is a duplicate. Commenters were concerned about the amount of work to reconcile data using the latter method.

Response. We thank commenters for supporting use of an increased number of test records during the testing and certification process and we agree that testing should more robustly test the pathways by which a patient can enter the numerator or denominator of a measure, including exclusions and exceptions. In regard to auto de-duplication, while we have adopted the requirement, we have not prescribed how systems would demonstrate de-duplication or what systems must do with the imported data. We are providing flexibility in allowing health IT developers and providers to determine the most suitable methods for de-duplication and

import of data for the given situation.

- Clinical Quality Measures – Report

2015 Edition Health IT Certification Criterion § 170.315(c)(3) (Clinical quality measures – report)

In the Proposed Rule, we stated that we intend to better align with the reporting requirements of other CMS programs, and thus, would propose certification policy for reporting of CQMs in or with annual PQRS and/or Hospital IQR program rulemaking anticipated in CY 2015. We explained that we anticipated proposing standards for reporting of CQMs that reflect CMS' requirements for the "form and manner" of CQM reporting (e.g., CMS program-specific QRDA standards), allowing for annual updates of these requirements as necessary. Under this approach, we noted that the "CQMs – report" certification policy and associated standards for the 2015 Edition that support achieving EHR Incentive Programs requirements would be proposed jointly with the calendar year (CY) 2016 PFS and/or IPPS proposed rules. We clarified that we anticipated removing "electronic" from the name of this certification criterion because we expected that all functions proposed in the 2015 Edition health IT certification criteria to be performed or demonstrated electronically, unless specified otherwise. We also explained that we anticipated naming this certification criterion "report" instead of "submission" to better align with the language we use in other certification criteria that also require demonstration of a "reporting" functionality (i.e., to submit data).

We subsequently proposed a 2015 Edition "CQMs – report" certification criterion in the 2016 IPPS/LTCH PPS proposed rule that would require a Health IT Module to enable a user to electronically create a data file for transmission of clinical quality measurement data using the "base" (i.e., industry-wide, non-program-specific) HL7 QRDA Category I and Category III standards, at a minimum (80 FR 24613-24614). We also proposed, as part of this proposed

criterion, to permit optional certification for health IT in accordance with the CMS "form and manner" requirements defined in the CMS QRDA Implementation Guide.[79] CMS specified that health IT certified to this proposed certification criterion would be required to meet the proposed CEHRT definition for the EHR Incentive Programs.

As detailed in the FY 2016 IPPS/LTCH PPS proposed rule, we solicited comment on the appropriate versions of the Quality Reporting Document Architecture – Category I (individual patient level quality reports) and Category III (aggregate level quality reports) standards that should be adopted. In order to give full consideration to the comments received on the appropriate versions of the standards we should adopt, we did not adopt a "CQMs-report" certification criterion in the 2016 IPPS/LTCH PPS final rule (80 FR 49760). We stated that we anticipate adopting both the certification criterion and the appropriate versions of the standards in a subsequent final rule later this year. We also noted we intended to address comments received on both the proposed "CQMs-report" certification criterion and the versions of the standards in that same rule. We have used this final rule to address the comments and adopt the criterion and standards as specified below.

Comments. Commenters were supportive of the proposal to adopt a 2015 Edition certification criterion for CQM reporting. There was mixed feedback on whether a 2015 Edition "CQMs – report" criterion should require adherence to the HL7 QRDA Category I and Category III standards, or solely to the CMS QRDA Implementation Guide. The majority of commenters recommended that we not move to the Quality Improvement and Clinical Knowledge (QUICK) CQM[80] standards as they are unpublished and have not yet been balloted. Rather, commenters

[79] The CMS QRDA Implementation Guide can be accessed at http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/eCQM_Library.html.
[80] http://wiki.siframework.org/Clinical+Quality+Framework+Initiative

suggested we adopt incremental versions the QRDA standards because health IT developers and providers have focused efforts on fully supporting QRDA reporting. To this end, some commenters recommended that we adopt Release 3 of the QRDA Category I standard, and the November 2012 version of the QRDA Category III standard with the September 2014 Errata. Other commenters did not support Release 3 of the QRDA Category I standard, stating it was too immature for adoption. One commenter suggested that while Release 3 of QRDA Category I may be a new standard and require more work compared to Release 2 of QRDA Category I with the 2014 Errata, it offers more efficiencies and reduces errors that would ultimately improve eCQM processing.

Response. We thank commenters for their support for proposal and comments regarding the versions of standards. We believe that certification to the HL7 QRDA Category I and III standards provides a baseline for interoperability of CQM data as these standards are consensus-based and industry developed. Additionally, the HL7 QRDA standards are program-agnostic and can support a number of use cases for exchanging CQM data. Providers participating in CMS payment programs such as the EHR Incentive Programs, IPPS, or Hospital IQR may need to adhere to additional CMS QRDA reporting requirements as detailed in the CMS QRDA IG. However, we do not believe that all certified health IT is intended to be used for CMS reporting, and therefore have only included requirements for reporting to CMS (e.g., use of the CMS QRDA IG) as an optional provision within the criterion. We note that the CMS QRDA IG has been aligned with the HL7 QRDA Category I and III standards, but the CMS QRDA IG includes additional requirements beyond the HL7 IGs specific to CMS program reporting.

Our adoption of an optional provision to certify CQM reporting in the form and manner of CMS submission allows CMS to determine as part of its program requirements whether this

optional provision of the CQM reporting criterion is required for participation in certain CMS programs. For example, CMS has proposed to revise the CEHRT definition to require health IT be certified to the provision of the "CQMs – report" criterion we have deemed optional (80 FR 41880-41881), which would affect, at a minimum, providers participating in the EHR Incentive Programs.

We agree with the comments supporting the adoption of Release 3 of the QRDA Category I IG as the IG will improve eCQM processing and reduce errors. The IG will also better align with the C-CDA Release 2.1 for purposes of interoperability as compared to QRDA Category I Release 2 with the 2014 Errata. Further, Release 3 of the QRDA Category I IG also aligns with the CMS 2015 update to eCQM measures for 2016 e-reporting (https://ecqi.healthit.gov/ecqm).

We agree with commenters that it is too early to adopt the QUICK CQM standards, but will continue to support the development and piloting of these harmonized CQM and CDS standards and reassess their appropriateness for certification at the time of a relevant future rulemaking.

In sum, after consideration of public comments, we have adopted a 2015 Edition "CQMs – report" criterion that requires a Health IT Module to enable a user to (electronically) create a data file for transmission of CQM data in accordance with:

- HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture – Category I (QRDA I); Release 1, DSTU Release 3 (US Realm) (both Volumes 1 and 2); and

- HL7 Implementation Guide for CDA® Release 2: Quality Reporting Document Architecture – Category III, DSTU Release 1 (US Realm) with September 2014 Errata.

All Health IT Modules must certify to the above standards to meet the criterion. As noted above, the criterion also includes an optional provision that requires the electronic creation of a data file for transmission of CQM data that can be electronically accepted by CMS (i.e., the form and manner of submission as specified in the CMS QRDA IG[81]).

In order to accommodate the new QRDA standards in the regulation text, we have revised the paragraph levels at § 170.205(h) and (k) to move the QRDA standards adopted in the 2014 Edition to § 170.205(h)(1) and (k)(1) respectively. We have also made a technical amendment to the regulation text for the 2014 Edition certification criteria for capturing, calculating, and reporting CQMs (at 45 CFR 170.314(c)(1), (c)(2), and (c)(3), respectively) to continue to reference the appropriate implementation specifications.

Comments. Commenters requested clarification on whether our proposal to adopt a 2015 Edition "CQMs – report" certification criterion through the 2016 IPPS/LTCH PPS proposed rule implies that annual recertification to the proposed criterion would be required as CMS updates the measure specifications and the CMS QRDA IG annually.

Response. We clarify that the proposal for a 2015 Edition "CQMs – report" certification criterion would not require Health IT Modules to be recertified annually as part of the ONC Health IT Certification Program. However, in conjunction with our CMS colleagues, we also clarify that CMS requires that health IT be certified to the CMS QRDA IG and be updated to the latest annual measure specifications if providers intend to use the health IT to report CQMs

[81] Available at: https://www.cms.gov/regulations-and-guidance/legislation/ehrincentiveprograms/ecqm_library.html

electronically to CMS. This does not mean recertification is required each time the health IT system is updated to a more recent version of the CQMs. As CMS stated in the 2016 IPPS/LTCH PPS proposed rule, CMS intends to publish a request for information (RFI) on the establishment of an ongoing cycle for the introduction and certification of new measures, the testing of updated measures, and the testing and certification of submission capabilities (80 FR 24614-24615). We and CMS encourage readers to submit their comments and recommendations for consideration upon publication of the RFI.

- Clinical Quality Measures – Filter

2015 Edition Health IT Certification Criterion § 170.315(c)(4) (Clinical quality measures – filter)

We proposed to adopt a new 2015 Edition certification criterion that would require health IT to be able to record data (according to specified standards, where applicable) and filter CQM results at both patient and aggregate levels. We listed proposed data elements and vocabulary standards for some data elements to maintain consistency in the use of adopted national standards, and we clarified that a Health IT Module must be able to filter by any combination of the proposed data elements (i.e., by any one (e.g., provider type) or a combination of any of the data elements). We noted that the combination requirement is different than other certification criteria in the Proposed Rule in that it requires all combinations to be demonstrated for certification and not just one. We requested comment on the appropriateness of the proposed data elements for CQM filtering, including whether they are being captured in standardized vocabularies, and additional data elements that we should consider for inclusion and standardized vocabularies that might be leveraged for recording this information in health IT.

Comments. Many commenters were in support of adopting a new criterion for CQM filtering. Commenters noted the benefit for supporting the identification and reduction of

disparities by filtering by patient demographics and problem list. A number of commenters also supported the list of proposed data elements as a good starting point with mature standards.

Response. We thank commenters for the feedback. Our overall goal for this functionality is to allow a provider to make a query for CQM results using one or a combination of data captured in the certified Health IT Module for quality improvement and quality reporting purposes. We agree with commenters on the value of this functionality for identification of health disparities, helping providers identify gaps in quality, and supporting a provider in delivering more effective care to sub-groups of their patients. As such, we have adopted this certification criterion with the following modifications described below.

Comments. Some commenters noted it would be valuable to filter both QRDA Category I and Category III quality reports for this criterion to assist with individual patient quality improvement and for population health. One commenter noted that providing a filtered view to the provider would allow for easy spot-checking of health disparity trends to inform quality improvement projects.

Response. We thank commenters for the feedback and agree with the value of being able to filter QRDA I and Category III files as well as for providing a filtered view of the quality results for supporting the quality improvement and quality reporting use cases. QRDA Category I enables an individual patient-level quality report that contains quality data for one patient for one or more quality measures.[82] The QRDA Category III standard enables an aggregate quality report containing calculated summary data for one or more measures for a specified population of patients within a particular health system over a specific period of time.[83] We have, therefore, required that a Health IT Module certified to this criterion must be able to filter CQM results at

[82] Available at: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=35.
[83] Available at: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=286.

the patient and aggregate levels and be able to create a data file of the filtered data in accordance with the QRDA Category I and Category III standards, as well as be able to display the filtered data results in human readable format. To align with the versions of the QRDA standards we are adopting for the 2015 Edition "CQMs – record and export," "CQMs – import and calculate," and "CQMs – report" criteria, we have adopted the following standards for this criterion:

- HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture – Category I (QRDA I); Release 1, DSTU Release 3 (US Realm) (both Volumes 1 and 2); and
- HL7 Implementation Guide for CDA® Release 2: Quality Reporting Document Architecture – Category III, DSTU Release 1 (US Realm) with September 2014 Errata.

Comments. One commenter expressed concern that the proposed criterion aims to achieve attribution of eCQM results to particular providers or groups of providers for participation in certain quality reporting programs, but that the proposed functionality to filter does not actually achieve attribution. The commenter noted that attribution requires a more complex approach than is currently proposed with the filtering of CQM results using different combinations of data, and suggested that it was appropriate for the industry to develop attribution standards in upcoming quality standards work.

Response. We thank the commenter for the feedback. We agree that proper attribution of eCQM results to a particular provider or group of providers will require a set of defined processes. We believe that the functionality in this criterion is a good step forward toward establishing such a process while the industry continues to improve eCQM standards as described further in the Proposed Rule (80 FR 16842-16843). We intend to continue working

with stakeholders to establish standards and processes for proper attribution of quality measure results for consideration in future rulemaking.

Comments. A few commenters requested clarification of the language in the preamble and suggested that testing should not require that all possible combinations of data be demonstrated as it would be time-consuming and a very large number.

Response. We clarify that for testing Health IT Modules will not be tested to every possible combination of data, but that any combination could be tested at the discretion of the tester. We also note that we have not prescribed a workflow that must be demonstrated for certification in order to provide flexibility as long as the desired outcome can be achieved.

Comments. A few commenters indicated concern over the lack of alignment between the data and associated standards proposed for this criterion compared with our proposed 2015 Edition Common Clinical Data Set definition (80 FR 16871-16872), the data proposed in the 2015 Edition "demographics" criterion (80 FR 16816-16817), and the request for comment for "future considerations for electronically specified measures using Core Clinical Data Elements" in the CMS 2016 Inpatient Prospective Payment System (IPPS) proposed rule (80 FR 24583-24584). Commenters suggested we work to ensure alignment of the data proposed in this criterion with those in the Common Clinical Data Set definition and proposed for the demographics criterion. Commenters also suggested we work with CMS on the Core Clinical Data Elements definition.

Response. We thank commenters for the recommendation to ensure data definitions are aligned. This criterion proposes a filter by "patient age" whereas the Common Clinical Data Set and demographics certification criterion specify "date of birth." For this certification criterion, we intend that "patient age" is derived from the patient's date of birth, but specify "patient age"

because we believe that providers should be able to filter/query CQM results by the patient's age rather than their date of birth. For example, the provider may query for patients older than a certain age, younger than a certain age, or between a range of ages. Therefore, we have adopted patient age as a data element for this certification criterion. We believe that all the other data in this criterion are aligned with the 2015 Edition Common Clinical Data Set and "demographics" criterion. We note that the "Core Clinical Data Elements" in CMS' 2016 IPPS proposed rule is not being proposed for the 2016 program year and is a comment solicitation for future rulemaking. We intend to continue to work with CMS on alignment of data elements being required for capture across programs.

Comments. Commenters indicated some concern that providers may use multiple Tax Identification Numbers (TINs) and different levels of TIN/National Provider Identifier (TIN/NPI) combinations. There was general support for the use of the NPI as a data element for this criterion.

Response. We believe that including TIN and NPI in this criterion offers a baseline for filtering by these data for certification. We would expect that any programs that may require CQM reporting using TIN and/or NPI would provide additional guidance on the level to use for participation in its programs. Therefore, we have adopted TIN and NPI as data elements for this criterion.

Comments. There was general support for use of the Healthcare Provider Taxonomy Code Set[84] for classifying provider types. Commenters indicated they were not aware of additional existing standards for provider types. A few commenters indicated concern that

[84] http://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/MedicareProviderSupEnroll/Taxonomy.html

providers can select multiple codes in the NPI system that reflects their overall practice rather than their individual specialty, and that the code may have low reliability.

Response. We thank commenters for the feedback. We agree that the Healthcare Provider Taxonomy Code Set (the "Code Set") is the best available standard for classifying provider type at this point in time, and have therefore adopted the CMS Crosswalk: Medicare Provider/Supplier to Healthcare Provider Taxonomy, April 2, 2015 as the standard for provider type for this criterion (to the version updated April 2, 2015 as a minimum version for certification).[85] This crosswalk maps the Medicare Provider/Supplier type to the relevant healthcare provider taxonomy codes. It is our understanding that when a provider registers for an NPI number, they are required to select at least one provider type code from the Code Set, but may select more than one code. However, the provider is required to select one code as the primary code. It is also our understanding that the NPI record for a given provider contains all codes a provider selected, and so we would expect that CQM results could be filtered by any one of the provider's selected codes (e.g., primary, secondary, tertiary, etc.). In order to ensure the NPI record is up-to-date, we would recommend that health care providers update and/or verify their registration annually in the CMS National Plan and Provider Enumeration System (NPPES)[86] to reflect the most accurate codes for the type of care the provider is currently providing. There are three methods by which an individual can access the NPI files: 1) through a downloadable file, 2) through a display/query on the NPPES website, and 3) through an interface to the NPPES API. While health systems may keep their own internal records of NPI information for the providers practicing in their system, we recommend that any of the three above methods

[85] https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/MedicareProviderSupEnroll/Downloads/TaxonomyCrosswalk.pdf
[86] https://nppes.cms.hhs.gov/NPPES/Welcome.do

provides the most up-to-date information and would encourage systems to verify and use this information for their internal records.

Comments. As discussed in the "transitions of care" criterion, a number of commenters suggested adoption of the US Postal Service postal address standard for address as concerns patient matching. Commenters noted that the standard is widely supported by health care organizations today and is recommended by the American Health Information Management Association.[87] Some commenters were concerned about complexity in systems being able to choose the correct practice site that a patient was seen at as a patient may visit more than one practice site for a given provider. Another commenter suggested we consider the GS1 Global Location Number (GLN) standard[88] for practice site address as it is based on the USPS standard and could be filtered to provide a specific practice site address through the level of "party" and "location" using the GS1 GLN standard.

Response. We thank commenters for the input. At this point in time, we believe that use of the QRDA Category I and III standards which reference the HL7 postal format is an incremental step toward an industry standard. This is the same HL7 postal format standard referenced in C-CDA Release 2.1; and QRDA is based on the same underlying standard as C-CDA (i.e., the CDA). While we continue to analyze the USPS address standard[89] and other industry standards, we believe these standards were developed for other use cases (such as the shipping and delivery of mail or tracking medical products) than for querying for health information in the health care industry. We see a need for continued industry work to determine

[87] http://perspectives.ahima.org/wp-content/uploads/2014/12/PatientMatchingAppendixA.pdf
[88] http://www.gs1.org/gln
[89] http://pe.usps.gov/cpim/ftp/pubs/Pub28/pub28.pdf

the appropriateness of existing standards and tools for normalizing postal address for health care uses cases, and intend to work with stakeholders in this space.

Testing and validation to the HL7 postal format in the QRDA standard is already available as part of Cypress testing[90] to QRDA for the 2014 Edition CQM certification criteria. We anticipate the Cypress testing tool for 2015 Edition CQMs criteria, including for CQM filtering, will carry over this testing and suggest that health IT developers and implementers adhere to the guidance in the QRDA Category I and III standards adopted for this criterion for the HL7 postal format. We believe it is best left to health IT developers and providers to work together to determine how to provide results for queries for patient seen at a particular practice site address at this point in time, and note that testing and certification will only test that a Health IT Module is able to filter CQM results by practice site address. Other programs that may require the use of this certification criterion may provide additional guidance on the definition of practice site address and guidance on attribution.

Comments. Commenters supported the Public Health Data Standards Consortium Source of Payment Typology Code Set[91] for representing patient insurance. SDOs such as ANSI X12 and HL7 recognize the Source of Payment Typology Code Set for representing patient insurance in their standards.[92]

Response. We have adopted the Public Health Data Standards Consortium Source of Payment Typology Code Set Version 5.0 (October 2011) to represent patient insurance for this criterion.

---

[90] http://projectcypress.org/ Cypress is the testing tool used to test and certify products for CQMs in the ONC Health IT Certification Program.
[91] http://www.phdsc.org/standards/pdfs/SourceofPaymentTypologyVersion5.0.pdf
[92] http://www.phdsc.org/standards/payer-typology.asp

Comments. Commenters expressed concern over the value set proposed to represent patient sex.

Response. We address the value set for patient sex in the "demographics" certification criterion discussed in section III.A.3 of this preamble, to which we refer readers. As noted above and recommended by commenters, we have adopted the same standard for this criterion as for the "demographics" certification criterion, which supports alignment and consistency.

Comments. Commenters expressed concern about the proposed requirement to filter all 900+ race and ethnicity codes in the "Race & Ethnicity – CDC" code system in PHIN VADS.

Response. We addressed the comments about the CDC Race and Ethnicity code set in the "demographics" certification criterion discussed elsewhere in this section of the preamble, to which we refer readers. We continue to believe in the value of querying by granular patient race and ethnicity for identification of health disparities and supporting a provider in delivering more effective care to sub-groups of their patients. As noted above and recommended by commenters, we have adopted the same standard for this criterion as for the "demographics" certification criterion, which supports alignment and consistency.

Comments. Commenters expressed concern on the level of complexity for filtering by SNOMED CT® codes for patient problem list.

Response. We acknowledge commenters' concerns about the level of complexity of filtering by SNOMED CT® codes for this certification criterion. To lessen the burden while continuing to provide value for quality improvement, we clarify that for testing and certification, a Health IT Module would only need to demonstrate it can filter by the parent level code in SNOMED CT® as the code system is designed in a hierarchical manner with more specific codes grouped under more general parent codes.

Comments. One commenter suggested we consider adding the CMS Certification Number (CCN) as an additional data element for this criterion as it is used by hospitals to report their CQM data to CMS.

Response. We thank the commenter for the suggestion. At this current point in time, we believe there are complexities with using the CCN as a filter for CQMs. For example, a certified Health IT Module may be certified partway through a reporting year. The CCN also represents a unique combination of certified Health IT Modules a provider is using to meet the CEHRT definition requirements. Thus, we are not clear on the use case that would be served in requiring a Health IT Module certified to this criterion to be able to filter CQM results by CCN. We will consider the use cases and implementation of using CCN for CQM filtering for the potential expansion of this criterion through future rulemaking.

- Authentication, Access Control, and Authorization

2015 Edition Health IT Certification Criterion § 170.315(d)(1) (Authentication, access control, and authorization)

We proposed to adopt a 2015 Edition "authentication, access control, and authorization" certification criterion that was unchanged in comparison to the 2014 Edition "authentication, access control, and authorization" criterion (§ 170.314(d)(1)).

Comments. Commenters were generally supportive of this criterion as proposed. One commenter suggested that we track the National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative and the NSTIC Trustmark Framework pilot. One commenter was supportive of us adopting standards for multi-factor authentication for remote authentication to EHR systems, whereas another commenter pointed out that current approaches to multi-factor authentication are costly and burdensome to implement. One commenter discussed digital signatures as they relate to the authenticity of medical documentation.

Response. We have adopted this certification criterion largely as proposed. We have made one minor revision by replacing the term "person" in the criterion with "user." This revision is consistent with our use of the term "user" in the 2015 Edition. We note that, notwithstanding this revision, this criterion remains eligible for gap certification.

In response to comments on multi-factor authentication, we have not adopted multi-factor authentication as part of this criterion or in another criterion or requirement as we did not propose such functionality. We will, however, continue to track NSTIC. We will also monitor industry progress with multi-factor authentication and may consider multi-factor authentication certification for a future rulemaking as noted in our discussion of the HITSC recommendations below.

Digital signatures were proposed as part of the "electronic submission of medical documentation" criterion, but were not proposed as part of this criterion. Accordingly, we have not adopted such a requirement as part of this criterion. We may, however, consider digital signatures as part of a future rulemaking.

HITSC Recommendations

We received recommendations from the HITSC after the close of the public comment period for the Proposed Rule. The HITSC recommended the adoption of a certification criterion that would include capabilities to "continuously protect the integrity and confidentiality of information used to authenticate users." The HITSC stated that the adoption of such a criterion would strengthen the authentication capabilities in currently certified health IT. The HITSC also recommended the adoption of a certification criterion for multi-factor authentication. These recommendations for the adoption of certification criteria must proceed through the processes outlined in sections 3001 and 3004 of the Public Health Service Act (HITECH Act), which may

lead to a future rulemaking proposing the adoption of criteria that include capabilities recommended by the HITSC.

- Auditable Events and Tamper-Resistance

2015 Edition Health IT Certification Criterion § 170.315(d)(2) (Auditable events and tamper-resistance)

We proposed to adopt a 2015 Edition "auditable events and tamper-resistance" certification criterion that was unchanged in comparison to the 2014 Edition "auditable events and tamper-resistance" criterion (§ 170.314(d)(2)) and sought comment on two issues. First, given that it does not appear that the ASTM standard indicates recording an event when an individual's user privileges are changed, we asked for comment on whether we need to explicitly modify/add to the overall auditing standard adopted in 170.210(e) to require such information to be audited or if this type of event is already audited at the point of authentication (e.g., when a user switches to a role with increased privileges and authenticates themselves to the system). We also sought comments on any recommended standards to be used in order to record those additional data elements. We reiterated our policy in the 2014 Edition "auditable events and tamper resistance" certification criterion in that the ability to disable the audit log must be restricted to a limited set of users to meet this criterion, and we stated that we believe our certification criterion is appropriately framed within the parameters of what our regulation can reasonably impose as a condition of certification. With regard to feedback to the Voluntary Edition proposed rule that there may be some events recorded in the audit log that may be more critical to record than other events, we again sought comment on whether: there is any alternative approach that we could or should consider; there is a critical subset of those auditable events that we should require remain enabled at all times, and if so, additional information regarding which

events should be considered critical and why; and any negative consequences may arise from keeping a subset of audit log functionality enabled at all times.

Comments. The majority of commenters requested that this criterion remain as proposed and be eligible for gap certification. Commenters overwhelming agreed that emergency access was being audited and is already covered under the ASTM E2147 standard. Some commenters expressed support for specifically auditing user privilege changes with the HITSC TSSWG recommending that this criterion require events to be audited in accordance with NIST SP 800-92.[93]

Most commenters, including the HITSC TSSWG, recommended that there should be no change in the requirements related to disabling and enabling the audit log. A commenter noted that determining when the audit log should or should not be enabled is best defined by end-users of Health IT Modules and not the health IT developers. Commenters representing consumer organizations suggested that the audit log should not be able to be disabled, which they argued would enhance consumer trust. Another commenter stated that any allowance for disabling the audit logs, for any reason, compromises the integrity of the auditing.

Commenters did not identify a critical subset of those auditable events that we should require remain enabled at all times. However, one commenter suggested that as an alternative to requiring the audit log to always be enabled, we should provide regulatory guidance on the specific information to be included in the audit log, such as is stipulated in the ASTM E2147 standard. The commenter also recommended that we provide clarity on the scope of the applicability of the ASTM standard as a part of that guidance when it comes to whether the

[93] http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

intent is to include only natural person/end user accesses or other access such as "machine to machine."

Response. We have adopted this criterion as proposed, except that we have revised the auditing standard referenced by this criterion and adopted in § 170.210(e)(1)(i)[94] to include a requirement to audit changes in user privileges. With consideration of public comments, we believe that this is an event that should be audited for the purposes of certification. We do not, however, believe that at this time certification should expand to an extensive list of auditable events as recommended by the HITSC TSSWG. Rather, we believe that certification should remain a baseline and health IT developers and providers can expand their auditing practices as appropriate.

We did not receive an overwhelming response or rationale from commenters that convinced us to change our approach to require that a Health IT Module not permit an audit log to be disabled. In fact, comments remained mixed and the HITSC continued to support our current approach. As recited in the Proposed Rule, there are valid reasons for disabling the audit log. We continue to believe that it is appropriate to restrict the ability to disable the audit log to a limited set of users, which permits the end user to determine if, when, and by whom the audit log may be disabled. As to the alternative approach to always enabling the audit log, we note that we have chosen to maintain the current approach, but will consider as part of the finalizing of the 2015 Edition test procedure for this criterion what additional guidance we can provide related to auditable actions consistent with the ASTM E2147 standard.

- Audit Report(s)

[94] We note that the ASTM E2147 standard has been reapproved (in 2013) with no changes. We have, therefore, revised the regulation text to reflect the reapproval. http://www.astm.org/Standards/E2147.htm

2015 Edition Health IT Certification Criterion
§ 170.315(d)(3) (Audit reports)

We proposed to adopt a 2015 Edition "audit reports(s)" certification criterion that was unchanged in comparison to the 2014 Edition "audit reports(s)" criterion (§ 170.314(d)(3)).

Comments. Commenters recommended that we adopt this criterion as proposed. A couple of commenters requested that we include additional functionality in this criterion, such as a filtering functionality (beyond sorting) and automated reporting without manual searches/sorting.

Response. We have adopted this criterion as proposed. We appreciate commenters' suggested additional functionalities, but these functionalities are beyond the scope of our proposal. To note, certification serves as a baseline for health IT. We would expect health IT developers to incorporate such functionalities to possibly differentiate their products in the market or if specifically desired by their customers (e.g., providers).

- Amendments

2015 Edition Health IT Certification Criterion
§ 170.315(d)(4) (Amendments)

We proposed to adopt a 2015 Edition "amendments" certification criterion that was unchanged in comparison to the 2014 Edition "amendments" criterion (§ 170.314(d)(4)). We noted that this certification criterion only partially addresses the amendment of protected health information (PHI) requirements of 45 CFR 164.526.

Comments. Commenters supported this criterion as proposed. A commenter requested clarification as to whether amendment steps such as request, approval/denial, and updating are to be tracked as separate unique events or as a single event with a single timestamp. A couple of commenters suggested this criterion include the capability to maintain the provenance of amendments made by patients and other patient generated health data to reduce the numbers of errors.

Response. We have adopted this certification criterion as proposed. The "tracking" or auditing of events mentioned by the commenter is outside the scope of this criterion. Rather, we would expect such actions to be subject of an entity's auditing technology and practices. We appreciate the suggestion to maintain provenance of amendments made by patients and other patient generated health data, but this is outside the scope of the functionality proposed for this criterion.

- Automatic Access Time-Out

2015 Edition Health IT Certification Criterion § 170.315(d)(5) (Automatic access time-out)

We proposed to adopt a 2015 Edition "automatic access time-out" certification criterion that was unchanged in comparison to the 2014 Edition "automatic log-off" criterion (§ 170.314(d)(5)). In terms of the functionality within the criterion, we proposed to restate the language to require a Health IT Module to demonstrate that it can automatically stop user access to health information after a predetermined period of inactivity and require user authentication in order to resume or regain the access that was stopped. This proposal was based on feedback previously received from the HITSC Privacy and Security Workgroup (PSWG).[95] The PSWG noted in June 2014 that many systems are not session-based. Instead, systems may be stateless, clientless, and/or run on any device. The HITSC recommended that this certification criterion should not be overly prescriptive so as to inhibit system architecture flexibility. We agreed with the substance of the PSWG and HITSC recommendations and proposed to state the functionality required as specified above, noting that we do not believe this would have any impact on testing and certification as compared to testing and certification to the 2014 Edition "automatic log-off"

[95] http://www.healthit.gov/facas/sites/faca/files/HITSC_PSWG_2015NPRM_Update_2014-06-17.pdf. The HITSC Privacy & Security Work Group changed names and became the HITSC Transport & Security Standards Work Group in July 2014.

criterion (i.e., the 2015 "automatic access time-out" criterion would be eligible for gap certification).

Comments. Commenters expressed support for this criterion as proposed. The HITSC Transport and Security Standards Workgroup (TSSWG) again recommended that we change the language of the criterion to read "automatically terminate access to protected health information after a system- and/or administrator-defined period of inactivity, and reinitiate the session upon re-authentication of the user."

Response. We thank commenters for their support. We continue to believe that the language offered by the TSSWG prescribes a particular session-based design and is not the most appropriate language for this criterion. As mentioned above, not all systems are session-based. Therefore, we have adopted this criterion as proposed.

- Emergency Access

2015 Edition Health IT Certification Criterion
§ 170.315(d)(6) (Emergency access)

We proposed to adopt a 2015 Edition "emergency access" certification criterion that was unchanged in comparison to the 2014 Edition "emergency access" criterion (§ 170.314(d)(6)).

Comments. Commenters supported this criterion as proposed.

Response. We have adopted this criterion as proposed.

- End-User Device Encryption

2015 Edition Health IT Certification Criterion
§ 170.315(d)(7) (End-user device encryption)

We proposed to adopt a 2015 Edition "end-user device encryption" certification criterion that was unchanged in comparison to the 2014 Edition "end-user device encryption" criterion (§ 170.314(d)(7)). We proposed to require certification to this criterion consistent with the most

recent version of Annex A: Approved Security Functions (Draft, October 8, 2014) for Federal Information Processing Standards (FIPS) Publication 140-2.[96] We noted, however, that we do not believe that this would have any impact on testing and certification as compared to testing and certification to the 2014 Edition "end-user device encryption" criterion (i.e., the 2015 "end-user device encryption" criterion would be eligible for gap certification).

Comments. Many commenters expressed support for leaving the certification criterion unchanged in comparison to the 2014 Edition "end-user device encryption" criterion. Many commenters also supported our proposal for using the most recent version of Annex A as cited in the Proposed Rule.

Response. We appreciate the support expressed by many commenters. We have adopted this certification criterion as proposed, including the updated version of Annex A.

Comments. Some commenters suggested that we expanded the functionality of this criterion to include server-side encryption or encryption of data in-motion. One commenter said that data should be encrypted when using cloud storage technologies. Another commenter requested clarification if this criterion applied to data at-rest or in-motion.

Response. As described in the 2014 Edition final rule (77 FR 54236-54238), the functionality included in the 2014 Edition certification criterion (and this 2015 Edition unchanged criterion) does not focus on server-side or data center hosted technology. We recognize that these implementations could employ a variety of different administrative, physical, and technical safeguards, including hardware-enabled security protections that would be significantly more secure than software oriented encryption capabilities. Rather, this criterion focuses on data locally stored on end-user devices after the use of the technology is stopped.

[96] http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf

Comments. Some commenters stated that we should address encryption key management and key storage in this certification criterion.

Response. We agree with commenters that encryption controls depend on the encryption key remaining secure. However, this functionality is outside the scope of the proposed criterion. We also note that encryption key management often occurs outside of certified health IT and depends on the environment in which the certified health IT is deployed, and, as such, depends on organizational policy and security risk assessments. We encourage stakeholders to follow applicable guidance from the Office for Civil Rights (OCR)[97] and the National Institutes of Standards and Technology[98] for securing encryption keys.

- Integrity

2015 Edition Health IT Certification Criterion § 170.315(d)(8) (Integrity)

We proposed to adopt a 2015 Edition "integrity" certification criterion that was unchanged in comparison to the 2014 Edition "integrity" criterion (§ 170.314(d)(8)). We did, however, propose a change in how a Health IT Module would be tested and certified to this criterion. We explained that the 2015 Edition "integrity" criterion would be tested and certified to support the context for which it was adopted – upon receipt of a summary record in order to ensure the integrity of the information exchanged (see § 170.315(d)(8)(ii)). Therefore, we stated that we expect that this certification criterion would most frequently be paired with the "ToC" certification criterion for testing and certification.

[97] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html
[98] http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

We sought comment on if, and when, we should set the baseline for certification to the 2015 Edition "integrity" certification criterion at SHA–2[99]. In support of this potential change, we noted that SHA-2 has much more security strength compared to the SHA-1 standard. We also pointed out that many companies, including Microsoft and Google, plan to deprecate SHA-1 no later than January 1, 2017.

Comments. Several commenters and the HITSC expressed support for increasing the integrity standard to SHA-2. One commenter pointed out that NIST has deprecated the use of SHA-1, whereas another commenter claimed that health IT would have to eventually get recertified to SHA-2 if we moved to SHA-2 at a later date (beyond the effective date of this final rule) or in a future edition. A few commenters requested that we wait until 2017 or 2018 to increase the standard to SHA-1.

Response. In 2012, NIST Special Publication 800-57[100] recommended that federal systems not be permitted to create new hashes using SHA-1 starting in 2014. Given that NIST, technology companies, and health IT developers are moving away from SHA-1, we believe now is the appropriate time to move towards the more secure SHA-2 standard. Therefore, we will make this new requirement effective with the effective date of this final rule. We note that there is no requirement obligating health IT developers to get their products certified to this requirement immediately, and we would expect health IT developers to not begin seeking certification to this criterion until later in 2016 for implementation in 2017 and 2018. We further note that certification only ensures that a Health IT Module can create hashes using SHA-2, it does not require the use of SHA-2. For example, users of certified health IT may find it

[99] http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf
[100] http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf

appropriate to continue to use SHA-1 for backwards compatibility if their security risk analysis justifies the risk.

Consistent with this decision, we have also updated this criterion and standard to reference the most recent version of FIPS PUB 180-4, Secure Hash Standard, 180-4 (August 2015).[101]

2015 Edition Health IT Certification Criterion § 170.315(d)(9) (Trusted connection)

Please see the discussion under the "Application Access To Common Clinical Data Set" certification criteria later in this section of the preamble.

2015 Edition Health IT Certification Criterion § 170.315(d)(10) (Auditing actions on health information)

Please see the discussion under the "Application Access To Common Clinical Data Set" certification criteria later in this section of the preamble.

- Accounting of Disclosures

2015 Edition Health IT Certification Criterion § 170.315(d)(10) (Accounting of disclosures)

We proposed to adopt a 2015 Edition "accounting of disclosures" certification criterion that was unchanged in comparison to the 2014 Edition "accounting of disclosures" criterion (§ 170.314(d)(9)). We noted that the 2015 Edition criterion is no longer designated "optional" because such a designation is no longer necessary given that we have discontinued the Complete EHR definition and Complete EHR certification beginning with the 2015 Edition certification criteria.

[101] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

Comments. Commenters expressed support for this certification criterion as proposed. A commenter recommended removing the criterion until the HHS Office for Civil Rights (OCR) issues a final rule for its previously published proposed rule regarding accounting of disclosures (76 FR 31426)[102]. Other commenters recommended strengthening this criterion and specifications to enhance the ability to identify inappropriate access inside an entity or organized health care arrangement and to provide reports with sufficiently relevant data.

Response. We have adopted this certification criterion as proposed. We initially adopted an "accounting of disclosures" certification criterion to supplement HITECH Act requirements and rulemaking by OCR (75 FR 2016-17 and 75 FR 44623-24) and believe there is value in its continue adoption as proposed. We appreciate the suggested revisions offered by commenters, but believe that alignment with an "account of disclosures" final rule will provide the most certainty and useful functionality for providers, while also mitigating any health IT development and implementation burdens that may accrue through compliance with potential multiple adopted versions of this certification criterion. We believe it is most appropriate to wait and consider the provisions of an "accounting of disclosures" final rule to be issued by OCR before making any revisions to this certification criterion. As currently adopted, health IT developers have the option of pursuing certification to this criterion if they deem it advantageous.

- View, Download, and Transmit to 3rd Party

2015 Edition Health IT Certification Criterion § 170.315(e)(1) (View, download, and transmit to 3rd party)

We proposed to adopt a 2015 Edition "view, download, and transmit to 3rd party" (VDT) criterion that was revised in comparison to the 2014 Edition "VDT" criterion (§ 170.314(e)(1)).

Clarified Introductory Text for 2015 Edition VDT Certification Criterion

[102] http://www.gpo.gov/fdsys/pkg/FR-2011-05-31/pdf/2011-13297.pdf

We proposed to revise the introductory text to lead with "Patients (and their authorized representatives) must be able to use health IT to . . ." We also proposed to use this same phrase at the beginning of each specific capability for VDT to reinforce this point. We noted that this does not override or substitute for an individual's right to access protected health information (PHI) in a designated record set under 45 CFR 164.524.

Comments. Many commenters voiced support for the inclusion of "authorized representative" in the introductory text of VDT, noting that specifically granting the patient's authorized representative the ability to view/download/transmit patient health information reinforces the importance of the caregiver role on the care team and supports a vision of patient-centered care. One commenter urged us to adopt the "personal representative" term used in HIPAA.

Response. We have adopted the proposed introductory language as it clarifies that these capabilities must enable patients and their authorized representatives. We decline to use the HIPAA term "personal representative." Rather, we have adopted our proposal of "patients (and their authorized representatives)" to be consistent with the approach we have used in previous rulemakings that aligns with the use of the term under the EHR Incentive Programs. A "patient-authorized representative" is defined as any individual to whom the patient has granted access to their health information (see also 77 FR 13720). Examples would include family members, an advocate for the patient, or other individual identified by the patient. A patient would have to affirmatively grant access to these representatives with the exception of minors for whom existing local, state, or federal law grants their parents or guardians access without the need for the minor to consent and individuals who are unable to provide consent and where the state appoints a guardian (see also 77 FR 13720).

Additionally, consistent with our certification program approach to apply particular privacy and security certification criteria to a product's certification based on the scope of capabilities presented, we have determined that this certification criterion would be clearer and more focused if we were to remove the secure access language included in (e)(1)(i) in favor of having a specific privacy and security certification criterion that would be applicable to this criterion. In transitioning this text, we have also made a conforming revision to note that the "technology" used would need to be "internet-based" which we believe is a more generally applicable and innovation supportive term compared to the user of the word "online," which was part of the sentence that included the security specific language that we have removed.

Updated C-CDA and Common Clinical Data Set

We proposed to reference the updated version of the C-CDA (Draft Standard for Trial Use, Release 2.0) for the "VDT" criterion and noted that compliance with Release 2.0 cannot include the use of the "unstructured document" document-level template for certification to this criterion. We also solicited comment on whether we should limit the scope of the C-CDA document created for the purposes of this criterion to just the CCD document template. We also solicited comment on whether we should require in this criterion to permit patients and their authorized representatives to select their health information for, as applicable, viewing, downloading, transmitting, or API based on a specific date or time, a period of time, or all the information available.

Comments. Multiple commenters supported the reference to C-CDA Release 2.0 document template. Some commenters voiced concern about adoption C-CDA Release 2.0 if backwards compatibility is not fully addressed. Other commenters suggested additional information that patients may need outside of the C-CDA, including referral summaries,

discharge instructions, documents listed in the Patient Health Information Capture criterion, and nutrition and diet orders. Multiple commenters supported the focus on the creation of a CCD document template based on the C-CDA Release 2 for the "VDT" criterion, stating that it would be less confusing for consumers who may not be able to distinguish between different document types. In regard to our solicitation on time and date range functionality, multiple commenters were in support of adding such capabilities, while a few commenters did not agree with including this functionality.

Response. Consistent with our decision for the "ToC" criterion, we will reference C-CDA Release 2.1 in the "VDT" criterion. In response to public comment, we have narrowed the scope of the C-CDA document templates to only the CCD for this criterion. We emphasize that this requirement serves as a "floor" rather than a "ceiling" and that Health IT Modules and their purchasers may choose to add additional document types as appropriate for different practice and care settings.

We have included an updated Common Clinical Data Set for the 2015 Edition that includes references to new and updated vocabulary standards code sets. Please also see the Common Clinical Data Set definition in section III.B.3 of this preamble.

In consideration of public comments that focused on our comment solicitation around the addition of date and time filtering capabilities, we have decided to adopt such requirements as part of this criterion. We believe that adding this explicit functionality to the certification criterion provides specific clarity that patients should have certain baseline capabilities available to them when it comes to selecting the data (or range of data) they wish to view, download, or transmit. Specifically, we have adopted within this criterion two timeframe filters that patients must be able to select and configure on their own. The first would ensure that a patient can select

data associated with a specific date (to be viewed, downloaded, or transmitted) and the second would ensure that the patient could select data within an identified date range (to be viewed, downloaded, or transmitted), which must be able to accommodate the patient selecting a range that includes all data available to them. We also clarify that we are not including the ability to select a specific data element category as part of this requirement, but reiterate that these requirements represent a floor rather than a ceiling, and health IT developers may choose to add other functionalities as appropriate. The technology specifications should be designed and implemented in such a way as to provide maximum clarity to a patient (and their authorized representative) about what data exists in the system and how to interpret it, and we expect that health IT developers will make choices following design and usability best practices that will make it easier and clearer for patients to find and use their records.

Diagnostic Image Reports

We proposed to require that a Health IT Module would need to demonstrate that it can make diagnostic image reports available to the patient in order to be certified. We explained that a diagnostic image report contains a consulting specialist's interpretation of image data, that it is intended to convey the interpretation to the referring (ordering) physician, and that it becomes part of the patient's medical record.

Comments. Commenters were generally supportive of including diagnostic image reports and associated context in the "VDT" criterion. Some commenters requested clarification on where this data would be accessible within the C-CDA.

Response. We have adopted this proposal to include the diagnostic imaging report (including the consulting specialist's interpretation) as a requirement in the "VDT" criterion.

Health IT Modules may include this information in the "Results" section of the CCD. We clarify that unstructured data for the interpretation text is acceptable.

VDT – Application Access to Common Clinical Data Set

We have addressed all comments on this proposed provision under the "Application Access to Common Clinical Data Set" in this section of the preamble.

Activity History Log

We proposed to include "addressee" as a new data element in the 2015 Edition "VDT" criterion related to the activity history log. In the Proposed Rule, we noted that this transactional history is important for patients to be able to access, especially if a patient actively transmits his or her health information to a 3rd party or another health care provider.

Comments. Commenters were generally supportive of this new data element. One commenter suggested that we not include transmission status in the final rule because few patients actually transmit.

Response. We have adopted the new data element of "addressee" as part of the VDT criterion. While fewer patients may currently use "transmit" than "view" or "download," we anticipate that more patients will use this functionality in the future and that this information will be helpful for transaction history.

Patient Access to Laboratory Test Reports

In the Proposed Rule, we noted recent regulatory changes addressing the intersection of the CLIA rules, state laws governing direct patient access to their laboratory test reports, and the HIPAA Privacy Rule. These regulatory changes converged in a final rule that permits a patient, or his or her "personal representative," as applicable, to request a copy of the patient's completed test reports directly from the laboratory or to request that the test results be transmitted to a

designated person. To ensure fidelity of such reports regardless of the system delivering laboratory results to a patient, we proposed that a Health IT Module presented for certification to this criterion must demonstrate that it can provide laboratory test reports that include the information for a test report specified in 42 CFR 493.1291(c)(1) through (7); the information related to reference intervals or normal values as specified in 42 CFR 493.1291(d); and the information for corrected reports as specified in 42 CFR 493.1291(k)(2).

Comments. One commenter suggested that this requirement be removed until the C-CDA specification supports the requisite CLIA data referenced in the Proposed Rule. Another commenter noted that some laboratory results require provider annotation and/or follow up testing before they can be released to the patient to avoid harm, particularly with certain sensitive tests such as HIV tests. Thus, a laboratory result awaiting provider annotation may not be fully "available" until the annotation is complete.

Response. We have adopted the proposed laboratory test reports requirement for the VDT criterion. We note that the C-CDA can support this information in a structured way using the "Result Observation Template" in the "Results" section. We recommend that health IT developers follow the best practices for use of these C-CDA templates as outlined by HL7 (see, e.g., HL7 Task Force Examples: http://wiki.hl7.org/index.php?title=CDA_Example_Task_Force). Further, we strongly recommend an approach favoring coded data where possible and appropriate, and anticipate that future certification editions will require more extensively coded data.

Web Content Accessibility Guidelines (WCAG)

We proposed to modify the regulatory text hierarchy at § 170.204(a) to designate the WCAG 2.0 Level A (Level A) conformance at § 170.204(a)(1) instead of § 170.204(a). This

would also require the 2014 Edition "VDT" certification criterion to be revised to correctly reference § 170.204(a)(1). We also sought comment on whether we should adopt WCAG 2.0 Level AA (Level AA) conformance requirements for the "view" capability included in the 2015 Edition VDT criterion, instead of the current Level A.

Comments. Many commenters representing the patient advocate community supported the increase to Level AA; additionally, the U.S. Access Board noted that other federal agencies and programs are moving toward Level AA. Other commenters said that Level A conformance was sufficient and that level AA is not needed and overly burdensome.

Response. We have adopted and retained the Level A requirement for this criterion. However, we have included Level AA as an optional component of this certification criterion via an "or" in the certification criterion so that if a developer so chooses it can demonstrate that a Health IT Module can meet Level AA. We reiterate that the "or" does not mean that a technology would need to meet both levels. At a minimum it would need to meet Level A. We note that such information would be listed with the product as part of its Certified Health IT Product List (CHPL) listing. We believe this option adds transparency to what capabilities products include and can better inform purchasers. We have adopted Level AA as a standard at § 170.204(a)(2). Additionally, we have determined that the certification criterion's requirements for the application of WCAG would be clearer if it were expressed in the general requirement at the paragraph 170.315(e)(1)(i) since WCAG needs to apply to all user viewable functionality and would equally apply to and include the user experience aspects of download and transmit.

"Transmit" Request for Comment

We requested comment on (1) whether we should include the Direct Project's Implementation Guide for Direct Project Trust Bundle Distribution specification as part of

certification for the "VDT" certification criterion; and (2) whether any additional requirements are needed to support scalable trust between Security/Trust Agents (STAs) as well as ways in which we, in collaboration with other industry stakeholders, could support or help coordinate a way to bridge any gaps.

Comments. One commenter noted that the proposed inclusion of the Direct Project's Implementation Guide for Trust Bundle Distribution will be confusing because most of the Direct Project IG for the trust bundle focuses on creating a trust bundle, not consuming it. The commenter recommended pointing developers to Section 3.0 Trust Bundle Requestors for additional guidance, and that we support participation in existing trust communities such as the National Association for Trusted Exchange (NATE). Another commenter recommended that we require EHR and HISP vendors to preload all Blue Button Patient Trust Bundles into their systems so providers using these systems can transmit records using the Direct protocol.

Response. Our intent is to ensure that an individual who wants to transmit his or her health information to a third party has options to be able to do so, and those options should be easy and convenient. Individuals who are more concerned about sharing their data in transit can choose a more secure, simple option for transmitting this information. To provide greater flexibility for patients to effectively use the "transmit" capability and to ensure that patients have an easy and near universal ability to send their health information to a destination they select, we have adopted a more flexible approach for testing and certifying "transmit" as part of this certification criterion. In order to satisfy this portion of the certification criterion a Health IT Module must demonstrate two forms of transmission:

1) Email transmission (of a CCD) to any email address[103]; and

2) An encrypted method of electronic transmission.

This approach will provide patients with a readily understood and convenient option to simply send their health information via email. Patients, under current HIPAA regulations[104], may presently ask that data be disclosed to them via unencrypted email. Therefore, including email as an option for transmission capabilities is consistent with HIPAA as well as with common communications for other purposes. We also provide and encourage an encrypted option for transmitting their health information if they prefer or need to transmit their data with added security. There is a heightened interest in security of information in transit and at rest across all industries. As such, we encourage developers to provide innovative options for individuals to easily and efficiently protect their health information based on generally available mechanisms for security and new advances in this area. In either case—whether by email or an encrypted method—the goal is to support patients in transmitting their health information on demand to a third party of their own choice. We note that, for certification, the encrypted method would be subject to the 2015 Edition privacy and security certification framework, particularly the "trusted connection" certification criterion. We refer readers to section IV.C.1 ("Privacy and Security") of this preamble for further discussion of the 2015 Edition P&S certification framework and to the "application access to Common Clinical Data Set" section of this preamble for more information of the "trusted connection" certification criterion.

In adding flexibility to this portion of the certification criterion, the other proposals and topics on which we sought comment are moot. However, we wish to reiterate that for the

[103] Please see the OCR frequently asked questions for best practices regarding the use of email for transmitting health information: http://www.hhs.gov/ocr/privacy/hipaa/faq/health_information_technology/570.html
[104] 45 CFR 164.524 and related guidance

purposes of meeting the second form of transmission, the Direct protocol is an encouraged and viable method, especially since health IT developers have already been certified to this functionality for the purposes of 2014 Edition certification, and will also be certified to this functionality as part of 2015 Edition certification to support transitions of care requirements through the 2015 Edition "ToC" criterion. Additionally, we clarify that with respect to the second method, health IT developers have the flexibility to either establish an encrypted connection between two end points or, alternatively, secure the payload via encryption. In other words, we make no presumption and do not imply through the language in the second method that only one approach will satisfy testing and certification.

C-CDA Data Provenance Request for Comment

We refer readers to our response to this request for comment under the "ToC" criterion.

- Secure Messaging

2015 Edition Health IT Certification Criterion § 170.315(e)(2) (Secure messaging)

We proposed to adopt a 2015 Edition "secure messaging" certification criterion that was unchanged in comparison to the 2014 Edition "secure messaging" criterion (§ 170.314(e)(3)).

Comments. The majority of commenters supported this criterion as proposed. Some commenters suggested additional functionality for this criterion, including the ability to track responses to patient-generated messages, support languages other than English, and other forms of communication including audio, video, or images. A few commenters questioned whether patients' devices would need to be secure and encrypted, and whether the encryption criteria would only apply to the message content. A commenter recommended that health IT developers should have to preload trust bundles. Another commenter suggested that health IT developers should be prohibited from charging significant add-on fees for secure messaging. Another

commenter recommended that in-the-field surveillance is needed to ensure that health IT developers and providers were enabling this functionality. A commenter listed several issues associated with the EHR Incentive Programs Stage 3 objective and measure related to secure messaging, including the lack of a routine secure messaging use case for eligible hospitals and CAHs, that only certain types of secure messages would count, that the API alternative might drive down secure messaging using certified health IT, and that measurement should be based on those patients who "opt in." This same commenter also suggests that if the CMS proposal is adopted, the criterion should clearly define exclusion criteria.

Response. We have adopted this criterion with modification. We have removed the specific security requirements out of the criterion because the appropriate privacy and security (P&S) requirements will be applied through the 2015 Edition P&S certification framework finalized in this final rule. To clarify, a Health IT Module certified to this criterion will still need to demonstrate the same security requirements as included in the proposed criterion (patient/user authentication and encryption and integrity-protection), but there will be more flexibility in that a health IT developer can choose between message-level or transport level certification in accordance with § 170.315(d)(9). Certification to this criterion will also require certification to other privacy and security criteria under the P&S certification framework, including automatic log-off (§ 170.315(d)(5)) and the auditing criteria (§ 170.315(d)(2) and (3)). Our revisions to the criterion and approach are consistent with our overall approach to applying the appropriate privacy and security certification requirements to each 2015 Edition certification criterion. We refer readers to section IV.C.1 ("Privacy and Security") of this preamble for further discussion of the 2015 Edition P&S certification framework, including specific application of the P&S

certification framework to a Health IT Module presented for certification to the "secure messaging" criterion in conjunction with other certification criteria.

This criterion is no longer eligible for gap certification as the new hashing standard (a hashing algorithm with a security strength equal to or greater than SHA-2) applies to this criterion.

We appreciate the suggested additional functionalities for inclusion in this criterion (tracking responses, use of languages beyond English, and other forms of communication, and preloaded trust bundles), but the functionalities are beyond the scope of our proposal. We will consider these additional functionalities for a future edition of this criterion. We clarify in this final rule that the encryption requirements only apply to the message content and not to patients' devices.

We cannot prescribe the fees health IT developers charge for their certified health IT, but note that our transparency provisions (§ 170.523(k)) require ONC-ACBs to ensure that health IT developers make public the types of costs they charge to enable certified health IT. ONC-ACBs also conduct surveillance of certified health IT under the ONC Health IT Certification Program to ensure that health IT continues to function as initially certified. Surveillance can be initiated randomly or in response to complaints.

For concerns and questions related to the EHR Incentive Programs, we refer readers to CMS and the EHR Incentive Programs Stage 3 and Modifications final rule published elsewhere in this issue of the **Federal Register**. We note that health IT certified to certification criteria that support percentage-based measures under the EHR Incentive Programs (i.e., this criterion) must also be able to record, at a minimum, the numerator for that measure per the CEHRT definition

requirements and the "meaningful use measurement calculation" certification criteria (§ 170.315(g)(1) and (g)(2)).

- Patient Health Information Capture

2015 Edition Health IT Certification Criterion § 170.315(e)(3) (Patient health information capture)

In following the HITSC recommendation for Health IT Module functionality to store an advance directive and/or include more information about the advance directive, we proposed a 2015 Edition "patient health information capture" certification criterion that would "replace" the 2014 Edition "advance directives" certification criterion (§ 170.314(a)(17)) and apply to various patient health information documents. We stated that a Health IT Module would need to enable a user to: (1) identify (e.g., label health information documents as advance directives and birth plans), record (capture and store) and access (ability to examine or review) patient health information documents; (2) reference and link to patient health information documents; and (3) record and access information directly and electronically shared by a patient.

We received general comments and comments on each of the capabilities included in the proposed criterion. We have divided and responded to the comments in a similar manner.

Comments. Commenters expressed general agreement with this criterion, with broad support across health IT developers, providers, consumers, and various advocacy groups. Commenters stated that this functionality could support addressing health disparities in populations that are less likely to execute healthcare planning documents or provide health information to providers.

Response. We thank commenters for their feedback. We have adopted this criterion as proposed with the revisions and clarifications specified below. As adopted, we anticipate health IT developers will develop innovative and efficient ways to meet this criterion and

simultaneously support providers accepting health information from patient.

Identify, Record, and Access Information Documents

Comments. Commenters universally supported this proposed provision.

Response. We thank commenters for their support. We have adopted the capabilities of this provision (identify, record, and access information documents) by combining them with the proposed provision of this criterion that included capabilities to record and access information directly and electronically shared by a patient. The capabilities to identify, record, and access patient health information documents are essentially a subset of the capabilities to record and access information directly and electronically shared by a patient, except for the proposed "identification" capability. Therefore, we have specifically retained the "identification" capability, while merging the other capabilities to finalize a provision that requires health IT to enable a user to identify, record, and access information directly and electronically shared by a patient (or authorized representative).

Reference and Link Documents

Comments. Most commenters supported this requirement, while some commenters did not agree that there was value in linking documents and others expressed security concerns. A commenter stated that a link could require additional log in credentials. A few commenters also expressed concerns regarding a system's need to capture information from any external internet site, stating that a patient (intentionally or unintentionally) could provide a URL to the provider that contained a virus.

Response. The criterion focuses solely on the ability of the Health IT Module to be able reference (providing narrative information on where to locate a specific health information document) and link to patient health information. "Linking," as described in the Proposed Rule,

requires a Health IT Module to demonstrate it could link to an internet site storing a health information document. While an intranet link to a health information document might suffice for provider use, a Health IT Module will still need to demonstrate the ability to link to an external site via the internet for the purposes of certification. The requirement of this provision does not go beyond this specified functionality.

This criterion is subject to the 2015 Edition privacy and security (P&S) certification framework adopted in this final rule. In this regard, a Health IT Module certified to this criterion would also need to be certified to the P&S certification criteria in § 170.315(d)(1) (authentication, access control, and authorization), (d)(2) (auditable events and tamper resistance), (d)(3) (audit reports), (d)(4) (amendments), (d)(5) (automatic log-off), and (d)(9) (trusted connection).[105] We believe these certification criteria and included capabilities will assist a provider in protecting its health IT system against potential security concerns. However, we note that certification is a baseline. Health IT developers and providers have the discretion to both determine what types of security features should be implemented (e.g., multi-factor authentication) with the functionality included in this criterion and whether to accept specific electronic information from a patient, such as a URL.

Record and Access Information Directly Shared by a Patient

Comments. Many commenters expressed support for this provision, including not specifying standards for compliance. A few commenters requested we identify standards or ensure compatibility with other standards such as the C-CDA or Direct messaging protocol. Most commenters sought clarification of this requirement. A couple of commenters suggested we drop this provision. A few commenters requested to know if this criterion was intended to directly

[105] We refer readers to section IV.C.1 ("Privacy and Security") of this preamble for further discussion of the 2015 Edition P&S certification framework.

support the proposed EHR Incentive Programs Stage 3 objective and measure regarding patient-generated health data and what types of patient health information was contemplated by this criterion. A commenter suggested making this functionality a separate criterion.

Response. The intent of this provision is to establish at least one means for accepting patient health information directly and electronically from patients in the most flexible manner possible. This approach means focusing on functionality and not standards. Further, we do not believe there are appropriate standards that we could adopt that cover all the conceivable use cases.

This criterion was specifically included in the CEHRT definition to ensure, at a minimum, providers participating in the EHR Incentive Programs had this capability. While it could potentially be used to support the Stage 3 objective and measure regarding patient-generated health data, it was not proposed with the intention of it being the only means available for meeting the Stage 3 objective and measure. Rather, the goal was to set a foundation for accepting information directly from patients.

We do not seek to define the types of health information that could be accepted as we believe this should be as broad as possible. The types of health information could be documents as described in the Proposed Rule (e.g., advance directive or birth plans) or health information from devices or applications. The devices and applications could include home health or personal health monitoring devices, fitness and nutrition applications, or a variety of other devices and applications. In addition, patient health information could be accepted directly and electronically through a patient portal, an API, or even email.

We have determined that it is most appropriate to keep all the functionality in one criterion and combine capabilities as noted above. We emphasize that it is always possible to have multiple technologies certified together as a one "Health IT Module" to meet this criterion.

We note that we intend for "patient" to be interpreted broadly to include an authorized representative. For clarity, we have specified this intent in regulation.

- Transmission To Immunization Registries

2015 Edition Health IT Certification Criterion § 170.315(f)(1) (Transmission to immunization registries)

We proposed to adopt a 2015 Edition "transmission to immunization registries" certification criterion that was revised in comparison to the 2014 Edition "transmission to immunization registries" criterion (§ 170.314(f)(2)). To note, we have structured the comments we received and our responses based on the specific proposed provisions of this criterion.

Comments. Most commenters supported the proposed criterion. Many commenters noted the value of the proposed criterion to bi-directional data exchange of immunization data, which was not supported by the functionality included in the 2014 Edition "transmission to immunization registries" criterion. Commenters also noted the importance of NDC and CVX codes, but expressed concern regarding issues with NDC codes as discussed in more detail below. One commenter suggested that intermediaries should be able to play a role, such as transformation of the data, in the transmission of immunization data and that only one system in the process of moving the immunization information from sender to public health agency should be required to be certified. Another commenter requested clarification if the criteria would be part of the Base EHR definition.

Response. We appreciate the support for the proposed certification criterion. We have adopted this certification criterion as proposed, but with an update to the proposed IG and the

clarifications in response to comments discussed in detail below. We clarify for commenters that any health IT can be certified to this criterion if it can meet all the requirements of the criterion, which include context exchange and vocabulary standards but do not specify a transport standard or mechanism. We further clarify that this criterion is not included in the 2015 Edition Base EHR definition, but would support meeting one of measures under the public health objective of the EHR Incentive Programs Stage 3.

Implementation Guide for Transmission to Immunization Registries

We proposed to adopt the CDC's updated implementation guide for immunization messaging, HL7 Version 2.5.1: Implementation Guide for Immunization Messaging, Release 1.5 (October 2014) ("Release 1.5"). We explained that the updated IG promotes greater interoperability between immunization registries and health IT systems, addresses issues from the previous release, and revises certain HL7 message elements to reduce data element recording differences between states and public health jurisdictions.

Comments. The majority of commenters supported adoption of Release 1.5, acknowledging that it resolves known issues in the previous release and offers improved support for standard data transmission. Some commenters noted that Release 1.5 includes references to the CDC Race and Ethnicity code set for purposes of the exchange of race and ethnicity data--which is more granular regarding race and ethnicity options for reporting when compared to the OMB standards. These commenters asked for clarification of the required use of aggregated OMB standard values.

Response. We appreciate the support for Release 1.5. We note that the CDC has issued an addendum to Release 1.5.[106] The addendum consolidates the IG information that clarifies the

[106] http://www.cdc.gov/vaccines/programs/iis/technical-guidance/hl7.html

conformance requirements, but does not specify additional substantive requirements. The addendum also provides value set requirements, general clarifications, and errata. The errata provides corrections to the length, data type, data type descriptions, usage, cardinality and/or value sets for various message elements, as well as corrections to, and addition of, conformance statements where they were mistakenly omitted. The addendum also includes clarifications to use of coding systems and value sets, additional examples of sending multiple forecast recommendations in a single message, usage of particular message elements (including those in the ORC and RXA segments), and updates to the value sets for patient eligibility status and vaccine funding source. We believe that Release 1.5 and the addendum are important components to advancing public health reporting and interoperability. We, therefore, have adopted HL7 Version 2.5.1: Implementation Guide for Immunization Messaging, Release 1.5 (October 1, 2014) and HL7 Version 2.5.1: Implementation Guide for Immunization Messaging, Release 1.5, Addendum (July 2015) for the transmission to immunization requirement. We clarify that to meet this criterion, health IT must comply with all mandatory requirements of Release 1.5 and its addendum, which would include the coding for race and ethnicity. The 2015 Edition "demographics" criterion and Common Clinical Data Set requirements related to race and ethnicity are not implicated by this criterion.

National Drug Codes for Administered Vaccinations

We proposed to require for certification that a Health IT Module be able to electronically create immunization information for electronic transmission to immunization registries using NDC codes for vaccines administered (i.e., the National Drug Code Directory – Vaccine Codes, updates through January 15, 2015[107]). For historical vaccines, we proposed to continue the use of

[107] http://www2a.cdc.gov/vaccines/iis/iisstandards/ndc_tableaccess.asp

CVX codes and proposed to adopt the HL7 Standard Code Set CVX—Vaccines Administered, updates through February 2, 2015[108] as the baseline version for certification to the 2015 Edition.

We solicited comment on whether we should allow use of NDC codes for administered vaccines as an option for certification, but continue to require CVX codes for administered vaccines for the 2015 Edition. We also solicited comment on whether we should require CVX plus the HL7 Standard Code Set MVX - Manufacturers of Vaccines Code Set (October 30, 2014 version)[109] as an alternative to NDC codes for administered vaccines, and we sought feedback on the implementation burden for health IT developers and health care providers related to requiring CVX plus MVX codes versus NDC codes for administered vaccines.

Comments. The majority of commenters supported the use of NDC codes for administered vaccines and CVX codes for historical vaccines. Commenters stated that using NDC codes for administered vaccines is valuable because NDC codes provide more granular data than CVX codes, which can improve patient safety. Comments also stated that adopting NDC for administered vaccines aligns with on-going industry efforts related to vaccine data capture.

Some commenters suggested that mapping NDC codes to CVX could be burdensome for health IT developers and immunization registries, especially for a multiple component vaccine. Commenters noted that NDC codes are subject to change and codes are added and changed more frequently than CVX and MVX codes. Commenters further noted that the reuse of NDC codes by FDA can present difficulties regarding the transmission of immunization data using such codes. One commenter requested clarification on when NDC and CVX codes are required and

[108] http://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=cvx
[109] http://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=mvx

noted the importance of clear requirements by states when NDC, CVX, or both codes would be needed.

Response. We appreciate commenters support for the use of NDC codes for administered vaccines and CVX codes for historical vaccines. For the purposes of administered vaccines, when an immunization is reported at the time it is administered and the actual product is known, the NDC code must be sent. We clarify that for when sending historical vaccines and the actual NDC code is not available, CVX codes can be sent as this method would be supported by health IT certified to this criterion. We understand the concerns regarding ensuring that the appropriate amount of information is available for immunizations and the concern regarding mapping between NDC and CVX for purposes of reporting. Therefore, we finalize a criterion that supports one set of codes to be used for administered vaccines at all times and another set of codes to be used for historical vaccines at other times. Therefore, we have adopted the August 17, 2015 version of the CVX code set as the minimum standards code set for historical vaccines. For purposes of administered vaccines, we have adopted the National Drug Codes (NDC) – Vaccine NDC Linker, updates through August 17, 2015 as the minimum standards code set. We refer readers to section III.A.2.c ("Minimum Standards" Code Sets) for further discussion of our adoption of minimum standards code sets and our decision to adopt these versions.

Immunization History and Forecast

We proposed that a Health IT Module would need to enable a user to request, access, and display a patient's immunization history and forecast from an immunization registry in accordance with Release 1.5. We requested comment on whether we should include an immunization history information reconciliation capability in this criterion and the factors we should consider regarding the reconciliation of immunization history information. We explained

that we believe that bidirectional exchange between health IT and immunization registries is important for patient safety and improved care. Immunization registries can provide information on a patient's immunization history to complement the data in the health IT system. We noted that immunization registries also provide immunization forecasting recommendations according to the Advisory Committee on Immunization Practices (ACIP)'s recommendations. This information allows for the provider to access the most complete and up-to-date information on a patient's immunization history to inform discussions about what vaccines a patient may need based on nationally recommended immunization recommendations.

Comments. Many commenters recognized the benefit of bi-directional data exchange to patient safety and population health, but some commenters expressed concern. Commenters primarily expressed concern that immunization registries were not ready for bi-directional data exchange. Other commenters, however, noted that 28 Immunization Information Systems(IIS) (which, according to the commenter, represents about 52% of reporting systems) have notified the CDC of their query capabilities in production today using HL7 2.5.1. The commenter noted that the proportion would likely rise to near 100% by 2018. A few commenters questioned the utility of the ability to query a state registry.

Many commenters also expressed concern regarding reconciliation of forecasting data. One commenter noted that we should permit innovation to occur by not prescribing the workflows related to reconciliation. Another commenter noted that where bi-directional exchange is already in production, several different workflows exist within health IT products for reconciliation of immunization history.

Commenters expressed support for vaccine forecasting, but many commenters also stated that incorporating a forecast from an immunization registry into a health IT system could be

difficult. Other commenters noted that some products already have forecasting functions, such as CDS functions for forecasting immunizations and, by association with forecasting, more complete data for allergies and contraindications.

Response. We have adopted the requirement for a Health IT Module to enable a user to request, access, and display a patient's immunization history and forecast from an immunization registry in accordance with the Release 1.5 IG. We note that this criterion and its included capabilities are designed and focused on health IT, such as EHRs. In this regard, the goal is that health IT is certified to the criterion and its included capabilities (e.g., the Release 1.5 IG). Providers who adopt health IT certified to this criterion would then have the capabilities to meet requirements under the EHR Incentive Programs or query an IIS.

While we agree with commenters that some health IT (e.g., EHR products) may sometimes have a version of the immunization history or a version of the forecast that may differ from the immunization registry, we still believe that it is important for an EHR to receive the history and forecast from the registry. Based on compliance with the Release 1.5 IG, a user would be able to see and compare the forecast from the certified health IT (e.g., EHR products) with the forecast from the immunization registry. However, we note that this criterion does not prescribe a particular workflow or reconciliation requirements. Providers and health IT developers may reconcile forecast and history information in a manner that best meets their needs for workflow and patient safety.

- Transmission To Public Health Agencies – Syndromic Surveillance

2015 Edition Health IT Certification Criterion
§ 170.315(f)(2) (Transmission to public health agencies – syndromic surveillance)

We proposed to adopt a 2015 Edition certification criterion for transmission of syndromic surveillance to public health agencies that was revised in comparison to the 2014 Edition version

(§ 170.314(f)(3)) for the inpatient setting. We noted, however, that this proposed certification criterion is unchanged (for the purposes of gap certification) for the ambulatory setting. Given the varied adoption of methods for transmitting syndromic surveillance information to public health agencies from ambulatory settings, we proposed to continue to distinguish between ambulatory and emergency department, urgent care, and inpatient settings.

Comments. Commenters expressed support for distinguishing ambulatory settings from emergency department, urgent care and inpatient settings, especially given the variations in data requirements and readiness for data acceptance among the states. A commenter also noted that the distinction was appropriate because ambulatory systems are still evolving. Some commenters requested clarification of exclusions, active engagement, and other requirements to meet the syndromic surveillance measure under the EHR Incentive Programs.

Response. We appreciate the support offered by commenters and agree that it is appropriate to distinguish between settings. For questions related to the EHR Incentive Programs, we refer readers to CMS and the EHR Incentive Programs Stage 3 and Modifications final rule published elsewhere in this issue of the **Federal Register**.

Emergency Department, Urgent Care, and Inpatient Settings

We proposed to adopt the PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent Care, Inpatient and Ambulatory Care Settings, Release 2.0, September 2014 ("Release 2.0"), due to its improvements over previous versions.

Comments. The majority of commenters supported the proposed IG. One commenter suggested that, due to state variability, a standard should not be referenced until at least 75% of states are committed to the use of a common standard. Other comments noted that Release 2.0 is the standard used by all states accepting hospital-based syndromic surveillance data. A

commenter suggested that laboratory information be removed as required from the IG as states already collect this information under electronic laboratory reporting. One commenter suggested that there was a potential discrepancy between OMB value sets for race and ethnicity and the CDC Race and Ethnicity referenced code set in the IG. Another commenter asked for clarification of the "message frequency requirement of syndromic messages," noting that the requirements within Release 2.0 may be burdensome for health IT developers. A commenter requested that certification include optional data elements within the IG.

Response. We appreciate the overall support for this criterion and the Release 2.0 IG. The CDC has recently published an updated version of the IG (April 21, 2015)[110] that reflects work to correct errors and clarify ambiguities that were present in the proposed version (dating back to Release 1.0) as well as provide missing information. The CDC also recently published an addendum to the IG, titled "Erratum to the CDC PHIN 2.0 Implementation Guide, August 2015; Erratum to the CDC PHIN 2.0 Messaging Guide, April 2015 Release for Syndromic Surveillance: Emergency Department, Urgent Care, Inpatient and Ambulatory Care Settings" ("Erratum").[111] The Erratum consolidates Release 2.0 information and clarifies existing conformance requirements of the IG. For example, it specifies conformance statements and conditional predicates that clarify message requirements. It also specifies value set requirements, provides general clarifications, and PHIN MG corrections. Overall, the April 21, 2015, updated version and the addendum do not create additional substantive requirements in comparison to Release 2.0. Rather, through the corrections, clarifications, and additional information the IG will improve testing, certification, implementation, and interoperability. Therefore, we have adopted this criterion with both the April 21, 2015, updated version and addendum.

[110] http://www.cdc.gov/nssp/documents/guides/syndrsurvmessagguide2_messagingguide_phn.pdf
[111] http://www.cdc.gov/nssp/documents/guides/erratum-to-the-cdc-phin-2.0-implementation-guide-august-2015.pdf

We believe that the additional IG requirements for laboratory information are critical for public health as not all laboratory information is reportable to public health through electronic laboratory reporting. These additional data elements enable public health jurisdictions to monitor the nation's public health. We also clarify that the aggregated OMB value sets for race and ethnicity are acceptable within Release 2.0. We decline to make the optional elements of the IG required for certification as we believe that certification to the IG as published appropriately supports the use case. We also note that any IG instructions regarding the frequency of submission are outside the scope of certification as certification focuses on the technical capabilities of the Health IT Module presented for certification.

Ambulatory Syndromic Surveillance

We proposed to permit, for ambulatory setting certification, the use of any electronic means for sending syndromic surveillance data to public health agencies as well as optional certification to certain syndromic surveillance data elements. Due to the continued lack of mature IGs, we proposed to provide the option for health IT to electronically produce syndromic surveillance information that contains patient demographics, provider specialty, provider address, problem list, vital signs, laboratory results, procedures, medications, and insurance.

Comments. Most commenters stated that the majority of public health jurisdictions do not accept ambulatory syndromic surveillance data and that the standards for ambulatory syndromic surveillance are not mature. In particular, one commenter noted that syndromic surveillance standards for ambulatory encounters remain ill-defined and derivative of the inpatient standards. A few commenters stated that the "flexibility" in certification created burden on both providers and health IT developers to develop and implement health IT to meet the specified data elements without an established use case across public health jurisdictions.

Response. With consideration of public comments, comments received on a prior rulemaking (79 FR 54439-54441), and stakeholder feedback through public health outreach, we have determined to not adopt certification requirements for the ambulatory setting. Without mature standards and the widespread acceptance of ambulatory syndromic surveillance data across public health jurisdictions, sufficient reason does not exist to justify certification to the proposed functionality. To clarify, the PHIN 2.0 IG does support the urgent care ambulatory setting and would be appropriate for use in that particular setting.

- Transmission To Public Health Agencies – Reportable Laboratory Tests and Values/Results

2015 Edition Health IT Certification Criterion
§ 170.315(f)(3) (Transmission to public health agencies – reportable laboratory tests and values/results)

We proposed to adopt a 2015 Edition certification criterion that was revised in comparison to the 2014 Edition "transmission of reportable laboratory tests and values/results" criterion (§ 170.314(f)(4)). We proposed to name this criterion "transmission to public health agencies – reportable laboratory tests and values/results" to clearly convey the capabilities included in this criterion as they relate to the intended recipient of the data. We proposed to include and adopt an updated IG, the HL7 Version 2.5.1 Implementation Guide: Electronic Laboratory Reporting to Public Health, Release 2 (US Realm), DSTU R1.1, 2014 or "Release 2, DSTU R1.1") that addresses technical corrections and clarifications for interoperability with laboratory orders and other laboratory domain implementation guides. Given the improvements included in the updated IG (Release 2, DSTU R1.1), we proposed to adopt it at § 170.205(g)(2) and include it in the 2015 Edition "transmission of reportable laboratory tests and values/results" certification criterion at § 170.315(f)(3). We also proposed the September 2014 Release of the U.S. Edition of SNOMED CT® and LOINC® version 2.50. We also proposed to make a technical

amendment to the regulation text for the 2014 Edition criterion in order to have it continue to reference the appropriate standard and implementation specifications[112] after we restructured the regulatory text hierarchy at § 170.205(g) to accommodate our 2015 Edition proposal.

Comments. Most commenters supported the proposed criterion and standards. A few commenters expressed concern with the proposed IG related to use of OIDs, SPM-22 and SPM-24.

Response. We appreciate the expression of support for this criterion and the proposed standards. We note, however, that the HL7 Public Health and Emergency Response Workgroup is currently working on a newer version of the proposed IG that harmonizes with the HL7 Laboratory Results Interface (LRI) profiles. Harmonization with LRI will address the noted concerns as well as ensure alignment across laboratory IGs, including the LRI IG and the Laboratory Orders Interface (LOI) IG. This updated IG is not yet complete and cannot be adopted at this time. With these considerations, we do not believe it would be appropriate to adopt the proposed IG as health IT developer and provider efforts to meet and implement the requirements of the proposed IG would shortly be superseded by the updated IG. Therefore, we have not adopted the proposed IG. We have also not adopted the updated vocabulary standards because without a newer IG, there is little benefit from having health IT developers be tested and certified to updated vocabulary standards for this particular use case.

We have adopted a 2015 Edition "transmission to public health agencies – reportable laboratory tests and values/results" certification criterion that requires adherence to the same standards as we referenced in the 2014 Edition "transmission of reportable laboratory tests and values/results" criterion. Data from CDC and CMS indicates that over 80% of hospitals are

[112] HL7 2.5.1 and HL7 Version 2.5.1: Implementation Guide: Electronic Laboratory Reporting to Public Health, Release 1 with Errata and Clarifications and ELR 2.5.1 Clarification Document for EHR Technology Certification

already in the process of submitting electronic laboratory results using the previously adopted standards (HL7 Version 2.5.1 Implementation Guide: Electronic Laboratory Reporting to Public Health, Release 1 with Errata and Clarifications, ELR 2.5.1 Clarification Document for EHR Technology Certification, and versions of SNOMED CT® and LOINC®). Our decision to adopt these same standards for the 2015 Edition criterion will ensure continuity in reporting and reduce burden for providers as well as health IT developers as this criterion is eligible for gap certification. We will continue to monitor the development of the updated IG and may consider proposing it for adoption through a future rulemaking to give health IT developers and providers another option to meet EHR Incentive Programs requirements for use of certified health IT to meet public health objectives and measures.

- Transmission To Cancer Registries

2015 Edition Health IT Certification Criterion § 170.315(f)(4) (Transmission to cancer registries)

We proposed to adopt a 2015 Edition "transmission to cancer registries" certification criterion that was revised in comparison to the 2014 Edition "transmission to cancer registries" certification criterion (§ 170.314(f)(6)). We proposed to adopt the HL7 Implementation Guide for CDA© Release 2: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers Release 1 or "HL7 Release 1 IG") to address technical corrections and clarifications for interoperability with EHRs and cancer registries, at § 170.205(i)(2). We proposed to include the September 2014 Release of the U.S. Edition of SNOMED CT® and LOINC® version 2.50 in this criterion. We proposed to modify the 2014 Edition certification criterion to reference § 170.205(i)(1) to establish the regulatory text hierarchy necessary to accommodate the standard and IG referenced by the proposed 2015 Edition certification criterion.

Comments. The majority of commenters expressed support for this criterion as proposed, including the HL7 Release 1 IG. Commenters stated that the proposed IG would provide substantial improvements in cancer reporting. Commenters also expressed support for incorporating updated versions of SNOMED CT® and LOINC® in this criterion as the vocabulary standards align with the IG requirements. Some commenters suggested mapping the IG to the currently used North American Association of Central Cancer Registries (NAACCR) format for any new cited standards. A commenter contended there was contradictory use of null values within the proposed IG. A few commenters expressed general concern regarding a lack of standardization across public health jurisdictions and registries to accept data according to proposed public health standards.

Response. We appreciate the overall support for this criterion and the HL7 Release 1 IG. The CDC recently published and updated version of the IG (HL7 CDA® Release 2 Implementation Guide: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1; DSTU Release 1.1, U.S. Realm)[113] ("Release 1.1."). Release 1.1 involves technical corrections to Release 1. No new content has been included. The templates in the IG were versioned due to the versioning of included templates (see the detailed section "Changes from Previous Version" in Volume 2 of this guide for a detailed view of these changes). The TNM Clinical Stage Observation was separated into a nested series of smaller, easier to implement templates. To note, the TNM Clinical Stage Observation template had grown into a large, multi-level template that was difficult to implement and test. Similar changes were made to the TNM Pathologic Stage Observation template. Release 1.1 also addresses the contradictory use of nullFlavor attributes. A final notable revision is a constraint in the Cancer

[113] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=398

Diagnosis Observation that provided a choice between the TNM Pathologic Stage Observation and a No Known TNM Pathologic Stage Observation was replaced by a choice of standard constraints on the same two templates. This revision results in both an easier to understand specification and a simplified schematron file used for validation.

We have adopted this criterion with the updated IG, Release 1.1 (both Volumes 1 and 2). Commenters were supportive of our overall proposed approach and the proposed IG. As detailed above, Release 1.1 addresses errors, ambiguities, implementation issues, and commenters' concerns. Therefore, the adoption of Release 1.1 will lead to improved implementation and interoperability.

Mapping to the NAACCR format is not included in the IG because the mapping rules are complex, and can change over time based on continued input and refinement by the cancer registry community. It is our understanding that the CDC will work closely with the cancer registry community to develop mapping rules for the IG and will incorporate the rules into the software tools CDC provides state cancer registries. In regard to concerns expressed about jurisdictional variations, all public health jurisdictions have all adopted the HL7 IG Release 1 for cancer reporting and will be moving to the updated version published by the CDC.

We have adopted a newer baseline versions of SNOMED CT® (September 2015 Release of the U.S. Edition) and LOINC® (version 2.52) for the purposes of certification. We refer readers to section III.A.2.c ("Minimum Standards" Code Sets) for further discussion of our adoption of minimum standards code sets and our decision to adopt these versions.

<u>Cancer Case Information</u>

We did not propose a "cancer case information" criterion as part of the 2015 Edition (80 FR 16854-855), but welcomed comments on this approach.

Comments. Commenters expressed agreement with discontinuing the "cancer case information" certification criterion, with a commenter noting the relevant data elements are already contained in the IG referenced in the 2015 Edition "transmission to cancer registries" certification criterion. A commenter asked for clarification as to whether the discontinuation of this criterion affects the requirements of the "transmission to cancer registries" certification criterion and the requirements of the IG.

Response. We thank commenters for their feedback and have not adopted a "cancer case information" certification criterion. This decision has no impact on the requirements of the 2015 Edition "transmission to cancer registries" certification criterion or the requirements of the IG. Certification to the 2015 Edition "transmission to cancer registries" criterion requires a Health IT Module to demonstrate that it can create a file with the necessary cancer case information in accordance with the IG.

- Transmission To Public Health Agencies – Electronic Case Reporting

2015 Edition Health IT Certification Criterion
§ 170.315(f)(5) (Transmission to public health agencies – electronic case reporting)

We proposed to adopt a new 2015 Edition "transmission to public health agencies – case reporting" certification criterion, which would support the electronic transmission of case reporting information to public health agencies. We proposed to require a Health IT Module to be able to electronically create case reporting information for electronic transmission in accordance with the IHE Quality, Research, and Public Health Technical Framework Supplement, Structured Data Capture, Trial Implementation (September 5, 2014) standard. We noted that a Health IT Module would need to demonstrate that it can create and send a constrained transition of care document to a public health agency, accept a URL in return, be

able to direct end users to the URL, and adhere to the security requirements for the transmission of this information.

In addition, we requested comment on whether we should consider adopting the HL7 FHIR Implementation Guide: SDC DSTU that would be balloted in mid-2015 in place of, or together with, the IHE Quality, Research, and Public Health Technical Framework Supplement.

Comments. Commenters expressed agreement on the importance of case reporting for public health. Some commenters expressed no concerns with the IHE profile, while others were unsure whether public health agencies had been sufficiently involved in the creation of the IG to warrant adoption in the 2015 Edition. The latter commenters stated that the IG is primarily driven by clinical research requirements and has not been adopted by the public health community. Some commenters expressed concern with the potential use of the FHIR standard, stating it is immature and requires piloting and initial deployments before it can be adopted as a national standard. A commenter recommended that case reporting remain as a public health reporting option for the EHR Incentive Programs, but not be constrained by a requirement to use a specific standard.

Response. We understand commenters' concerns with the current state of standards available and the continual evolution of standards. We also agree with commenters' suggestions that an appropriate approach for this criterion would be to permit flexibility for case reporting by not referencing a specific content exchange standard for certification at this time.

We understand the industry is moving towards RESTful approaches and considering FHIR for different exchange patterns, including case reporting. To accommodate this evolution, we have not adopted the proposed IHE profile as part of this certification criterion or another exchange standard. We understand that there are certain functional requirements that a Health IT

Module would need to support to enable electronic case reporting. Specifically, a Health IT Module would need to support the ability to electronically: (1) consume and maintain a table of trigger codes to determine which encounters should initiate an initial case report being sent to public health; (2) when a trigger is matched, create and send an initial case report to public health; (3) receive and display additional information, such as a "notice of reportability" and data fields to be completed; and (4) submit a completed form.

Public health agencies have, however, prioritized receiving the initial electronic case report form, while building the infrastructure to request supplemental data over time. Given the priority to receive the initial case report form, we have adopted the following functionality that supports the first two identified steps above. To meet this certification criterion, a Health IT Module must be able to (1) consume and maintain a table of trigger codes to determine which encounters should initiate an initial case report being sent to public health to determine reportability; and (2) when a trigger is matched, create an initial case report that includes specific data (Common Clinical Data Set; encounter diagnoses; provider name, office contact information, and reason for visit, and an identifier representing the row and version of the trigger table that triggered the case report).

The CCD template of the C-CDA Release 2.1 is currently the most viable approach for achieving step (2) above. We note, however, that the CDC and CSTE, with the HL7 Public Health and Emergency Response Working Group, are currently developing C-CDA and FHIR IGs to specify the data needed in the initial case report form and the data that would be provided in the information returned to the provider. As standards evolve, additional/supplemental data would likely be requested electronically about cases for which public health has received an initial case report that is deemed reportable. To support this additional data reporting, the future

might include a FHIR-based approach that could utilize the FHIR Structured Data Capture (SDC) IG. Therefore, we believe this overall initial certification approach establishes necessary flexibility within the ONC Health IT Certification Program related to electronic case reporting in that as technical approaches evolve to accomplish electronic case reporting they can be certified. In the future, we may be able to consider a specific standard for certification through rulemaking.

We note that we have inserted "electronic" in the criterion name to emphasize the evolution of case reporting and the importance of electronic case reporting.

Comments. Many commenters expressed concern around the burden of connecting to multiple jurisdictions. One commenter noted a typical practice may be required to report in three different states using entirely different technologies, standards, and processes. The commenter recommended that the public health community develop a single reporting hub where all reports are submitted using the same technologies, standards, and processes. A couple of commenter suggested the use of a centralized platform or intermediary, which could streamline connectivity and reduce jurisdictional variability.

Response. We agree with commenters that a common public health interface or intermediary would reduce the burden on health IT developers and state and local public health agencies. The CDC and the public health community have made an investment in a centralized approach for receipt of electronic case reports. The CDC will identify a test harness and tool for all the functional requirements described above. Additionally, as the CDC and public health approach matures to include other interfaces, the CDC will continue to monitor the development of standards to support these functional requirements. As noted above, this may lead to future rulemaking for the certification of electronic case reporting.

Comments. Many commenters identified a difference in the description of case reporting between the Proposed Rule and the EHR Incentive Programs Stage 3 proposed rule. In particular, a commenter compared the examples given for the Structured Data Capture standard proposed for case reporting in the Proposed Rule with the description of case reporting provided in the EHR Incentive Programs Stage 3 proposed rule, which focused on submitting information about reportable conditions to monitor disease outbreaks.

Response. The examples in the Proposed Rule of birth reports and other public health reporting were not examples of electronic case reporting. The examples were meant to illustrate how other public health domains have accomplished public health reporting through the use of the IHE RFD profile, upon which the IHE SDC profile proposed for adoption is based.

- Transmission To Public Health Agencies – Antimicrobial Use And Resistance Reporting

2015 Edition Health IT Certification Criterion
§ 170.315(f)(6) (Transmission to public health agencies – antimicrobial use and resistance reporting)

We proposed to adopt a new 2015 Edition certification criterion that would require a Health IT Module to be able to electronically create antimicrobial use and resistance reporting information for electronic transmission in accordance with specific sections of the HL7 Implementation Guide for CDA® Release 2 – Level 3: Healthcare Associated Infection Reports, Release 1, U.S. Realm (August 2013) ("HAI IG"). We explained that collection and analysis of data on antimicrobial use and antimicrobial resistance are important components of antimicrobial stewardship programs throughout the nation and electronic submission of antimicrobial use and antimicrobial resistance data to a public health registry can promote timely, accurate, and complete reporting, particularly if data is extracted from health IT systems and delivered using well established data exchange standards to a public health registry.

We proposed to test and certify a Health IT Module for conformance with the following sections of the IG in § 170.205(r)(1): HAI Antimicrobial Use and Resistance (AUR) Antimicrobial Resistance Option (ARO) Report (Numerator) specific document template in Section 2.1.2.1 (pages 69-72); Antimicrobial Resistance Option (ARO) Summary Report (Denominator) specific document template in Section 2.1.1.1 (pages 54-56); and Antimicrobial Use (AUP) Summary Report (Numerator and Denominator) specific document template in Section 2.1.1.2 (pages 56-58). We explained that we would expect a Health IT Module presented for certification to this criterion to conform to all named constraints within the specified document template.

Comments. Most commenters expressed support for the adoption the proposed certification criterion and the included standard. A commenter stated that data on antimicrobial use and antimicrobial resistance are essential components of antimicrobial stewardship programs throughout the nation and is a highlight of the National Action Plan for Combating Antibiotic Resistant Bacteria. Another commenter stated that the data elements for antimicrobial use and resistance reporting are positive steps to help guide public health activities. Commenters also stated that the proposed criterion and standard would bolster the CDC's National Healthcare Safety Network (NHSN) effort to develop coherent policies to fight antibiotic resistance through the reporting of standardized data about antibiotic use and resistance.

A commenter expressed concern about the pace and volume of changes between versions of the standard, the burden on health IT developers related to the timing of deployments, and that NHSN does not accept data submitted using prior versions. Another commenter expressed concern about state variations that are not addressed by this criterion, suggesting that the

criterion and standard not be adopted until at least 75% of public health agencies are committed to adopting this standard.

A commenter stated that there were inconsistences in the EHR Incentive Programs Stage 3 proposed rule related to this criterion regarding the standards available as well as a reference to meeting the measure four times. Another commenter suggested that the associated proposed measure under Stage 3 should be limited to eligible hospitals and CAHs (not EPs).

Response. We appreciate the overall support for this criterion and the IG. We have adopted this criterion as proposed (with both Volumes 1 and 2 of the HAI IG). We intend to work with federal partners, such as the CDC, to eliminate or reduce any negative impacts on health IT developers resulting from the frequency of reporting changes or the manner in which changes are implemented in the associated program. We note that certification to the adopted version of the standard is what is necessary to meet the CEHRT definition under the EHR Incentive Programs. In regard to the concern about state variations, this data will only be collected by the CDC at the national level. The CDC is the only public health agency that needs to be able to receive these surveys electronically, which it is capable of doing. The use of a national interface for receipt avoids the problems associated with jurisdictional variation.

For concerns and questions related to the EHR Incentive Programs, we refer readers to CMS and the EHR Incentive Programs Stage 3 and Modifications final rule published elsewhere in this issue of the **Federal Register**.

- Transmission To Public Health Agencies – Health Care Surveys

2015 Edition Health IT Certification Criterion § 170.315(f)(7) (Transmission to public health agencies – health care surveys)

We proposed to adopt a new 2015 Edition certification criterion for transmission of health care surveys to public health agencies that would require a Health IT Module to be able to

create health care survey information for electronic transmission in accordance with the HL7 Implementation Guide for CDA® Release 2: National Health Care Surveys (NHCS), Release 1 - US Realm, Draft Standard for Trial Use (December 2014)[114]. We explained that the National Ambulatory Medical Care Survey (NAMCS) is a national survey designed to meet the need for objective, reliable information about the provision and use of ambulatory medical care services in the U.S We also explained that the National Hospital Ambulatory Medical Care Survey (NHAMCS) is designed to collect data on the utilization and provision of ambulatory care services in hospital emergency and outpatient departments. We clarified that the proposed IG is intended for the transmission of survey data for both the NAMCS (e.g., for ambulatory medical care settings) and NHAMCS (e.g., for hospital ambulatory settings including emergency departments and outpatient departments). We noted that templates included in the IG align with the C-CDA standard. Additionally, we noted that the templates in the IG expand on the scope of the original NAMCS and NHAMCS survey data elements. The templates do not constrain the data collected to the narrow lists on the survey instruments; rather they allow any service, procedure or diagnosis that has been recorded.

Commenters. Commenters overwhelmingly supported the certification criterion and the use of the NHCS IG. Commenters expressed support for the continued effort to advance use of health care surveys as a means of improving patient outcomes. Commenters also expressed support for the specified data elements in the IG. One commenter, however, questioned the maturity of the standard and its adoption for certification at this time. Commenters requested clarification (and confirmation) on the surveys that must be supported for the purposes of

[114] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=385

certification. In particular, a commenter noted that it was not unclear whether the NAMCS and NHAMCS are the only surveys covered for certification.

A commenter requested information on the number of public health agencies that can electronically accept data in accordance with the IG.

Response. We appreciate the overall support for this criterion and the IG. We have adopted this criterion as proposed. While we understand the concerns that this standard may not be fully mature, the IG has gone through the HL7 balloting process and is currently a Draft Standard for Trial Use, which is no different than other standards in use today and adopted as part of the 2015 Edition. Further, the CDC has been working with providers to submit this data electronically using these surveys prior to this rulemaking. As such, we believe that the IG is mature enough for widespread adoption.

We clarify that, as proposed, certification would cover the entire NHCS IG. The NHCS IG consists of the National Hospital Care Survey, NHAMCS, and NAMCS. In the Proposed Rule, we focused on clarifying that the NHAMCS and NAMCS were included in the IG and the changes in the surveys as compared to past versions. However, all three surveys are covered by the NHCS IG and will be covered as part of testing and certification.

All public health agencies may not be able to receive this data electronically and that variability across jurisdictions could be problematic. However, this data will only be collected by the CDC at the national level. The CDC is the only public health agency that needs to be able to receive these surveys electronically, which it is capable of doing. The use of a national interface for receipt avoids the problems associated with jurisdictional variation.

- Automated Numerator Recording

2015 Edition Health IT Certification Criterion
§ 170.315(g)(1) (Automated numerator recording)

We proposed to adopt a 2015 Edition "automated numerator recording" certification criterion that was unchanged in comparison to the 2014 Edition "automated numerator recording" criterion. We noted that the test procedure for this criterion would be different from the 2014 Edition "automated numerator recording" certification criterion in order to remain consistent with the applicable objectives and measures required under the EHR Incentive Programs.

Comments. We received mixed comments in response to the proposal. A number of commenters supported this criterion as proposed. A few commenters stated that this criterion has been burdensome and complicated as its implementation has led to interruptions in provider workflows solely for the purposes of reporting on measures under the EHR Incentive Programs. These commenters further contended that such data collection was unrelated to improving patient care. A commenter suggested that we ensure that the terminology used in the test procedures aligns with that used for the measures under the EHR Incentive Programs. Another commenter suggested that this criterion should be gap certification eligible if the associated EHR Incentive Programs measure has not changed from Stage 2.

Response. We have adopted this criterion as proposed. This criterion is included in the CEHRT definition under the EHR Incentive Programs. This certification criterion could ease the burden of reporting particularly for small providers and hospitals (77 FR 54184). We will work to ensure consistency with the test procedure and the measures under the EHR Incentive Programs. As stated in the 2015 Edition proposed rule (FR 80 16868), this certification criterion's gap certification eligibility is "fact-specific" and depends on any modifications made to the specific certification criteria to which this criterion applies. As mentioned above and in the

Proposed Rule, it would also depend on changes to the test procedure that are made to align with applicable objectives and measures under the EHR Incentive Programs.

We have changed the term "meaningful use" to "EHR Incentive Programs" and removed "objective with a" in the first sentence of the criterion to more clearly align with the terminology and framework used under the EHR Incentive Programs.

- Automated Measure Calculation

2015 Edition Health IT Certification Criterion § 170.315(g)(2) (Automated measure calculation)

We proposed to adopt a 2015 Edition "automated measure calculation" certification criterion that was unchanged in comparison to the 2014 Edition "automated measure calculation" criterion. We proposed to apply the guidance provided for the 2014 Edition "automated measure calculation" certification criterion in the 2014 Edition final rule that a Health IT Module must be able to support all CMS-acceptable approaches for measuring a numerator and denominator in order for the Health IT Module to meet the proposed 2015 Edition "automated measure calculation" certification criterion.[115] We also proposed that the interpretation of the 2014 Edition "automated measure calculation" certification criterion in FAQ 32[116] would apply to the 2015 Edition "automated measure calculation" certification criterion. We also noted that the test procedure for this criterion would be different from the 2014 Edition "automated measure calculation" certification criterion in order to remain consistent with the applicable objectives and measures required under the EHR Incentive Programs.

Comments. We received mixed comments in response to our proposal. One commenter noted that this criterion and included functionality has value for helping providers understand

[115] 77 FR 54244–54245.
[116] http://www.healthit.gov/policy-researchers-implementers/32-question-11-12-032

their quality outcomes and performance on certain EHR Incentive Programs measures. A few commenters stated that this criterion has been burdensome and complicated as its implementation has led to interruptions in provider workflows solely for the purposes of reporting on measures under the EHR Incentive Programs. These commenters further contended that such data collection was unrelated to improving patient care.

Commenters were generally supportive of applying the guidance provided in the 2014 Edition final rule (77 FR 54244–54245) and the guidance in FAQ 32 to the 2015 Edition criterion. One commenter suggested that this criterion should be gap certification eligible if the associated EHR Incentive Programs measure has not changed from Stage 2. This commenter recommended that ONC provide revised draft test procedures for this criterion for public comment prior to the release of the final rule.

Response. We have adopted this criterion as proposed. This criterion is included in the CEHRT definition under the EHR Incentive Programs. This certification criterion could improve the accuracy of measure calculations to reduce reporting burdens for EPs, eligible hospitals, and CAHs (77 FR 54244). We will apply the guidance in the 2014 Edition final rule and FAQ 32 to this criterion.

As stated in the 2015 Edition proposed rule (FR 80 16868), this certification criterion's gap certification eligibility is "fact-specific" and depends on any modifications made to the specific certification criteria to which this criterion applies. As mentioned above and in the Proposed Rule, it would also depend on changes to the test procedure that are made to align with applicable objectives and measures under the EHR Incentive Programs. We note that draft test procedures for the 2015 Edition were released with the publication of the Proposed Rule[117] and

[117] http://healthit.gov/policy-researchers-implementers/2015-edition-draft-test-procedures

were open for public comment from March 20, 2015, to June 30, 2015. Revised draft final test procedures will be made available after publication of this final rule for public review and comment.

We have changed the first use of the term "meaningful use" to "EHR Incentive Programs" and removed its second use in the criterion. We have also removed the phrase "objective with a." We have made these revisions to more clearly align with the terminology and framework used under the EHR Incentive Programs.

- Safety-Enhanced Design

2015 Edition Health IT Certification Criterion § 170.315(g)(3) (Safety-enhanced design)

We proposed to adopt a 2015 Edition "safety-enhanced design" (SED) certification criterion that was revised in comparison to the 2014 Edition "safety-enhanced design" criterion. We proposed to include seventeen (17) certification criteria (seven new) in the 2015 Edition SED certification criterion (80 FR 16857), and for each of the referenced certification criteria and their corresponding capabilities presented for certification, we proposed to require that user-centered design (UCD) processes must have been applied in order satisfy this certification criterion. We stated we intend to continue submission of summative usability test results to promote transparency and foster health IT developer competition, spur innovation, and enhance patient safety. With this in mind, we sought comment on whether there are other certification criteria that we omitted from the proposed SED criterion that commenters believe should be included.

Comments. Comments generally supported the proposed SED criterion, but questioned the number of certification criteria included. Some commenters questioned rationale for adding the new criteria and the carryover inclusion of the "drug-drug, drug-allergy interaction checks for

CPOE" criterion, while other commenters generally questioned whether this criterion has contributed to improving usability or patient safety. A few commenters suggested that this criterion only apply to criteria that involve tasks performed by clinical users. A couple of commenters expressed concern about the additional burden the new criteria presented.

Response. We thank commenters for their feedback. We have adopted the proposed SED with revisions and clarifications. We note that 5 criteria proposed for inclusion in the SED criterion have not been adopted as part of the 2015 Edition. These criteria are: "vital signs," "eMAR," "incorporate laboratory tests/results," and both "decision support" criteria. Consequently, these criteria cannot be included in the SED criterion and, therefore, there is only a net increase of two criteria subject to the SED criterion. We do not believe this will create a significant burden for health IT developers and note that many developers have had their products certified to the 2014 Edition versions of the criteria included in the 2015 SED criterion and the 2014 Edition SED criterion. The criteria included in the 2015 Edition SED criterion are as follows (emphasis added for the new criteria):

- Section 170.315(a)(1) Computerized provider order entry – medications
- Section 170.315(a)(2) Computerized provider order entry – laboratory
- Section 170.315(a)(3) Computerized provider order entry – diagnostic imaging
- Section 170.315(a)(4) Drug-drug, drug-allergy interaction checks
- Section 170.315(a)(5) Demographics
- Section 170.315(a)(6) Problem list
- Section 170.315(a)(7) Medication list
- Section 170.315(a)(8) Medication allergy list
- Section 170.315(a)(9) Clinical decision support

- Section 170.315(a)(14) Implantable device list
- Section 170.315(b)(2) Clinical information reconciliation and incorporation
- Section 170.315(b)(3) Electronic prescribing

We believe the inclusion of criteria such as "demographics," "implantable device list," "drug-drug, drug-allergy interaction checks for CPOE," and "CDS" are appropriate because data entry errors and poor user interfaces for responding to alerts and interventions can compromise patient safety. While we do not have empirical data related to the "effectiveness" of the SED criterion, we believe that our approach contributes to improving usability and patient safety through both the application of the SED criterion's requirements to a significant number of health technologies being used in the market today and in the future as well as through the SED information being available on the CHPL for stakeholder review and evaluation.

NISTIR 7742 Submission Requirements, New Requirements and Compliance Guidance

We proposed to include the specific information from the NISTIR 7742 "Customized Common Industry Format Template for Electronic Health Record Usability Testing" (NIST 7742)[118] in the regulation text of the 2015 Edition SED criterion to provide more clarity and specificity on the information requested in order to demonstrate compliance with this certification criterion. We reiterated that the information must be submitted for each and every one of the criteria specified in the 2015 Edition SED criterion to become part of the test results publicly available on the Certified Health IT Product List (CHPL). We specified that all of the data elements and sections must be completed, including "major findings" and "areas for improvement."

[118] http://www.nist.gov/manuscript-publication-search.cfm?pub_id=907312

We identified the table on page 11 of NISTIR 7742 for the submission of demographic characteristics of the test participants because it is important that the test participant characteristics reflect the audience of current and future users. In accordance with NISTIR 7804 (page 8)[119], we recommended that the test scenarios be based upon an analysis of critical use risks for patient safety, which can be mitigated or eliminated by improvements to the user interface design.

We strongly advised health IT developers to select an industry standard process because compliance with this certification criterion requires submission of the name, description, and citation (URL and/or publication citation) of the process that was selected, and we provided examples of method(s) that could be employed for UCD, including ISO 9241-11, ISO 13407, ISO 16982, ISO/IEC 62366, ISO 9241-210 and NISTIR 7741. We explained that, in the event that a health IT developer selects a UCD process that was not an industry standard (i.e., not developed by a voluntary consensus standards organization), but is based on one or more industry standard processes, the developer may name the process(es) and provide an outline of the process in addition to a short description as well as an explanation of the reason(s) why use of any of the existing UCD standards was impractical. We also noted that health IT developers can perform many iterations of the usability testing, but the submission that is ultimately provided for summative usability testing and certification must be an expression of a final iteration, and the test scenarios used would need to be submitted as part of the test results. We noted that we do not expect developers to include trade secrets or proprietary information in the test results.

[119] http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909701

Comments. Commenters expressed appreciation for the clarity the proposed 2015 Edition SED criterion provided in terms of requirements. Some commenters agreed with including major findings and areas for improvement sections in the summative testing documentation, while other commenters did not support the public reporting of major findings and areas for improvement because they argued that the information is usually meant to inform the developer.

Many commenters expressed concern on the proposed limitation for measuring user satisfaction. Commenters mentioned that user satisfaction ratings are often now based on non-standard surveying processes. Commenters suggested that we not solely rely on task-based satisfaction measures and consider post-session satisfaction measures. Commenters suggested that we use industry standard, literature-recognized satisfaction measures such as the Single Ease-of-use Question, System Usability Scale, or Software Usability Measurement Inventory.

Response. We thank commenters for their feedback. We have finalized our proposed requirements with one revision. In response to comments, we now also permit the submission of an alternative acceptable user satisfaction measure to meet the requirements of this criterion. Stated another way, a health IT developer could meet the proposed NIST 7742 based approach for user satisfaction or provide documentation of an alternative acceptable user satisfaction measure. We will take into consideration the other user satisfaction measures identified by commenters in the development and finalization of the 2015 SED test procedures and related guidance for complying with this criterion and particularly the user satisfaction measure.

Number of Test Participants

We recommended following NISTIR 7804[120] "Technical Evaluation, Testing, and Validation of the Usability of Electronic Health Records" for human factors validation testing of

[120] http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909701

the final product to be certified, and recommended a minimum of 15 representative test participants for each category of anticipated clinical end users who conduct critical tasks where the user interface design could impact patient safety (e.g., physicians, nurse practitioners, physician assistants, nurses, etc.) and who are not include employees of the developer company. We additionally requested comment on whether we should establish a minimum number(s) and user cohort(s) for test participants for the purposes of testing and certification to the 2015 Edition under the ONC Health IT Certification Program.

Comments. We received a large number of comments in response to this request for comment with the majority of commenters advocating for a required minimum number of test participants and some commenters advocating for established user cohorts per capability. Commenters strongly stated that establishing a minimum number of participants would allow for proper validation of testing results. Many commenters advocated for a minimum of 12 or 15 participants. Another large contingent of commenters advocated for 10 participants. A few commenters suggested that the number of test participants should remain as guidance. A few commenters also stated that a high participant threshold could be burdensome to small developers.

Commenters generally recommended that cohorts should be consistent with the capability under testing. Some commenters stated, for example, that clinicians would not be appropriate for a more administrative capability such as recording demographics. Commenters gave mixed responses on whether this described approach should be required or simply guidance.

Response. As a general matter, the more users tested, the more likely developers will be able to identify and remedy design flaws. To this point, research suggests that “with ten participants, 80 percent of the problems are found whereas 95 percent of the problems are found

with twenty participants."[121] For the purposes of this final rule, we have adopted a provision as part of this criterion that requires 10 participants per criterion/capability as a mandatory minimum for the purposes of testing and certification. We believe this minimum is responsive to commenters and will ensure more reliable summative testing results. We also believe this number will balance any potential burden for health IT developers, including small developers. However, we strongly encourage health IT developers to exceed the mandatory minimum in an effort to identify and resolve more problems.

We agree with commenters that cohorts should not be limited to clinicians but instead consist of test participants with the occupation and experience that aligns with the capability under testing. We believe, however, that it would be too restrictive and complicated to establish cohort requirements per criterion. Instead, we continue to recommend that health IT developers follow NISTIR 7804 for human factors validation testing of the final product to be certified. We will also work with NIST to provide further guidance as needed.

Request for Comment on Summative and Formative Testing

We requested comment regarding options that we might consider in addition to – or as alternatives to – summative testing. We asked whether a standardized report of formative testing could be submitted for one or more of the 17 proposed certification criteria for which summative testing would be required, if formative testing reflected a thorough process that has tested and improved the usability of a product. Additionally, we asked for feedback on the requirements for such a formative testing report and on how purchasers would evaluate these reports.

Comments. Commenters acknowledged the benefits of formative testing, with some noting that it can act as a risk management process before getting to summative testing. The

[121] Pg. 42. NISTIR 7804 Technical Evaluation, Testing, and Validation of the Usability of Electronic Health Records http://www.nist.gov/healthcare/usability/upload/EUP_WERB_Version_2_23_12-Final-2.pdf

majority of the commenters, however, were against formative testing as an alternative to summative testing. One commenter stated that one of the main objectives for the SED criterion is to allow purchasers and consumers to compare competing products on the quality of human interaction and usability. The commenter contended that test results are therefore publicly available for this purpose on the Certified Health IT Product List (CHPL). The commenter maintained that this essential function cannot be fulfilled, however, with the results of formative testing as they cannot be compared across products but only between the iterations of a single product. The commenter noted, as other commenters did, that formative tests are intended to identify problems rather than produce measures. A few commenters suggested that we require both summative and formative testing, while a few other commenters suggested formative testing was not reliable or useful.

Response. We thank commenters for their insightful feedback. We agree with the commenters that see value in formative testing, but we also agree with the commenters that contend it should not be a substitute for summative testing for the purposes of this criterion. With this in mind and consideration of the potential burden imposed by requiring both summative and formative testing, we have decided to retain summative testing requirements and not adopt formative testing requirements.

Retesting and Certification

We stated that we believe that ONC-ACB determinations related to the ongoing applicability of the SED certification criterion to certified health IT for the purposes of inherited certified status (§ 170.550(h)), adaptations and other updates would be based on the extent of changes to user-interface aspects of one or more capabilities to which UCD had previously been applied. We specified that ONC-ACBs should be notified when applicable changes to user-

interface aspects occur, and we included these types of changes in our proposal to address adaptations and updates under the ONC-ACB Principles of Proper Conduct (§ 170.523).

We discuss the comments received on this proposal and our response under section IV.D.6 of this preamble.

- Quality Management System

2015 Edition Health IT Certification Criterion § 170.315(g)(4) (Quality management system)

We proposed to adopt a 2015 Edition "quality management system" certification criterion that was revised in comparison to the 2014 Edition and proposed that all Health IT Modules certified to the 2015 Edition would need to be certified to the 2015 Edition QMS criterion "quality management system" criterion. We proposed to require the identification of the Quality Management System (QMS) used in the development, testing, implementation, and maintenance of capabilities certified under the ONC Health IT Certification Program. We specified that the identified QMS must be compliant with a quality management system established by the federal government or a standards developing organization; or mapped to one or more quality management systems established by the federal government or standards developing organization(s). We stated that we will not permit health IT to be certified that has not been subject to a QMS and that we will require health IT developers to either use a recognized QMS or illustrate how the QMS they used maps to one or more QMS established by the federal government or a standards developing organization(s) (SDOs). We explained that we encourage health IT developers to choose an established QMS, however, developers may also use either a modified version of an established QMS, or an entirely ''home grown'' QMS. In cases where a health IT developer does not use a QMS established by the federal government or an SDO, we proposed to require the health IT developers illustrate how their QMS maps to one or more QMS

established by the federal government or SDO through documentation and explanation that links the components of their QMS to an established QMS and identifies any gaps in their QMS as compared to an established QMS. We added that documentation of the current status of QMS in a health IT development organization would be sufficient. We also provided a list of QMS standards established by the federal government and SDOs (80 FR 16858).

Comments. The majority of commenters supported the proposed criterion and its approach, with broad support across health IT developers, providers, and consumers. A commenter questioned whether we provided the appropriate example standards, citing ISO 14971 as a risk-management standard for medical devices and not a QMS standard. Other commenters stated that the identified standards were too focused on medical devices. A few commenters indicated that other standards and processes should be considered as acceptable means for meeting this criterion. These commenters specifically mentioned ISO 12207, IEEE 730, IEEE 1012, ISO 14764, ISO 80001, the health IT QMS standards under development through the Association for the Advancement of Medical Instrumentation (AAMI), and the accreditation process software quality systems run by the Capability Maturity Model Integration Institute (CMMI). A few commenters expressed concern that it would be burdensome to map an internal QMS to one or more QMS established by the federal government or SDO, including more burdensome on small health IT developers.

A few commenters requested clarifications. A commenter noted that health IT developers use agile software development practices and requested clarification if these processes would be sufficient for certification. A commenter asked how this criterion would apply to a self-developer or open source software. A couple of commenters asked how Health IT Modules would be evaluated against this criterion, including what type of documentation would be required for

mapping and whether a documented combined QMS approach for the entire Health IT Module would be sufficient in lieu of a capability by capability identification.

Response. We thank commenters for their feedback and support. We have adopted this criterion as proposed with further clarification in response to comments. We note that this criterion applies to any health IT presented for certification to the 2015 Edition, including self-developed and open source software that is part of the Health IT Module because one of the goals of this criterion is to improve patient safety through QMS.

We expect that ONC-ACBs will certify health IT to this criterion in the same manner as they certify health IT to the 2014 Edition QMS criterion, but accounting for any differences that are finalized through the 2015 Edition ACD test procedure. To this point, we have removed the term "compliant" from the provision requiring identification of a QMS compliant with a quality management system established by the federal government or a standards developing organization. Similar to the mapping provision, the focus and intent of the provision (and the criterion as a whole) is the identification of the QMS, not a determination of compliance by the ONC-ACB. We note that the identification of a single QMS is permitted for a Health IT Module, which is consistent with testing and certification to the 2014 Edition QMS certification criterion.

As noted in the 2014 Edition final rule (77 FR 54191), we agree that existing standards may not explicitly state support for agile development methodologies and that such methods may be part of an optimal QMS. As such, documented agile development methodologies may be used in meeting the mapping provision of this criterion. We will issue further compliance guidance as necessary, including through the 2015 Edition QMS test procedure. This guidance will include updated identification of QMS standards and more specification of documentation requirements necessary to meet this criterion. Overall, we do not believe this criterion presents a significant

burden as many health IT products have been previously certified to the 2014 Edition QMS criterion and most, if not all, developers (with previously certified products or not) should have QMS documentation readily available for their health IT products as a standard practice.

- Accessibility-Centered Design

2015 Edition Health IT Certification Criterion § 170.315(g)(5) (Accessibility-centered design)

We proposed to adopt a new 2015 Edition "accessibility-centered design" certification criterion that would apply to all Health IT Modules certified to the 2015 Edition and require the identification of user-centered design standard(s) or laws for accessibility that were applied, or complied with, in the development of specific capabilities included in a Health IT Module or, alternatively, the lack of such application or compliance.

We proposed to require that for each capability that a Health IT Module includes and for which that capability's certification is sought, the use of a health IT accessibility-centered design standard or compliance with a health IT accessibility law in the development, testing, implementation, and maintenance of that capability must be identified. Further, we proposed to permit that a health IT developer could document that no health IT accessibility-centered design standard or law was applied to the health IT's applicable capabilities as an acceptable means of satisfying this proposed certification criterion. We added that the method(s) used to meet this proposed criterion would be reported through the open data CHPL. We solicited comment on whether the standards and laws identified in the Proposed Rule were appropriate examples and whether we should limit the certification criteria to which this criterion would apply.

We explained that the proposed certification criterion would serve to increase transparency around the application of user-centered design standards for accessibility to health IT and the compliance of health IT with accessibility laws. We stated that this transparency

would benefit health care providers, consumers, governments, and other stakeholders, and would encourage health IT developers to pursue the application of more accessibility standards and laws in product development that could lead to improved usability for health care providers with disabilities and health care outcomes for patients with disabilities.

We also proposed to revise § 170.550 to require ONC-ACBs follow this proposed approach and referred readers to section IV.C.2 of the Proposed Rule's preamble for this proposal.

Comments. The vast majority of commenters supported the proposed criterion and its approach, with broad support across health IT developers, providers, and consumers. One commenter suggested that we narrow the list of example standards to those that have the widest applicability to EHRs. Another commenter suggested that the focus should be on more accessibility-centered standards such as ISO 9241-20 (2008) "Ergonomics of Human-System Interaction - Part 20: Accessibility guidelines for information/communication technology (ICT) equipment and services," ISO 9241-171 (2008) "Ergonomics of Human-System Interaction - Part 171: Guidance on software accessibility," Section 508 of the Rehabilitation Act, and Section 504 of the Rehabilitation Act. A few commenters suggested that this criterion would have a significant development burden for health IT developers. One commenter requested clarification on how testing and certification will be conducted.

Response. We thank commenters for their feedback. We have adopted this criterion as proposed. We will work with our federal partners (e.g., NIST, Administration for Community Living and Aging Policy, and the HHS Office for Civil Rights) and consider comments on the final test procedure for this criterion in providing more precise identification and guidance on accessibility-centered standards and laws. We believe this criterion poses minimal burden on

health IT developers as it only requires health IT developers to identify relevant standards or laws; and, alternatively, permits a health IT developer to state that its health IT product presented for certification does not meet any accessibility-centered design standards or any accessibility laws. That said, as noted above, we remind health IT developers and providers that the existence of an option to certify that health IT products do not meet any accessibility design standards or comply with any accessibility laws does not exempt them from their independent obligations under applicable federal civil rights laws, including Section 504 of the Rehabilitation Act, Section 1557 of the Affordable Care Act, and the Americans with Disabilities Act that require covered entities to provide individuals with disabilities equal access to information and appropriate auxiliary aids and services as provided in the applicable statutes and regulations.

We expect that ONC-ACBs will certify health IT to this criterion in the same manner as they certify health IT to the 2014 Edition QMS criterion, but accounting for any differences that are finalized through the 2015 Edition ACD test procedure. We will issue further compliance guidance as necessary.

- Consolidated CDA Creation Performance

2015 Edition Health IT Certification Criterion § 170.315(g)(6) (Consolidated CDA creation performance)

We proposed to adopt a new certification criterion at § 170.315(g)(6) that would rigorously assess a product's C-CDA creation performance (for both C-CDA Release 1.1 and 2.0) when it is presented for a Health IT Module certification that includes within its scope any of the proposed certification criteria that require C-CDA creation (e.g., "transitions of care" at § 170.315(b)(1)). We explained that to implement this proposal, we would amend § 170.550 to add a requirement that ONC-ACBs shall not issue a Health IT Module certification to a product that includes C-CDA creation capabilities within its scope, unless the product was also tested and

satisfied the certification criteria requirements proposed at § 170.315(g)(6). If the scope of certification included multiple certification criteria that require C-CDA creation, we noted that § 170.315(g)(6) need only be tested in association with one of those certification criteria and would not be expected or required to be tested for each. Specifically, we proposed that three technical outcomes be met: reference C-CDA match, document template conformance, and vocabulary conformance.

We noted that we coordinated with our colleagues at NIST and understand that NVLAP-Accredited Testing Laboratories would retain the C-CDA files created under test and contribute them to an ONC-maintained repository.

Comments. A number of commenters expressed support for the proposal for this certification criterion that would test a Health IT Module's C-CDA creation performance as proposed. Some commenters suggested that the gold standard needs to be specific on what to do with optionality permitted in the C-CDA standard. A few commenters requested clarifications on how the gold standard would be structured, whether it would be one or multiple documents, and whether the testing would be done through an automated tool or by visual inspection.

Response. We thank commenters for their support and have adopted a C-CDA creation performance certification criterion with the following changes described below. As discussed in the 2014 Edition Release 2 proposed rule (79 FR 10899), we continue to believe in the value of this capability to promote the ability of providers to exchange C-CDA documents and subsequently be able to parse and use the C-CDA received. This is especially important for interoperability when the C-CDA standard allows for optionality and variations.

We intend to publish sample gold standard C-CDA documents on www.healthit.gov or another ONC-maintained repository for the public to review and provide comment. We also

anticipate that there will be multiple gold standard documents for each C-CDA document template we require for this criterion with variations in each to test optionality for which the C-CDA standard allows. With respect to testing, we anticipate that testing will be performed, at a minimum, through a conformance testing tool and could also include visual inspection as necessary to verify reference C-CDA match, document template conformance, and vocabulary conformance.

Comments. Similar to comments received to other certification criteria such as "transitions of care," commenters did not support the proposal to be able to create C-CDA documents in accordance with both C-CDA Releases 1.1 and 2.0.

Response. We have adopted C-CDA Release 2.1 for this certification criterion for the same reasons as noted in the preamble for the "transitions of care" criterion.

C-CDA Document Templates

We proposed that Health IT Modules would have to demonstrate compliance with the C-CDA creation performance functions of this criterion for the following C-CDA Release 2.0 document templates:

- Continuity of Care;
- Consultation Note;
- History and Physical;
- Progress Note;
- Care Plan;
- Transfer Summary;
- Referral Note; and
- Discharge Summary (for inpatient settings only).

Comments. A few commenters suggested that ONC not require certification to all proposed document templates and indicated that not all document templates are applicable to every setting. They also cited potential development burdens with the proposed scope.

Response. As discussed in the preamble for other certification criteria that include C-CDA creation within its scope, we have limited the C-CDA Release 2.1 document template requirements based on the use case for each certification criterion. Therefore, some criteria (e.g., ToC) require three C-CDA templates whereas others (e.g., care plan) only require one C-CDA template. As such, we have required that C-CDA creation performance be demonstrated for the C-CDA Release 2.1 document templates required by the 2015 Edition certification criteria presented for certification. For example, if a Health IT Module only included §170.315(e)(1) within its certificate's scope, then only the Continuity of Care Document (CCD) document template would be applicable within this criterion. Conversely, if a Health IT Module designed for the inpatient setting included §170.315(b)(1) within its certificate's scope, then all three document templates referenced by that criterion would need to evaluated as part of this certification criterion.

If the scope of certification includes more than one certification criterion with C-CDA creation required, C-CDA creation performance only has to be demonstrated once for each C-CDA document template (e.g., C-CDA creation performance to the CCD template would not have to demonstrated twice if the Health IT Module presents for certification to both "ToC" and the "data export" criteria).

Comments. One commenter was concerned that the proposed regulation text language "upon the entry of clinical data consistent with the Common Clinical Data Set" implies the incorrect workflow, and would only allow creation to be done while the user finishes creating or

composing the C-CDA document. The commenter noted that there is an additional step between creation and sending where additional vocabulary mapping steps need to be applied.

Response. We thank the commenter for the input. We clarify that the purpose of the phrase was to provide a clear scope to the certification criterion for health IT developers. Given that the C-CDA includes many section templates to represent data outside of the data specified by the Common Clinical Data Set definition, we sought to indicate that testing would be limited to only the data within scope for the Common Clinical Data Set definition. We have modified the language in the certification criterion to more clearly reflect this scope limitation.

C-CDA Completeness

Due to past feedback from providers that indicated the variability associated with different functionalities and workflows within certified health IT can ultimately affect the completeness of the data included in a created C–CDA, we requested comment on a proposal that would result in a certification requirement to evaluate the completeness of the data included in a C-CDA. This additional requirement would ensure that the data recorded by a user in health IT is equivalent to the data included in a created C-CDA.

Comments. We received mixed comments in response to this request for comment. One commenter was supportive of the proposal. Another commenter requested clarification on whether the request for comment intended to specify how the user interface captures specific data using specific vocabulary, and was not supportive of imposing data capture requirements for this criterion. One commenter was concerned that ONC was being too prescriptive by soliciting comment on this potential requirement to test C-CDA completeness and suggested ONC test this in a sub-regulatory manner and/or through improved conformance test tools. One commenter suggested that some C-CDA document templates do not include all information entered into an

EHR for certain use cases, as some document templates are meant to include targeted and specific information for a particular setting to which a patient is being transitioned.

Response. We thank commenters for the input and, in consideration of the comments, have adopted this proposal as part of this certification criterion. As we stated in the Proposed Rule, the intent and focus of this proposal was to ensure that however data is entered into health IT – via whatever workflow and functionality – that the C-CDA output would reflect the data input and not be missing data a user otherwise recorded. We also clarify that the scope of the data for this certification criterion is limited to the Common Clinical Data Set definition. We did not intend imply and note that that this criterion does not prescribe how the user interface captures data.

Repository of C-CDA Documents

We did not receive any comments regarding our understanding that NVLAP-Accredited Testing Laboratories would retain the C-CDA files created under test and contribute them to an ONC-maintained repository. We note that we intend to implement this repository as noted in the Proposed Rule.

- Application Access To Common Clinical Data Set

2015 Edition Health IT Certification Criterion § 170.315(g)(7) (Application access – patient selection)

2015 Edition Health IT Certification Criterion § 170.315(g)(8) (Application access – data category request)

2015 Edition Health IT Certification Criterion § 170.315(g)(9) (Application access – all data request)

We proposed a new 2015 Edition criterion at § 170.315(g)(7) that would require health IT to demonstrate it could provide application access to the Common Clinical Data Set via an application programming interface (API), and requiring that those same capabilities be met as

part of the "VDT" criterion. We noted that providing API functionality could help to address many of the challenges currently faced by individuals and caregivers accessing their health data, including the "multiple portal" problem, by potentially allowing individuals to aggregate data from multiple sources in a web or mobile application of their choice. We emphasized that the proposed approach was intended to provide flexibility to health IT developers to implement an API that would be most appropriate for its customers and allow developers to leverage existing standards that most health IT developers would already need in order to seek certification for other criteria.

Because many commenters provided feedback on the "API" criterion within the context of the "VDT" criterion and in the order of this final rule the VDT discussion comes first, we address all comments to proposed § 170.315(g)(7) here.

Comments. The HITSC recommended that we permit Health IT Modules to certify towards each of the three API scenarios (get patient identifier, get document, get discrete data) individually, while stating the expectation that Health IT developers and provider organizations should ensure that the APIs work together functionally. The HITSC also recommended providing a "sub-regulatory flexibility" certification testing approach to allow developers to achieve certification by participating in "a public-private effort that provides adequate testing and other governance sufficient to achieve functional interoperability."

Response. We agree with the approach suggested by the HITSC to split our original proposed certification criterion into three separate certification criteria with each individual criterion focused on specific functionality. Based on prior experience with certification criteria that "lump" functionality together that can otherwise be separately performed, we believe that this additional flexibility will allow for health IT developers to be more innovative. This will

enable additional modularity as part of the ONC Health IT Certification Program in the event that a health IT developer seeks to change and recertify one of the three API functionalities and leave the other two capabilities unchanged. The three certification criteria will be adopted at § 170.315(g)(7), (g)(8), and (g)(9). Each will include the documentation and terms of use requirement that was part of the single proposed criterion. Additionally, in consideration of this change and because CMS has required as part of the EHR Incentive Program Stage 3 and Modifications final rule that providers will need to have health IT certified to both the VDT certification criterion and these three "API" criteria to meet Stage 3 Objectives 5 and 6, we have removed the API functionality embedded within the VDT certification criterion and adopted these three criteria to simplify our rule and reduce redundancy.

For the purposes of testing for each of the "API" certification criteria, a health IT developer will need to demonstrate the response (i.e., output) for each of the data category requests and for the "all" request, the output according to the C-CDA in the CCD document template. For all other aspects of these certification criteria, we expect the testing would include, but not be limited to, attestation, documentation, functional demonstration, and visual inspection.

We appreciate suggestions as to a "sub-regulatory approach" and will consider whether such approaches could fit within our regulatory structure as well as lead to consistent and efficient testing and certification.

Comments. Multiple commenters voiced concern that we did not name a standard for API functionality in the Proposed Rule. Of these commenters, some suggested that we specifically name FHIR as the standard for this criterion, while others expressed concern that FHIR is not yet mature enough for inclusion in regulation, and suggested that ONC eliminate or make optional

API functionality until a time when API standards have undergone more testing in the market. However, many commenters strongly supported the inclusion of API functionality for patient access, discussing the criterion's provision of more flexibility and choice for the consumer, better facilitation of communication and education for individuals, fostering of more efficient and modern information exchange, and encouraging innovation by app developers and entrepreneurs to create better online experiences for users. Several commenters also voiced support for the approach of encouraging movement towards APIs, without locking in any specific standard, and urged ONC to maintain an open, transparent process with public input as it works with industry to identify and develop emerging standards in this space.

Response. We have adopted three new criteria as a new component of the 2015 Base EHR definition in § 170.102. We appreciate the number of detailed and thoughtful comments on this criterion, and the concerns regarding standardization. We agree with the many comments supportive of the inclusion of API functionality for Health IT Modules, and note that in addition to enhanced flexibility for consumers and increased innovation, we believe that the "API" criteria will enable easier access to health data for patients via mobile devices, which may particularly benefit low income populations where smartphone and tablet use may be more prevalent than computer access. Regarding comments on standardization, we believe that the criterion is at an appropriate level of specificity given the ongoing development of API standards for health care, and continue to support our initial proposal to allow for a flexible approach without naming a specific standard. However, we emphasize that we intend to adopt a standards-based approach for certification in the next appropriate rulemaking and we note the existence and ongoing piloting of promising work such as the Fast Healthcare Interoperability Resources (FHIR) specification. We agree with commenters' suggestions that ONC continue to monitor and

actively participate in industry efforts to support testing of these and other emerging standards. We understand that many Health IT Modules have APIs today and providing for flexibility in the final rule will allow them to certify their existing APIs.

Security

We proposed that the API include a means for the establishment of a trusted connection with the application that requests patient data. We stated that this would need to include a means for the requesting application to register with the data source, be authorized to request data, and log all interactions between the application and the data source.

Comments. Multiple commenters cited a need to provide security standards for this criterion while also noting that current and emerging standards, such as OAuth, are not yet tested and fully mature for inclusion in regulation. Other commenters suggested that ONC specifically name OAuth and/or some combination of OAuth, Open ID Connect, and User Managed Access (UMA) as the standards for authentication and authorization within this criterion. A few commenters cited other standards, such as HTTPS and SSL/TLS. Multiple commenters noted that the consumers of the API – the web and mobile applications – were ultimately the entities responsible for security, rather than the Health IT Module itself, and that the market for third party applications is currently unregulated.

Response. We have adopted a final criterion without the proposed requirement for registration of third party applications. Our intention is to encourage dynamic registration and strongly believe that registration should not be used as a means to block information sharing via APIs. That is, applications should not be required to pre-register (or be approved in advance) with the provider or their Health IT Module developer before being allowed to access the API. Under the 2015 Edition privacy and security (P&S) certification framework, health IT

certified to the API criteria must support an application connecting to the API. The P&S certification framework for the API criteria requires that a Health IT Module certified to this criterion be capable of ensuring that: valid user credentials such as a username and password are presented (that match the credentials on file at the provider for that user); the provider can authorize the user to view the patient's data; the application connects through a trusted connection; and the access is audited (§ 170.515(d)(1); (d)(9); and (d)(2) or (d)(10); respectively). These certification requirements should be sufficient to allow access without requiring further application pre-registration. The applicable P&S certification criteria are discussed in more detail below.

We intend to pursue a standards-based approach for this criterion in the future, but believe that providing flexibility currently is more appropriate as emerging standards continue to mature and gain traction in industry, and consistent with our overall "functional" approach to the API certification criteria at § 170.315(g)(7), (g)(8), (g)(9). We recognize and encourage the work being done to develop emerging standards in this space, including OAuth, OpenID Connect, UMA, and the Open ID Foundation's HEART profile. Accordingly, we emphasize that the security controls mentioned in the Proposed Rule establish a floor, not a ceiling. We encourage organizations to follow security best practices and implement security controls, such as penetration testing, encryption, audits, and monitoring as appropriate, without adversely impacting a patient's access to data, following their security risk assessment. We expect health IT developers to include documentation on how to securely deploy their APIs in the public documentation required by the certification criteria and to follow industry best practices. We also seek to clarify that a "trusted connection" means the link is encrypted/integrity protected according to § 170.210(a)(2) or (c)(2). As such, we do not believe it is necessary to specifically

name HTTPS and/or SSL/TLS as this standard already covers encryption and integrity protection for data in motion.

While we appreciate the concerns of commenters regarding privacy and security of third party applications, we note that the regulation of third party applications is outside the scope of certification, unless those applications are seeking certification as Health IT Modules. As consumer applications, third-party applications may fall under the authority of the Federal Trade Commission (FTC). In addition, if third-party applications are offered on behalf of a HIPAA covered entity or business associate, they would be governed by the HIPAA Privacy and Security Rules as applicable to those entities. We also note that the Federal Trade Commission and the National Institute of Standards and Technology (NIST) have issued guidance regarding third-party applications; we encourage third-party application developers to take advantage of these resources.[122]

Comments. Commenters pointed out that the proposed process for certifying security & privacy requirements for the "Application Access to Common Clinical Data Set" criterion was inconsistent with the proposed privacy and security certification approach listed in Appendix A of the Proposed Rule's preamble. The HITSC recommended that we include encryption and integrity protection as a security requirement for the "API" criterion.

Response. We agree with commentators that the approach from our prior rules and our most recent Proposed Rule were inconsistent. We have finalized an approach that standardizes the way Health IT Modules certify for privacy and security (P&S). For consistency, we have

[122] See, e.g., NIST Technical Considerations for Vetting 3rd Party Mobile Applications, *available at* http://csrc.nist.gov/publications/drafts/800-163/sp800_163_draft.pdf; FTC, Careful Connections: Building Security in the Internet of Things (Jan. 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things; FTC, Mobile App Developers: Start with Security (Feb. 2013), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security

moved the trusted connection security requirements included proposed § 170.315(g)(7)(i) into two new certification criteria under § 170.315(d) and have applied them back to the three adopted "API" certification criteria as part of the 2015 Edition P&S certification framework (§ 170.550(h)).[123] To be certified for the "API" criteria, a Health IT Module must certify to either Approach 1 (technically demonstrate) or Approach 2 (system documentation) for the following security criteria:

- Section 170.315(d)(1) "authentication, access control, and authorization;"
- Section 170.315(d)(9) "trusted connection;" and
- Section 170.315(d)(10) "auditing actions on health information" or § 170.315(d)(2) "auditable events and tamper resistance."

We intended the trusted connection requirement to encompass encryption and integrity. The "trusted connection" criterion at § 170.315(d)(9) requires health IT to establish a trusted connection in accordance with the standards specified in § 170.210(a)(2) and (c)(2). We have adopted § 170.315(d)(10) "auditing actions on health information" as an abridged version of § 170.315(d)(2) "auditable events and tamper resistance" as some of the capabilities included in § 170.315(d)(2) would likely not apply to a Health IT Module certified only to the "API" criteria, such as recording the audit log status or encryption status of electronic health information locally stored on end-user devices by the technology. A Health IT Module presented for certification to the "API" criteria, depending on the capabilities it included for certification, could be certified to either § 170.315(d)(2) or (d)(10) as part of the 2015 Edition P&S certification framework.

[123] We refer readers to section IV.C.1 ("Privacy and Security") of this preamble for further discussion of the 2015 Edition P&S certification framework.

We have removed the requirement that the API must include a means for the requesting application to register with the data source. Our intention was that APIs should support dynamic registration that does not require pre-approval before an application requests data from the API. However, from the comments received it was clear that our intention was not understood. Further, open source standards for dynamic registration are still under active development, there is currently no consensus-based standard to apply, and we do not want registration to become a barrier for use of Health IT Modules' APIs. We are removing this requirement at this time for the purposes of certification and will consider verifying this technical capability for a potential future rulemaking.

Comments. Several commenters expressed concern that APIs may increase security risks. In particular, these commenters called for security standards to specify the manner in which the API is authorized, authenticated, and how data must be secured in transit.

Response. Entities must follow federal and state requirements for security. APIs, like all technology used in a HIPAA-regulated environment, must be implemented consistent with the HIPAA Security Rule. Namely, covered entities and their business associates must perform a security risk assessment and must meet the HIPAA Security Rule standards, consistent with their risks to the administrative, technical, and physical security of the ePHI they maintain. The security safeguards required by certification establish a floor of security controls that all APIs must meet; an organization's security risk assessment may reveal additional risks that must be addressed in the design or implementation their EHR's particular API or they may have additional regulatory requirements for security. Therefore, users of health information technology should include APIs in their security risk analysis and implement appropriate security safeguards. We also strongly encourage health IT developers to build security into their APIs and

applications following best practice guidance, such as the Department of Homeland Security's Build Security In initiative.[124] We also reiterate that at this time, we are requiring a read-only capability—read-only capabilities may have fewer security risks because the EHR does not consume external data.

Provider organizations already transmit information outside their networks such as electronic claims submission, lab orders, and VDT messages. These transmissions may be occurring using APIs today. Therefore, provider organizations could already be implementing safeguards needed to secure APIs. We encourage providers to employ resources released by OCR and ONC, such as the Security Risk Assessment Tool[125] and the Guide to Privacy and Security of Electronic Health Information[126], as well as the Office for Civil Rights' website[127] to make risk-based decisions regarding their implementation of APIs and the selection of appropriate and reasonable security safeguards.

It is important to recognize that an API may be used to enable a patient to access data in the Designated Record Set for that individual, pursuant to 45 CFR 164.524(a)(1)[128]. Additionally, the electronic tools an individual uses to handle or transport data in the individual's custody are not required to meet the HIPAA Security Rule. Those tools cannot pose an unreasonable threat to the covered entity's system, but the tools used by the individual themselves are not regulated by HIPAA. For example, a patient may insist that in providing an electronic copy of data about them, the email that delivers the ePHI to the patient is not

---

[124] https://buildsecurityin.us-cert.gov/
[125] ONC Security Risk Assessment Tool: http://www.healthit.gov/providers-professionals/security-risk-assessment
[126] ONC Guide to Privacy and Security of Electronic Health Information: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
[127] HHS Office for Civil Rights: http://www.hhs.gov/ocr/office/index.html
[128] 45 CFR 164.524(a)(1): http://www.gpo.gov/fdsys/pkg/CFR-2013-title45-vol1/xml/CFR-2013-title45-vol1-sec164-501.xml

encrypted.[129] A patient may also select a third party product that will receive their data through the API that is not subject to HIPAA Security Rule requirements.

Comments. Several commenters stated that APIs should align with patient privacy expectations.

Response. We appreciate the commenters' concerns about patient privacy expectations and agree that use of APIs must align with all federal and state privacy laws and regulations. We expect APIs to be used in circumstances when consent or authorization by an individual is required, as well as in circumstances when consent or authorization by an individual is not legally required for access, use or disclosure of PHI. In other words, APIs, like faxes before them, will be used in light of the existing legal framework that already supports the transmission of protected health information, sensitive health information, and applicable consent requirements.

In circumstances where there is a requirement to document a patient's request or particular preferences, APIs can enable compliance with such documentation requirements. The HIPAA Privacy Rule[130] permits the use of electronic documents to qualify as writings for the purpose of proving signature, e.g., electronic signatures. Electronic signatures can be captured by a patient portal or an API, absent the application of a more privacy-protective state law.

The existing legal framework would support the use of APIs to facilitate patient access to electronic health information or patient access requests made pursuant to 45 CFR 164.524 to transmit their information to a designated third party. For example, an individual may request a copy of their data from their provider's API using software tools of the individual's choosing.

---

[129] HHS Office for Civil Rights FAQs on HIPAA: http://www.hhs.gov/ocr/privacy/hipaa/faq/health_information_technology/570.html

[130] 45 CFR Part 160 and Part 164, Subparts A and E

Assuming the individual has been properly authenticated and identity-proofed, the provider's obligation under HIPAA is to fulfill the "access" request through the API if that functionality is available, because that is the medium so chosen by the patient. The addition of APIs to the technical landscape of health IT does not alter HIPAA requirements, which support reliance on the established and prevailing standards for electronic proof of identity.[131] This policy supports the availability of health information for treatment, payment, and health care operations (45 CFR 164.506) and leverages the progress already made to operationalize privacy laws in an electronic environment, while facilitating interoperability.

Patient Selection

We proposed that the API would need to include a means for the application to query for an identification (ID) or other token of a patient's record in order to subsequently execute data requests for that record.

Comments. Commenters noted that standardization of this requirement should include industry-accepted standards such as IHE PDQ or PIX query.

Response. Consistent with our approach throughout the "API" criteria, we decline to require a specific standard at this time, although we intend to do so in a future rulemaking. We note that the standards suggested by commenters have been adopted in industry and we encourage Health IT Modules to identify and implement any existing standards that best support the needs of their users. We have adopted these final requirements in the certification criterion adopted in § 170.315(g)(7). It includes the proposed requirement with specific conforming adjustments to be its own certification criterion. The criterion specifies that technology will need to be able to receive a request with sufficient information to uniquely identify a patient and

[131] NIST SP 800-63-2

return an ID or other token that can be used by an application to subsequently execute requests for that patient's data. We do not presume or prescribe a particular method or amount of data by which technology developer implements its approach to uniquely identify a patient. However, we note that such information must be included in the technical documentation also required to be made available as part of certification. Once the specific ID or other token is returned in a response, we expect and intend for the other "API" criteria discussed below to be able to use the ID or other token to then perform the data requests.

Data Requests, Response Scope, and Return Format

We proposed that the API would need to support two types of data requests and responses: "by data category" and "all." In both cases, the proposed scope for certification was limited to the data specified in the Common Clinical Data Set. For "by data category," the API would need to respond to requests for each of the data categories specified in the Common Clinical Data Set and return the full set of data for that data category. We also proposed that as the return format for the "by data category," that either XML or JSON would need to be produced. "All" requests for a specific patient would return a patient's fully populated summary record formatted in accordance with the C-CDA version 2.0.

Comments. Commenters suggested several specific changes to this criterion, including: we should clarify that access is for a specific patient; we should include a requirement that applications be able to request specific date ranges, ability to request patient lists or other identified populations; and we should remove the return format of either XML or JSON, because some APIs could return data in HL7 v2 format. For the "data category" request requirement, commenters asked that ONC clarify whether "each" means a query limited to one category at a time, or whether combinations of categories can be requested at one time. For "all" requests,

some commenters suggested that this functionality should support the ability to view or download based on specific data, time, or period of time; other commenters urged us to focus first on the narrow set of capabilities initially proposed to gain experience, and add additional capabilities in future certification. Most commenters supported focusing on the CCD document to create clear expectations and enhance interoperability. Two commenters were opposed to restricting the use of C-CDA 2 to CCD document type because other document types (i.e. Transfer Summary, Referral Note and Care Plan) are very commonly used documents in the real world, and would not be available through this functionality.

Response. We expect that all three API capabilities would function together; thus applications connecting to the API would be able to request data on a specific patient, as described in the "API – patient selection" criterion, using an obtained ID or other token. At this time, we have decided not to include an additional patient list creation requirement. However, we emphasize that this initial set of APIs represents a floor rather than a ceiling, and we expect developers to build enhanced APIs to support innovation and easier, more efficient access to data in the future.

In response to concerns regarding the return format for the data-category request, we have decided to make that requirement more flexible and have removed the specific proposed language of XML or JSON to say in the final criterion that the returned data must be in a computable (i.e., machine readable) format.

In response to comments concerning the "all-request," we clarify that the API functionality must be able to respond to requests for all of the data included in the CCDS on which there is data for patient, and that the return format for this functionality would be limited to the C-CDA's CCD document template. We believe that focusing on the CCD document

template will reduce the implementation burden for health IT developers to meet this certification criterion and will help application developers connecting to Health IT Modules' APIs because they will know with specificity what document template they are going to receive.

With regard to requests for each "data category," for the purposes of certification, the technology must demonstrate that it can respond to requests for each individual data category one at a time. However, this is a baseline for the purposes of testing and certification and health IT developers are free to enable the return of multiple categories at once if they choose to build out that functionality.

Similar to our response for "VDT" criterion, we clarify that patients should be provided access to any data included in the Common Clinical Data Set.

As with the VDT requirement, we have adopted date and time filtering requirements as part of this criterion. We agree with commenters that adding this functionality to these criteria will provide clarity that patients should have certain baseline capabilities available to them when it comes to selecting the data (or range of data) they wish to access using an application that interacts with the Health IT Module's APIs. Specifically, we have adopted two timeframe requirements: First, to ensure that an application can request data associated with a specific date, and the second, to ensure that an application can request data within an identified date range, which must be able to accommodate the application requesting a range that includes all data available for a particular patient. The technology specifications should be designed and implemented in such a way as to return meaningful responses to queries, particularly with regard to exceptions and exception handling, and should make it easy for applications to discover what data exists for the patient.

<u>Documentation and Terms of Use</u>

We proposed that the required technical documentation would need to include, at a minimum: API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns. We also stated that the terms of use must include the API's developer policies and required developer agreements so that third-party developers could assess these additional requirements before engaging in any development against the API. We also proposed that health IT developers would need to submit a hyperlink to ONC-ACBs, which the ONC-ACB would then submit as part of its product certification submission to the Certified Health IT Product List (CHPL) that would allow any interested party to view the API's documentation and terms of use.

Comments. One commenter suggested that ONC should clarify whether our intent is that terms of use would replace, include, or overlap with HIPAA privacy policies that health care providers are required to provide their patients. Another commenter voiced concern that the API-consuming application should be the party responsible for assuring effective use of the API in terms of safety, security, privacy, and accessibility. Multiple commenters suggested that ONC place certain restrictions on terms of use, including limits on any fees, copyright, or licensing requirements on APIs.

Response. We emphasize that nothing in this criterion is intended to replace federal or state privacy laws and regulations, nor the contractual arrangements between covered entities and business associates. Placing requirements or limitations on the specific content of the terms of use is beyond the scope of certification. However, we reiterate that our policy intent is to allow patients to access their data through APIs using the applications of their own choosing, and limit the creation of “walled gardens” of applications that only interact with certain Health IT Modules. As stated previously in this preamble, we intend to require a standards-based approach

to this criterion in the next appropriate rulemaking and we encourage vendors to start piloting the use of existing and emerging API standards. By requiring that documentation and terms of use be open and transparent to the public by requiring a hyperlink to such documentation to be published with the product on the ONC Certified Health IT Product List, we hope to encourage an open ecosystem of diverse and innovative applications that can successfully and easily interact with different Health IT Modules' APIs.

- Transport Methods and Other Protocols

We proposed two ways for providers to meet the 2015 Edition Base EHR definition using health IT certified to transport methods. The first proposed way to meet the proposed 2015 Edition Base EHR definition requirement would be for a provider to have health IT certified to § 170.315(b)(1) and (h)(1) (Direct Project specification). This would account for situation where a provider uses a health IT developer's product that acts as the "edge" and the HISP. The second proposed way would be for a provider to have health IT certified to § 170.315(b)(1) ("ToC" criterion) and (h)(2) ("Direct Project, Edge Protocol, and XDR/XDM"). This would account for situations where a provider is using one health IT developer's product that serves as the "edge" and another health IT developer's product that serves as a HISP.[132] To fully implement this approach, we proposed to revise § 170.550 to require an ONC-ACB to ensure that a Health IT Module includes the certification criterion adopted in § 170.315(b)(1) in its certification's scope in order to be certified to the certification criterion proposed for adoption at § 170.315(h)(1). We lastly proposed to revise the heading of § 170.202 from "transport standards" to "transport standards and other protocols."

[132] See the 2014 Edition Release 2 final rule for more discussion on such situations (79 FR 54436-38).

We received minimal comments on these proposals and discussed what comments we received under the "Direct Project, Edge Protocol, and XDR/XDM" certification criterion below.

- Direct Project

2015 Edition Health IT Certification Criterion § 170.315(h)(1) (Direct Project)

We proposed to adopt a certification criterion that includes the capability to send and receive according to the Applicability Statement for Secure Health Transport (the primary Direct Project specification). We noted that we previously adopted this capability for the 2014 Edition at § 170.314(b)(1), (b)(2) and (h)(1). We proposed to include as an optional capability for certification the capability to send and receive according to the Implementation Guide for Delivery Notification in Direct, Version 1.0, June 29, 2012 ("Delivery Notification IG"). We explained that the primary Direct Project lacked certain specificity and consistency guidance such that deviations from normal message flow could result if Security/Trust Agents (STAs) implemented only requirements denoted as "must" in Section 3 of the primary Direct Project. As a result, STAs may not be able to provide a high level of assurance that a message has arrived at its destination. We further stated that the Delivery Notification IG provides implementation guidance enabling STAs to provide a high level of assurance that a message has arrived at its destination and outlines the various exception flows that result in compromised message delivery and the mitigation actions that should be taken by STAs to provide success and failure notifications to the sending system.

Comments. Commenters overwhelmingly supported the adoption of this criterion as proposed. Many commenters also expressed strong support for the optional delivery notification provision as a means to support specific business practices. Some commenters stated that delivery notification will only work when both receiving and sending parties support the

functionality and, thus, delivery notification must be required of both sending and receiving entities in order for it to work. Commenters also requested clarification regarding "ownership" and maintenance of the Direct Project, including some that recommended that "ownership" should belong to a SDO.

Response. We have adopted a revised criterion in comparison to our proposal and the related 2014 Edition certification criteria. After careful consideration of comments, we believe it is appropriate to adopt the Applicability Statement for Secure Health Transport, Version 1.2 (August 3, 2015)[133]. This new version of the specification includes updates that improve interoperability through the clarification of requirements that have been subject to varying interpretations, particularly requirements around message delivery notifications. This version also clarifies pertinent requirements in the standards underlying the Applicability Statement for Secure Health Transport. Migration to this newer version will provide improvements for exchange of health information and should have minor development impacts on health IT developers. Further, we expect that many developers and technology organizations that serve as STAs will quickly migrate to version 1.2 due to its improvements. We note, for certification to this criterion, we have made it a requirement to send and receive messages in only "wrapped" format even though the specification (IG) allows use of "unwrapped" messages. This requirement will further improve interoperability among STAs, while having minor development impact on health IT developers.

We have also adopted as a requirement for this criterion the Implementation Guide for Delivery Notification in Direct, Version 1.0, June 29, 2012. While we proposed this IG as an

133 http://wiki.directproject.org/file/view/Applicability%20Statement%20for%20Secure%20Health%20Transport%20v1.2.pdf/556133893/Applicability%20Statement%20for%20Secure%20Health%20Transport%20v1.2.pdf

optional provision, we agree with commenters that this functionality must be required to best support interoperability and exchange, particularly for both sending and receiving parties. As we stated in the 2014 Edition Release 2 proposed rule (79 FR 10914-915), the capabilities in this IG provide implementation guidance enabling HISPs to provide a high level of assurance to senders that a message has arrived at its destination, a necessary component to interoperability.

We appreciate the recommendations and questions regarding "ownership" of the Direct specifications. We clarify that although ONC played a significant role in the creation and coordination of the Direct specifications that ONC does not "own" them. Rather, the specifications are publicly available and we view them as maintained by the community of stakeholders who have and continue to support the Direct specifications. To that end, as a participant in this community, we have been working with other stakeholders to locate an appropriate SDO who can maintain and mature these specifications over the long term. We believe this step is both necessary and critical for Direct specifications to be well maintained and industry supported over time.

- Direct Project, Edge Protocol, and XDR/XDM

2015 Edition Health IT Certification Criterion § 170.315(h)(2) (Direct Project, Edge Protocol, and XDR/XDM)

We proposed a 2015 Edition "Direct, Edge Protocol, and XDR/XDM" certification criterion that included three distinct capabilities. The first proposed capability focused on technology's ability to send and receive according to the Applicability Statement for Secure Health Transport (the primary Direct Project specification). The second proposed capability focused on technology's ability to send and receive according to both Edge Protocol methods specified by the standard adopted in § 170.202(d). The third proposed capability focused on technology's ability to send and receive according to the XDR and XDM for Direct Messaging

Specification. We noted that these three capabilities were previously adopted as part the 2014 Edition, including through the 2014 Edition and 2014 Edition Release 2 final rules, and we reminded health IT developers that best practices exist for the sharing of information and enabling the broadest participation in information exchange with Direct.[134]

Comments. Commenters overwhelmingly supported the adoption of this criterion as proposed. A commenter suggested that the primary Direct Project specification should only be included in the Direct Project certification criterion (§ 170.315(h)(1)). A commenter requested clarification on the anticipated advantage(s) of certifying with XDR/XDM. A commenter stated some systems are still using SMTP and IMAP. Another commenter stated that while certified Health IT Modules may implement Direct Edge protocols there is no requirement for HISPs to adopt the protocol. Commenters also requested clarification regarding "ownership" and maintenance of the Direct project, with some recommending that "ownership" should belong to a SDO.

Response. We have adopted this as a revised criterion in comparison to our proposal and the related 2014 Edition certification criteria. After careful consideration of comments, we believe it is appropriate to adopt the Applicability Statement for Secure Health Transport, Version 1.2 (August 3, 2015)[135].This new version of the specification includes updates that improve interoperability through the clarification of requirements that have been subject to varying interpretations, particularly requirements around message delivery notifications. This version also clarifies pertinent requirements in the standards underlying the Applicability

---

[134] http://wiki.directproject.org/Best+Practices+for+Content+and+Workflow

135 http://wiki.directproject.org/file/view/Applicability%20Statement%20for%20Secure%20Health%20Transport%20v1.2.pdf/556133893/Applicability%20Statement%20for%20Secure%20Health%20Transport%20v1.2.pdf

Statement for Secure Health Transport. Migration to this newer version will provide improvements for exchange of health information and should have minor development impacts on health IT developers. Further, we expect that many developers and technology organizations that serve as STAs will quickly migrate to version 1.2 due to its improvements. For certification to this criterion, we have made it a requirement to send and receive messages in only "wrapped" format even though the specification (IG) allows use of "unwrapped" messages. This requirement will further improve interoperability among STAs while having minor development impact on health IT developers.

We have also adopted as a requirement for this criterion the Implementation Guide for Delivery Notification in Direct, Version 1.0, June 29, 2012. While we proposed this IG as an optional provision, we agree with commenters that this functionality must be required to best support interoperability and exchange, particularly for both a sending and receiving HISP. As we stated in the 2014 Edition Release 2 proposed rule (79 FR 10914-915), the capabilities in this IG provide implementation guidance enabling HISPs to provide a high level of assurance to senders that a message has arrived at its destination, a <u>necessary</u> component to interoperability.

We require the use of XDR/XDM to support interoperability and ensure that certain messages packaged using XDR/XDM can be received and processed. This is the same approach we required with the 2014 Edition. We also refer readers to the "ToC" certification criterion discussed earlier in this preamble for further explanation of the interoperability concerns related to the use of XDR/XDM. We clarify for commenters that for health IT to be certified to this criterion it must be able to support both of the Edge Protocols methods referenced in the Edge IG version 1.1 (i.e., the "IHE XDR profile for Limited Metadata Document Sources" edge protocol

or an SMTP-focused edge protocol (SMTP alone or SMTP in combination with either IMAP4 or POP3)).

We note that even though the Edge Protocol requires support for XDS limited metadata, XDR/XDM supports capability to transform messages using full metadata wherever appropriate. Therefore, we require that a Health IT Module must support both the XDS Metadata profiles (Limited and Full), as specified in the underlying IHE specifications, to ensure that the transformation between messages packaged using XDR/XDM are done with as much appropriate metadata as possible.

This criterion requires the three capabilities specified (Direct Project specification, Edge Protocol compliance, and XDR/XDM processing) because it must support interoperability and all potential certified exchange options as well as support a provider in meeting the Base EHR definition. As we discussed above, a provider could use an "independent" HISP to meet the Base EHR definition. In such a case, the HISP would need to be certified to this criterion in order for the provider to use it to meet the Base EHR definition, which is part of the CEHRT definition under the EHR Incentive Programs. Therefore, there is incentive for a HISP to be certified to this criterion.

Please see our prior response regarding the "ownership" of the Direct specifications under the "Direct Project" certification criterion.

4. Gap Certification Eligibility Table for 2015 Edition Health IT Certification Criteria

We have previously defined gap certification at 45 CFR 170.502 as the certification of a previously certified Complete EHR or EHR Module(s) to: (1) all applicable new and/or revised certification criteria adopted by the Secretary at subpart C of part 170 based on the test results of a NVLAP-accredited testing laboratory; and (2) all other applicable certification criteria adopted

by the Secretary at subpart C of part 170 based on the test results used to previously certify the Complete EHR or EHR Module(s) (for further explanation, see 76 FR 1307-1308). Our gap certification policy focuses on the differences between certification criteria that are adopted through rulemaking at different points in time. This allows health IT to be certified to only the differences between certification criteria editions rather than requiring health IT to be fully retested and recertified to certification criteria (or capabilities) that remain "unchanged" from one edition to the next and for which previously acquired test results are sufficient. Under our gap certification policy, "unchanged" criteria are eligible for gap certification, and each ONC-ACB has discretion over whether it will provide the option of gap certification.

For the purposes of gap certification, we included a table in the Proposed Rule to provide a crosswalk of the proposed "unchanged" 2015 Edition certification criteria to the corresponding 2014 Edition certification criteria (80 FR 16868). We noted that with respect to the 2015 Edition certification criteria at § 170.315(g)(1) through (g)(3) that gap certification eligibility for these criteria would be fact-specific and would depend on any modifications made to the specific certification criteria to which these "paragraph (g)" certification criteria apply.

Comments. We did not receive specific comments on the gap certification eligibility table or our described gap certification policy.

Response. We have revised the proposed "gap certification eligibility" table to reflect the adopted 2015 Edition certification criteria discussed in section III.A.3 of this preamble. Table 6 below provides a crosswalk of "unchanged" 2015 Edition certification criteria to the corresponding 2014 Edition certification criteria. These 2015 Edition certification criteria have been identified as eligible for gap certification. We note that with respect to the 2015 Edition certification criteria at § 170.315(g)(1) ("automated numerator recording") and (g)(2)

("automated measure calculation"), a gap certification eligibility determination would be fact-specific and depend on any modifications to the certification criteria to which these criteria apply and relevant Stage 3 meaningful use objectives and measures.

Table 6. Gap Certification Eligibility for 2015 Edition Health IT Certification Criteria			
2015 Edition		**2014 Edition**	
Regulation Section 170.315	**Title of Regulation Paragraph**	**Regulation Section 170.314**	**Title of Regulation Paragraph**
(a)(1)	Computerized provider order entry – medications	(a)(1)	Computerized provider order entry
		(a)(18)	Computerized provider order entry – medications
(a)(2)	Computerized provider order entry – laboratory	(a)(1)	Computerized provider order entry
		(a)(19)	Computerized provider order entry – laboratory
(a)(3)	Computerized provider order entry – diagnostic imaging	(a)(1)	Computerized provider order entry
		(a)(20)	Computerized provider order entry – diagnostic imaging
(a)(4)	Drug-drug, drug-allergy interaction checks for CPOE	(a)(2)	Drug-drug, drug-allergy interaction checks
(a)(7)	Medication list	(a)(6)	Medication list
(a)(8)	Medication allergy list	(a)(7)	Medication allergy list
(a)(10)	Drug-formulary and preferred drug list checks	(a)(10)	Drug-formulary checks
(a)(11)	Smoking status	(a)(11)	Smoking status
(d)(1)	Authentication, access control, and authorization	(d)(1)	Authentication, access control, and authorization
(d)(3)	Audit report(s)	(d)(3)	Audit report(s)
(d)(4)	Amendments	(d)(4)	Amendments
(d)(5)	Automatic access time-out	(d)(5)	Automatic log-off
(d)(6)	Emergency access	(d)(6)	Emergency access
(d)(7)	End-user device encryption	(d)(7)	End-user device encryption
(d)(11)	Accounting of disclosures	(d)(9)	Accounting of disclosures
(f)(3)	Transmission to public health agencies – reportable laboratory tests and values/results	(f)(4)	Inpatient setting only – transmission of reportable laboratory tests and values/results

5. Not Adopted Certification Criteria

This section of the preamble discusses proposed certification criteria included in the Proposed Rule that we have not adopted and requests for comments on potential certification

criteria included in the Proposed Rule. We summarize the comments received on these proposed criteria and requests for comments and provide our response to those comments.

- Vital Signs, Body Mass Index, and Growth Charts

We proposed to adopt a 2015 Edition "vital signs, BMI, and growth charts" certification criterion that was revised in comparison to the 2014 Edition "vital signs, BMI, and growth charts" criterion (§ 170.314(a)(4)). Specifically, we proposed to: 1) expand the types of vital signs for recording;[136] 2) require that each type of vital sign have a specific LOINC® code attributed to it; 3) that The Unified Code of Units of Measure, Revision 1.9, October 23, 2013 ("UCUM Version 1.9") [137] be used to record vital sign measurements; and 4) that certain metadata accompany each vital sign, including date, time, and measuring- or authoring-type source. In providing this proposal, we stated awareness that several stakeholder groups are working to define unique, unambiguous representations/definitions for vital signs along with structured metadata to increase data standardization for consistent representation and exchange. To ensure consistent and reliable interpretation when information is exchanged, we stated that vital signs should be captured natively. In addition, we proposed "optional" pediatric vital signs for health IT to electronically record, change, and access. With regard to the proposed metadata, we requested comment on additional information that we should consider for inclusion and the best available standards for representing the metadata consistently and unambiguously. We also requested comment on the on the feasibility and implementation considerations for proposals that rely on less granular LOINC® codes for attribution to vital sign measurements and the inclusion of accompanying metadata. In the Proposed Rule's section III.B.3 ("Common Clinical Data

[136] Per 80 FR 16818: systolic blood pressure, diastolic blood pressure, body height, body weight measured, heart rate, respiratory rate, body temperature, oxygen saturation in arterial blood by pulse oximetry, body mass index (BMI) [ratio], and mean blood pressure.
[137] http://unitsofmeasure.org/trac/

Set"), we stated that vital signs would be represented in same manner for the "Common Clinical Data Set" definition as it applies to the certification of health IT to the 2015 Edition, with the exception of the proposed optional vital signs.

Comments. We received mixed feedback to the overall proposal, with many commenters suggesting that 1) ONC should not be mandating how vital signs are recorded natively within certified Health IT Modules, and 2) the proposed approach to require recording of vital signs using a less granular LOINC® code with associated metadata was not a mature or the right approach for ensuring semantic interoperability. Many commenters suggested that ONC should only specify how vital signs are exchanged for the Common Clinical Data Set.

Concerning the proposal to specify how vital signs are recorded natively in a health IT system, commenters noted that there would be workflow and usability issues, such as requiring the user to enter in metadata every time a vital sign is taken. As vital signs are routinely taken as a part of every patient visit in many provider settings, this could be burdensome and time-consuming.

Regarding the proposed approach to record vital signs using a less granular LOINC® code with associated metadata, commenters had a number of concerns. Some commenters were concerned that LOINC® was designed as a pre-coordinated code system (e.g., some LOINC® codes for vital signs are pre-specified to the site of vital sign measurement, method of vital sign measurement, and/or device used to take vital sign), but that our proposal to use a less granular code with associated metadata to assist with interpretation would treat LOINC® as a post-coordinated code system. Since LOINC® does not include specific syntax rules, our proposed method could lead to data integrity issues and patient safety concerns. Commenters suggested that the industry is working to define a methodology for structured data capture through

initiatives like the S&I Framework Structured Data Capture Initiative,[138] and that ONC should not adopt requirements for structured data capture as part of certification until there is a consensus-based way forward. A few commenters were concerned that the metadata could be lost or hidden from the user's view when exchanged, resulting in the receiving user's inability to accurately and safety interpret the vital sign measurement.

Some commenters noted that SNOMED CT® is the international standard used for vital signs. One commenter noted that IHE is working with the Department of Veterans Affairs and other stakeholders to create a utility that would allow conversion from SNOMED CT® to LOINC® or to make data accessible from other countries that use SNOMED CT® for vital signs.

Many commenters suggested that the complexity of the proposed approach for recording vital signs with metadata would require extensive rework and mapping of existing systems resulting in little additional benefit for workflow, usability, and semantic interoperability. As such, commenters stated there was little incentive to certify to the proposed criterion for vital signs as it was not proposed as a requirement for participation in the EHR Incentive Programs. Commenters also noted that most 2014 Edition certified health IT capture vital signs data in different methods based on the product and provider setting, but all of them still support the exchange of vital signs as specified by the industry-accepted C-CDA standard. Thus, most health IT already supports mapping to accepted industry standards for exchange today.

Response. We thank commenters for the thoughtful and detailed feedback. We agree with commenters' concerns regarding the proposed approach to record vital signs natively within a the certified Health IT Module using less specific LOINC® codes and associated metadata. Our

138 https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCUQFjAA&url=http%3A%2F%2Fwiki.siframework.org%2FStructured%2BData%2BCapture%2BInitiative&ei=l3KiVYW-MIKU-AH0kbjwCg&usg=AFQjCNFOieJjmvmMPbgBjd2zJ3igsdJVbw&sig2=GESy7uftrinE-ohpXqMQjw

long-term goal is for a vital sign measurement to be semantically interoperable during exchange and thereby retain its meaning and be correctly interpretable by a receiving system user. As vital signs data relates to clinical decision support (CDS) and other quality reporting improvement tools, we continue to believe that vital signs should be consistently and uniformly captured in order to apply industry-developed CDS and CQM standards. However, as noted by commenters, the proposed approach does not fully achieve these goals and does not offer an added benefit to the current 2014 Edition approach of requiring vital signs exchange using industry standards and capture in a standards-agnostic manner. We expect the industry to develop a consensus-based approach for structured data capture, including for vital signs, and we will continue to support these processes in consideration of a future rulemaking. Given these considerations, we have not adopted a 2015 Edition "vital signs, BMI, and growth charts" certification criterion at this time, as we believe there is no added certification value for capturing vital signs in either the proposed manner or in a simply standards-agnostic manner.

- Image Results

We proposed to adopt a 2015 Edition "image results" certification criterion that was unchanged in comparison to the 2014 Edition "image results" criterion (§ 170.314(a)(12)).

Comments. The majority of commenters supported this criterion as proposed, but some commenters questioned why health IT developers would seek certification to this criterion and why providers would adopt health IT certified to this criterion because it did not support an objective or measure of the proposed EHR Incentive Programs Stage 3 or another program requirement. Some commenters also questioned the value of this criterion without a required standard, with a few commenters recommending the adoption of the Digital Imaging and Communication in Medicine (DICOM) standard.

Response. We have not adopted this certification criterion as part of the 2015 Edition at this time. We have considered public comments and no longer believe there is sufficient value in making this criterion available for certification as proposed. The criterion was proposed with functional requirements that do not advance functionality beyond the 2014 Edition "image results" criterion, support interoperability, nor serve an identified HHS or other program requiring the use of health IT certified to this functionality. In the response to the commenters recommending DICOM as the standard we should adopt, we will further assess whether there is an appropriate use case for the adoption of a certification criterion that requires the use of the DICOM standard as part of any future rulemaking. However, for the particular criterion we proposed, we refer readers to our prior thoughts on the appropriateness of adopting DICOM (77 FR 54173).

- Family Health History - Pedigree

In the Proposed Rule, we proposed a 2015 Edition "family health history – pedigree" certification criterion that required health IT to enable a user to create and incorporate a patient's FHH according to HL7 Pedigree standard and the HL7 Pedigree IG, HL7 Version 3 Implementation Guide: Family History/Pedigree Interoperability, Release 1.[139]

Comments. While some commenters supported adoption of this functionality and criterion, many commenters expressed concerns about the standard and IG. Commenters stated that there has been very little adoption of the Pedigree standard and IG. Commenters also expressed specific concerns about the standard and IG. Commenters noted that the standard is out of date (not been updated since 2009) and not in sync with HL7 V3-based standards. Commenters also stated that the IG was immature and had not been updated since 2013. In

[139] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=301

particular, commenters noted that the W3C XML schema language cannot represent all constraints expressed in the base specifications referenced in the IG and that there was a lack of clear guidance on interactions and appropriate implementations, which would likely lead to inconsistent implementations. Overall, commenters suggested that a criterion not be adopted with the Pedigree standard and associated IG until the standard and IG have been appropriately updated, including addressing the interoperability interactions that need to be supported, matured, and widely adopted.

Response. We thank commenters for their detailed feedback. We have not adopted this criterion as part of the 2015 Edition at this time. We agree with commenters that further effort is necessary to address their concerns before adoption of this criterion and associated standards. We intend to follow up with relevant stakeholders to address these concerns and will consider whether it is appropriate to include such a criterion and associated standards in a future rulemaking as HHS' work to support the Precision Medicine Initiative matures.[140]

- Patient List Creation

We proposed to adopt a 2015 Edition "patient list creation" certification criterion that was unchanged in comparison to the 2014 Edition "patient list creation" criterion (§ 170.314(a)(14)) and explained the expectation that a Health IT Module must demonstrate its capability to use at least one of the more specific data categories included in the "demographics" certification criterion (§ 170.315(a)(5)) (e.g., sex or date of birth).

Comments. The majority of commenters supported this criterion as proposed, but some commenters questioned why health IT developers would seek certification to this criterion and why providers would adopt health IT certified to this criterion because it did not support an

[140] http://www.nih.gov/precisionmedicine/

objective or measure of the proposed EHR Incentive Programs Stage 3 or another program requirement. Conversely, some commenters suggested that we adopt a "patient list creation" criterion that had more functionality that would be valuable to providers. These commenters suggested that the criterion included required functionality to select, sort, and create patient lists on, for example: on all patient demographics, vital signs, orders, and referrals, and allergies beyond medication allergies. Commenters stated that such enhanced functionality would improve patient tracking and the monitoring of health disparities.

Response. We have not adopted this certification criterion as part of the 2015 Edition at this time. We have considered public comments and no longer believe there is sufficient value in making this criterion available for certification as proposed. The criterion was proposed with limited functionality that did not go beyond the 2014 Edition "patient list creation" criterion. Further, as proposed, it does not serve an identified HHS or other program. We will, however, consider the comments recommending more enhanced functionality as we consider certification criteria for future rulemaking.

- Electronic Medication Administration Record

We proposed to adopt a 2015 Edition electronic medication administration record (eMAR) certification criterion that was unchanged in comparison to the 2014 Edition "eMAR" criterion (§ 170.314(a)(16)).

Comments. The majority of commenters supported this criterion as proposed, but some commenters questioned why health IT developers would seek certification to this criterion and why providers would adopt health IT certified to this criterion because it did not support an objective or measure of the proposed EHR Incentive Programs Stage 3 or another identified program requirement. A few commenters requested clarification as to whether bar-code scanning

is required to meet this criterion, with a couple of commenters recommending that bar-code scanning be part of this criterion to improve patient safety.

Response. We have not adopted this certification criterion as part of the 2015 Edition at this time. We have considered public comments and no longer believe there is sufficient value in making this criterion available for certification as proposed. The criterion was proposed with functional requirements that do not advance functionality beyond the 2014 Edition "eMAR" criterion, support interoperability, nor serve an identified program requiring the use of health IT certified to this functionality. We will consider whether we should propose the same or a more enhanced eMAR certification criterion in future rulemaking, including giving consideration to the value of identifying or requiring specific assistive technologies (e.g., bar-code scanning) for demonstrating compliance with the functional requirements of the criterion.

- Decision Support – Knowledge Artifact; and Decision Support - Service

Decision Support – Knowledge Artifact

In the Proposed Rule, we proposed to adopt a new 2015 Edition "decision support – knowledge artifact" certification criterion that, for the purposes of certification, would require health IT to demonstrate that it could electronically send and receive clinical decision support (CDS) knowledge artifacts in accordance with a Health eDecisions (HeD) standard. To assist the industry in producing and sharing machine readable files for representations of clinical guidance, we proposed to adopt the HL7 Version 3 Standard: Clinical Decision Support Knowledge Artifact Specification, Release 1.2 DSTU (July 2014) ("HeD standard Release 1.2")[141] and to require health IT to demonstrate it can electronically send and receive a CDS artifact formatted in the HeD standard Release 1.2. We requested comment on specific types of CDS Knowledge

[141] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=337

Artifacts for testing and certification to the HeD standard Release 1.2, and on standards' versions to consider as alternative options, or for future versions of this certification criterion, given the ongoing work to harmonize CDS and quality measurement standards.

Decision Support – Service

In the Proposed Rule, we proposed to adopt a new 2015 Edition "decision support – service" certification criterion that, for the purposes of certification, would require health IT to demonstrate that it could electronically make an information request with patient data and receive in return electronic clinical guidance in accordance with an HeD standard and the associated HL7 Implementation Guide: Decision Support Service, Release 1.1 (March 2014), US Realm DSTU Specification [142]. We specified that health IT would need to demonstrate the ability to send and receive electronic clinical guidance according to the interface requirements defined in Release 1.1. We requested comment on alternative versions of standards and on future versions of this certification criterion to advance the work to harmonize CDS and quality measurement standards.

We have summarized and responded to comments on these "decision support" criteria together as the referenced HeD standards were developed by one S&I initiative to address two use cases, we received similar comments on both proposals, and have determined to not adopt both criteria.

Comments. Many commenters supported the overall goals of the HeD standards to provide standardized ways to exchange decision support artifacts and request decision support information. However, these same commenters recommended ONC not adopt these criteria because of the ongoing work to develop harmonized CDS and clinical quality measure (CQM)

[142] http://www.hl7.org/documentcenter/public/standards/dstu/HL7_DSS_IG%20_R1_1_2014MAR.zip

standards through the Clinical Quality Framework Standards & Interoperability (S&I) Framework Initiative.[143] Commenters noted that the harmonized standards are expected to offer clinical and operational improvements for quality improvement over existing standards. These commenters also stated that they expect health IT developers and providers to dedicate resources to adopting the harmonized standards upon their completion. Therefore, these commenters stated that they do not intend to adopt the HeD standards because the standards are based on a different data model (the Virtual Medical Record or vMR) than the anticipated harmonized CDS and CQM standards. A few commenters noted that they did not support any proposal to offer certification for functionalities or standards that did not directly support a requirement of the proposed the EHR Incentive Programs Stage 3.

Response. We thank commenters for their thoughtful feedback. We acknowledge that the overall direction of health IT developers and providers is to continue to support and eventually adopt the harmonized CDS and CQM standards. Therefore, we agree with commenters that meeting the proposed "decision support " criteria and HeD standards would likely be inconsistent with this overall direction and require inefficient use of resources. As such, we also agree with comments that few, if any, health IT developers would get certified to the proposed criteria and very few providers would demand CDS functionality using the HeD standards. Accordingly, we have not adopted these certification criteria. We will continue to monitor the development and implementation of the harmonized CDS and CQM standards; and will consider whether to propose certification criteria that include these standards in a future rulemaking.

- Incorporate Laboratory Tests and Values/Results

[143] http://wiki.siframework.org/Clinical+Quality+Framework+Initiative

We proposed to adopt a 2015 Edition "incorporate laboratory tests and values/results" certification criterion that was revised in comparison to the 2014 Edition "incorporate laboratory tests and values/results" criterion (§ 170.314(b)(5)). We proposed to adopt and include the HL7 Version 2.5.1 Implementation Guide: S&I Framework Lab Results Interface, Draft Standard for Trial Use, Release 2, US Realm ("LRI Release 2") in the final 2015 Edition "transmission of laboratory test reports" criterion for the ambulatory setting. We explained that the LRI Release 2 addresses errors and ambiguities found in LRI Release 1 and harmonizes interoperability requirements with other laboratory standards we proposed to adopt in this final rule (e.g., the HL7 Version 2.5.1 Implementation Guide: S&I Framework Laboratory Orders from EHR, DSTU Release 2, US Realm, 2013).

We proposed that a Health IT Module would be required to display the following information included in laboratory test reports it receives: (1) the information for a test report as specified in 42 CFR 493.1291(a)(1) through (a)(3) and (c)(1) through (c)(7); the information related to reference intervals or normal values as specified in 42 CFR 493.1291(d); the information for alerts and delays as specified in 42 CFR 493.1291(g) and (h); and the information for corrected reports as specified in 42 CFR 493.1291(k)(2). We also proposed to require a Health IT Module to be able to use, at a minimum, LOINC® version 2.50 as the vocabulary standard for laboratory orders.

Comments. We received mixed comments on this proposed certification criterion. Some commenters generally supported adopting the LRI Release 2 IG. Other commenters also expressed support for inclusion of LOINC©. One commenter pointed out potential issues with the use of LOINC© as its use may conflict with CLIA reporting requirements for the test description and that in some cases a textual description from the laboratory must be displayed for CLIA

reporting. This commenter encouraged the harmonization of requirements with CMS and CDC for CLIA reporting to eliminate potential conflicts. Some commenters expressed concerns that the proposed LRI Release 2 IG was immature and noted additional pilots and potential refinements should be pursued before requiring adoption of the IG for certification.

Response. We have not adopted this certification criterion as part of the 2015 Edition at this time. We have made this determination based on a number of factors, including (among other aspects) that this criterion is no longer referenced by the EHR Incentive Programs and that the best versions of the IGs (LRI and EHR-S Functional Requirements for LRI) that could be associated with this criterion are not sufficiently ready. We agree with commenters regarding the LRI Release 2 IG lack of readiness for widespread adoption. We believe, however, that there is great promise and value in the LRI Release 2 IG for improving the interoperability of laboratory test results/values, the electronic exchange of laboratory test results/values, and compliance with CLIA for laboratories. To that end, we emphasize that we remain committed to continued collaboration with stakeholders to take the necessary steps to support widespread adoption of this IG, including the availability of test tools for industry use. As necessary and feasible, we also remain interested in supporting appropriate pilots for the IG.

EHR-S Functional Requirements LRI IG/Testing and Certification Requirements – Request for Comment

We sought comment on the HL7 EHR-S Functional Requirements for the V2.5.1 Implementation Guide: S&I Framework Lab Results Interface R2, Release 1, US Realm, Draft Standard for Trial Use, Release 1 ("EHR-S IG"), under ballot reconciliation with HL7[144] in describing the requirements related to the receipt and incorporation of laboratory results for

[144] http://www.hl7.org/participate/onlineballoting.cfm?ref=nav#nonmember. Access to the current draft of the EHR-S IG is freely available for review during the public comment period by establishing an HL7 user account.

measuring conformance of a Health IT Module to LRI Release 2. We also requested comment on uniform testing and certification approaches, specifically for the EHR-S IG.

Comments. Commenters stated that while progress has been made with the EHR-S IG, the standard has not yet been finalized and remains unproven. One commenter requested that we consider this IG for inclusion in a later edition of certification. Some commenters noted that the functional requirements would only govern a Health IT Module's ability to receive specific laboratory result content, and there is no corresponding guarantee that a laboratory system will send well-formatted results using the EHR-S IG. Another commenter recommended that additional State variation and certification needs be accounted for in the IG. A commenter stated that the HL7 Allergies and Intolerances Workgroup[145] will produce standards on allergies and intolerances and that these standards should be utilized in expanding a future or revised version of the EHR-S IG to addresses genotype-based drug metabolizer rate information appropriately.

Response. We thank commenters for their feedback. We have not adopted the EHR-S IG primarily because we have not adopted this certification criterion. We also agree with commenters that the IG is not yet ready for adoption. The comments we received will be used to inform any future rulemaking related to LRI Release 2 and EHR-S IG.

- Transmission of Laboratory Test Reports

We proposed to adopt a 2015 Edition "transmission of laboratory test reports" certification criterion that was revised in comparison to the 2014 Edition "transmission of electronic laboratory tests and values/results to ambulatory providers" criterion (§ 170.314(b)(6)). We stated that we renamed the criterion to more clearly indicate its availability for the certification of health IT used by any laboratory. We proposed to adopt and include the

[145] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=308

HL7 Version 2.5.1 Implementation Guide: S&I Framework Lab Results Interface, Draft Standard for Trial Use, Release 2, US Realm ("LRI Release 2") in the criterion and discussed our rationale for its inclusion in the 2015 Edition "incorporate laboratory tests and values/results." We further explained that inclusion of this standard for certification should not only facilitate improved interoperability of electronically sent laboratory test reports, but also facilitate laboratory compliance with CLIA as it relates to the incorporation and display of test results in a receiving system. We also proposed to require a Health IT Module to be able to use, at a minimum, LOINC® version 2.50 as the vocabulary standard.

Comments. We received similar comments to those received for the proposed "incorporate laboratory tests and values/results" certification criterion described above (i.e., some general support for adoption and other commenters expressed concern). In regard to expressed concerns, as recited under "incorporate laboratory tests and values/results" certification criterion, commenters stated that the proposed LRI Release 2 IG was immature and noted additional pilots and potential refinements should be pursued before requiring adoption of the IG for certification. Commenters also expressed concern with the use of LOINC© in relation to CLIA requirements. One commenter requested that data provenance requirements be included in the standard and/or the criterion.

Response. We have not adopted this certification criterion as part of the 2015 Edition at this time. We have made this determination based on the same factors recited for the proposed 2015 Edition "incorporate laboratory tests and values/results" certification criterion as this criterion is similarly situated as discussed below. This criterion is no longer referenced by the EHR Incentive Programs and the best version of the LRI IG that could be associated with this criterion is not sufficiently ready. We agree with commenters regarding the LRI Release 2 IG

lack of readiness for widespread adoption. We believe, however, as stated under the "incorporate laboratory tests and values/results" certification criterion response to comments, that there is great promise and value in the LRI Release 2 IG for improving the interoperability of laboratory test results/values, the electronic exchange of laboratory test results/values, and compliance with CLIA for laboratories. To that end, we emphasize that we remain committed to continued collaboration with stakeholders to take the necessary steps to support widespread adoption of this IG, including the availability of test tools for industry use. As necessary and feasible, we also remain interested in supporting appropriate pilots for the IG.

- Accessibility Technology Compatibility

We proposed to adopt a new 2015 Edition "accessibility technology compatibility" certification criterion that would offer health IT developers that present a Health IT Module for certification to one or more of the clinical, care coordination, and patient engagement certification criteria listed in proposed § 170.315(a), (b), or (e) the opportunity to have their health IT demonstrate compatibility with at least one accessibility technology for the user-facing capabilities included in the referenced criteria. By "opportunity," we noted that we meant that the proposed criterion would be available for certification but not required (i.e., by the ONC Certification Program or the EHR Incentive Programs). We explained that to meet this proposed certification criterion, a Health IT Module would need to demonstrate that the capability is compatible with at least one accessibility technology that provides text-to-speech functionality to meet this criterion. We noted that an accessibility technology used to meet this criterion would also not be "relied upon" for purposes of § 170.523(f). However, we stated that it would need to be identified in the issued test report and would ultimately be made publicly available as part of the information ONC-ACBs are required to report to ONC for inclusion on the CHPL so that

users would be able to identify the accessibility technology with which the certified Health IT Module demonstrated its compatibility.

We sought comment on the extent to which certification to this criterion would assist in complying with Section 504 of the Rehabilitation Act of 1973 (29 U.S.C. 794) and other applicable federal (e.g., Section 508 of the Rehabilitation Act of 1973) and state disability laws. We also sought comment on whether certification to this criterion as proposed would serve as a valuable market distinction for health IT developers and consumers (e.g., "Health IT Module with certified accessibility features").

Comments. Some commenters supported the concept of health IT being compatible with accessibility technology. Conversely, other commenters stated that complying with the criterion would be burdensome and would effectuate policy that should not be part of certification. A few commenters contended that text-to-speech capabilities would be costly to implement organization-wide and are not frequently appropriate for many health care workflows, particularly when considering privacy issues. A few commenters suggested that this criterion should include other assistive technology beyond screen readers. One commenter stated that many operation systems are already equipped with accessibility features.

Response. We thank commenters for their feedback. We have not adopted this certification criterion as part of the 2015 Edition at this time. We believe additional research is necessary into the appropriate accessibility technologies that should be referenced by such a criterion and could be supported by a testing infrastructure.

We also believe further research or evidence is needed to determine whether customers would make purchasing decisions based on whether a health IT product was certified as being compatible with a text-to-speech technology or simply based on whether a health IT product is

compatible with the desired accessibility technology (e.g., Braille capability). In this regard, we did not propose that health IT must have certain accessibility capabilities beyond text-to-speech and, more importantly, that it must be certified to this criterion. Therefore, we have not adopted the proposed criterion.

We do, however, believe that certification can currently support the accessibility of health IT through other means. As such, we have adopted the proposed "accessibility-centered design" certification criterion. We refer readers to section III.A.3 of this preamble for further discussion of this criterion. Independent of this certification requirement, we remind health IT developers seeking certification and providers using certified health IT of their independent obligations under applicable federal civil rights laws, including Section 504 of the Rehabilitation Act, Section 1557 of the Affordable Care Act, and the Americans with Disabilities Act that require covered entities to provide individuals with disabilities equal access to information and appropriate auxiliary aids and services as provided in the applicable statutes and regulations.

- SOAP Transport and Security Specification and XDR/XDM for Direct Messaging

We proposed to adopt a 2015 Edition "SOAP Transport and Security Specification and XDR/XDM for Direct Messaging" certification criterion that included the capability to send and receive according to the Transport and Security Specification (also referred to as the SOAP-Based Secure Transport RTM) and its companion specification XDR and XDM for Direct Messaging Specification. We noted that we previously adopted these capabilities for the 2014 Edition at § 170.314(b)(1), (b)(2) and (h)(3).

Comments. We received comments in support of the proposed certification criterion. One commenter suggested that support of XDM should be eliminated and replaced with a translation solution. We received also received a number of comments from the Immunization Information

System (IIS) community noting their reliance on SOAP as the recommended transport mechanism for exchange of immunization information in many jurisdictions.

Response. We thank commenters for their feedback. We have not adopted this certification criterion as part of the 2015 Edition at this time. The SOAP specification was originally adopted as an alternative to, or for use in conjunction with, the Direct Project specification. The goal was to offer more certified ways to support the EHR Incentive Program Stage 2 meaningful use transition of care/exchange measure, which required the use of certified technologies in the transmission of health information. There is no longer an explicit need for certification to SOAP because the corresponding health information exchange objectives in the EHR Incentive Programs Stage 3 and Modifications final rule published elsewhere in this issue of the **Federal Register** permit any transport mechanism (i.e., not necessarily the use of a certified transport method). In addition, as part of SOAP testing under the ONC Health IT Certification Program, only base SOAP standards, such as the web services standards (WS-*) are tested. For implementation, health IT systems have to layer in additional profiles (IHE based such as XDS) and IGs (e.g., NwHIN specs for patient discovery, query for documents, and retrieve documents) that utilize SOAP. The current testing for SOAP does not test for these additional standards since there has not been a convergence in the industry for a concise set of IGs. Thus, the current testing of SOAP does not provide the rigor or assurance to health IT users that systems using SOAP will ultimately enable them to exchange seamlessly. We expect the convergence on standards will be accomplished through SDOs.

In response to the XDM comment, we had paired the "XDR/XDM for Direct" with SOAP to enable the testing of SOAP with XDR using XDM packaging. While the comments from the IIS community are beyond the scope of this proposal, we note for clarity that consistent

with the approach under the EHR Incentive Programs Stage 2 final rule (77 FR 53979), in the EHR Incentive Programs Stage 3 and Modifications final rule published elsewhere in this edition of the **Federal Register,** CMS adopts flexibility with respect to the public health and clinical data registry reporting objectives at § 495.316(d)(2)(iii). This policy allows states to specify the means of transmission of public health data, and otherwise change the public health agency reporting objective, so long as the state does not require functionality greater than what is required under the Medicare EHR Incentive Program CEHRT definition and the 2015 Edition certification criteria adopted in this final rule.

- Healthcare Provider Directory – Query Request

We proposed a new 2015 Edition "healthcare provider directory – query request" certification criterion that would require a Health IT Module to be capable of querying a directory using the Integrating the Healthcare Enterprise (IHE)[146] Healthcare Provider Directory (HPD).[147] In addition, we proposed including an optional capability within this certification criterion that addresses federated requirements. This optional capability would require a Health IT Module to follow the approved federation option of IHE HPD[148] to accomplish querying in federated environments. The proposed certification criterion sought to establish a minimum set of queries that a Health IT Module could support. We specified that the capabilities required by a Health IT Module would include: (1) querying for an individual provider; (2) querying for an organizational provider; (3) querying for both individual and organizational provider in a single query; (4) querying for relationships between individual and organizational providers; and (5) electronically processing responses according to the IHE HPD Profile.

[146] http://wiki.ihe.net/index.php?title=Healthcare_Provider_Directory
[147] http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_HPD.pdf
[148] http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_HPD.pdf

Comments. Many commenters confirmed the value of provider directories and the ability for EHRs to query a provider directory. Most commenters stated that the proposed IHE HPD standard was immature and had few current implementations beyond pilot projects, with some commenters expressing concern about the costs associated with potential changes as the standard matures. Other commenters expressed concern with potential performance issues related to federated queries as well as the potential to proliferate redundant data. Commenters also noted, to ensure quality data, there needs to be: centralized directories; a governance model for a centralized approach; and uniform directory sharing strategies among providers, organizations, and intermediaries. A commenter recommended the S&I Framework revisit consider expanding the scope of the use cases for provider directories and any solutions beyond query and response to include the maintenance of provider directories.

Some commenters stated a preference for an approach that utilized a RESTful architecture, such as FHIR, noting that a service stack utilizing SOAP protocols (as used by the IHE HPD protocol) is more difficult to implement and maintain.

Response. We thank commenters for their feedback and appreciate their comments in supporting the use of provider directories. We have not adopted this criterion as part of the 2015 Edition at this time. As noted in the draft ONC 2015 Interoperability Standards Advisory (draft ISA), the IHE HPD Profile is a provider directory standard and was listed as the best available standard in the draft ISA.[149] However, we agree with commenters that the IHE HPD standard requires further implementation to ensure stability and support widespread adoption and the same is true for the federated concepts. We also agree with commenters that RESTful solutions are being defined and may be a viable alternative in the near future. We note that HHS remains

[149] http://www.healthit.gov/standards-advisory

committed to advancing policies related to provider directories as a means of furthering health information exchange and interoperability. We believe that continued work in this space can inform the development and implementation of provider directory standards for consideration in future rulemaking.

- Healthcare Provider Directory – Query Response

We proposed to adopt a new certification criterion that would focus on the "query response" and include the corresponding set of capabilities to respond to a provider directory query. This proposed criterion was intended to complement the certification criterion we proposed for adoption related to health IT issuing a healthcare provider directory "query request," and we explained that the proposed separation would provide developers with the flexibility to test and certify for provider directory "query" independent of the provider directory "response." We stated that a health IT system would be able to be presented for testing and certification to both proposed certification criteria if applicable or just to one or the other as appropriate based on the product's capabilities.

We proposed that directory sources must demonstrate the capability to respond to provider directory queries according to the IHE HPD profile and must respond to the following provider directory queries: query for an individual provider; query for an organizational provider; and query for relationships between individual providers and organizational providers.

In addition we proposed including an optional capability within this certification criterion to address federated requirements that would require a Health IT Module to follow the approved federation option of for IHE HPD to accomplish querying in federated environments. The federation change proposal was approved in September, 2014 and was incorporated into the IHE HPD Profile.

Comments. Commenters submitted the same or equivalent comments as those submitted on the proposed "healthcare provider directory – query request" certification criterion, which are described above.

Response. We have not adopted this criterion for reasons specified in our response above for the proposed healthcare provider directory – query request" certification criterion.

- Electronic Submission Of Medical Documentation

We proposed to adopt a new 2015 Edition "electronic submission of medical documentation" (esMD) certification criterion that focused on the electronic submission of medical documentation through four specific capabilities.

We proposed Capability 1 would require a Health IT Module be able to support the creation of a document in accordance with the HL7 Implementation Guide for CDA Release 2: Additional CDA R2 Templates – Clinical Documents for Payers – Set 1, Release 1 – US Realm in combination with the C-CDA Release 2.0 standard. We proposed to adopt the most recent version of the CDP1 IG, which is designed to be used in conjunction with C-CDA Release 2.0 templates and makes it possible for providers to exchange a more comprehensive set of clinical information. We explained that a Health IT Module must be able to create a document that conforms to the CDP1 IG's requirements along with appropriate use of nullFlavors to indicate when information is not available in the medical record for section or entry level template required in the CDP1 IG. In addition, we proposed that a conformant Health IT Module must also demonstrate the ability to generate the document level templates as defined in the C-CDA Release 2.0, including the unstructured document. We proposed a list of the applicable document templates within the C-CDA Release 2.0 and CDP1 IG that would need to be tested and certified for specific settings for which a Health IT Module is designed: (regardless of setting) Diagnostic

Imaging Report; Unstructured Document; Enhanced Operative Note Document; Enhanced Procedure Note Document; Interval Document; (ambulatory setting only) Enhanced Encounter Document; and (inpatient setting only) Enhanced Hospitalization Document.

We proposed Capability 2 would require a Health IT Module be able to support the use of digital signatures embedded in C-CDA Release 2.0 and CDP1 IG documents templates by adopting the HL7 Implementation Guide for CDA Release 2: Digital Signatures and Delegation of Rights, Release 1 (DSDR IG).[150] This DSDR IG defines a method to embed digital signatures in a CDA document and provides an optional method to specify delegation of right assertions that may be included with the digital signatures. We proposed that for the purposes of certification, the optional method must be demonstrated to meet this certification criterion. The Proposed Rule listed the requirements that a system used to digitally sign C-CDA Release 2.0 or CDP1 IG documents must meet to create a valid digital signature that meets Federal Information Processing Standards (FIPS)[151], Federal Information Security Management Act of 2002 (FISMA)[152], and Federal Bridge Certification Authority (FBCA) requirements.[153] For the purposes of testing and certification, we proposed that cryptographic module requirements must be met through compliance documentation, and the remaining capabilities listed in the Proposed Rule would be met through testing and certification assessment. We also proposed that a Health IT Module must demonstrate the ability to validate a digital signature embedded in a C-CDA Release 2.0 document that was conformant with the DSDR IG. The requirements proposed to perform this action are included in the DSDR IG.

---

[150] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=375
[151] http://www.nist.gov/itl/fips.cfm
[152] http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
[153] http://www.idmanagement.gov/sites/default/files/documents/FBCA%20Certificate%20Policy%20v2.27.pdf

We proposed Capability 3 would require a Health IT Module be able to support the creation and transmission of "external digital signatures" for documents that may be used to sign any document for the purpose of both data integrity and non-repudiation. The esMD Initiative defines the requirements in the Author of Record Level 1: Implementation Guide;[154] and we proposed to adopt the IG. We explained that this "signing" capability is intended for use when the sender of one or more documents needs to ensure that the transmitted documents include the non-repudiation identity of the sender and ensure that the recipient can validate that the documents have not been altered from the time of signing, and it is not intended to replace the ability to embed multiple digital signatures in a C-CDA Release 2.0 and CDP1 IG document.

We proposed Capability 4 would require a Health IT Module to support the creation and transmission of digital signatures for electronic transactions for the purpose of both data integrity and non-repudiation authenticity. The esMD Initiative defines the requirements in the Provider Profiles Authentication: Registration Implementation Guide;[155] and we proposed to adopt the IG. We explained that this "signing" capability is intended for use when the sender or recipient of a transaction needs to ensure that the transmitted information include the non-repudiation identity of the sender and ensure that the recipient can validate that the authenticity and integrity of the transaction information, and it is not intended to replace the digital signature requirements defined in either Capability 2 or 3 above.

Comments. A few commenters expressed support for this criterion. However, many more commenters expressed concerns. Commenters stated that the IG was immature, there had been

---

154 http://wiki.siframework.org/file/view/esMD%20AoR%20Level%201%20Implementation%20Guide%20v5%20FINAL.docx/539084894/esMD%20AoR%20Level%201%20Implementation%20Guide%20v5%20FINAL.docx

155 http://wiki.siframework.org/file/view/esMD%20Use%20Case%201%20Implementation%20Guide%20V24%20FINAL.docx/539084920/esMD%20Use%20Case%201%20Implementation%20Guide%20V24%20FINAL.docx

few pilots, and it was not proposed as required for Stage 3 of the EHR Incentive Programs. A few commenters also expressed concern about advancing a digital signature standard that may conflict with the existing Drug Enforcement Administration (DEA) standard for electronic prescribing of controlled substances. Other commenters expressed concerns that the changes to existing administrative and clinical workflows would be required to integrate esMD at a significant cost and resource burden.

Response. We have not adopted this criterion as part of the 2015 Edition at this time. We acknowledge and agree with commenters' stated concerns about the relative immaturity of the proposed standards and recommendations for further industry piloting and implementation to determine the usefulness of the standards for meeting the stated use cases. We will continue to monitor the development and implementation of esMD and will consider whether proposing a certification criterion or criteria to support esMD is appropriate for a future rulemaking.

- Work Information – Industry/Occupation (I/O) Data – Request for Comment

In the Proposed Rule, we requested that commenters consider what additional support might be needed for health IT developers, implementers, and users to effectively include a certification criterion that would require health IT to enable a user to record, change, and access (all electronically) the following data elements in structured format:

- Patients' employment status and primary activities (e.g., volunteer work);
- Patients' current I/O, linked to one another and with time-stamp, including start date;
- Patients' usual I/O, linked to one another and with time-stamp, including start year and duration in years; and
- Patients' history of occupation with a time and date stamp for when the history was collected (to note, this is focused on the capability to record a history, not a

requirement that a history must be recorded or that a patient history be recorded for a certain historical period of time).

We also solicited public comment on the experience health IT developers and health care providers have had in recording, coding, and using I/O data, which included any innovation that is making I/O data more useful for providers.

To better understand the health care needs associated with work data, we specifically solicited public comment from health care providers, provider organizations, and patients on the following:

- The usefulness for providers to be able to access current and usual I/O and related data in the EHR, including whether additional data elements, such as work schedule, are useful.
- The usefulness of a history of positions provided as current I/O, with data from each position time-stamped, linked, retained, and accessible as part of the longitudinal patient care (medical) record.
- Narrative text (vs. codes) for both current and usual I/O.
- CDC_Census codes for both current and usual I/O; available through PHIN VADS at https://phinvads.cdc.gov/vads/SearchVocab.action.
- SNOMED CT® codes for occupation (current codes or potentially developed codes).
- Other standards and codes that may be in use by the health IT industry for both current and usual I/O.

Comments. Many commenters supported the capture of structured industry/occupation (I/O) data in EHRs and other health IT systems to improve patient health outcomes for health issues wholly or partially caused by work and for health conditions whose management is

affected by work. These commenters stated that the structured capture of I/O information would also improve interoperability as the information being collected today is largely unstructured. Commenters did, however, express a number of concerns relating to maturity of available standards for representing the information and the time needed for a provider to collect structured I/O information. In regard to standards, a number of commenters suggested that the codes currently available in SNOMED CT® are not specific enough to capture the level of I/O detail that would be of clinical value. Instead, commenters stated that the industry is working through a NIOSH-led effort to develop an interface between health IT and an I/O coding knowledge engine that would guide users through choosing CDC Census I/O titles based on the North American Industry Coding System (NAICS) and the Bureau of Labor Statistics Standard Occupational Codes (SOC). Commenters mentioned that this work is still underway and suggested we wait until this standard is available for use before adopting requirements for capture of I/O information through certification. Commenters stated that the NAICS/SOC code set is considered the most authoritative and mature code set. These comments further stated that the adoption of SNOMED CT® would not align with the NAICS/SOC code set or the NIOSH tool and, therefore, could potentially create unnecessary burden.

Response. We thank commenters for the thoughtful feedback. As stated in the 2015 Edition proposed rule (80 FR 16829), we continue to believe in the value of I/O information to provide opportunities for health care providers to improve patient health outcomes for health issues wholly or partially caused by work and for health conditions whose management is affected by work. Our long-term goal is for health care providers to use I/O information to assess symptoms in the context of work activities and environments, inform patients of risks, obtain information to assist in return-to-work determinations and evaluate the health and information

needs of groups of patients.

Given the feedback about the immaturity of the standards currently available for supporting these goals, we have not adopted a 2015 Edition certification criterion for the collection of I/O information. We are, however, optimistic about the NIOSH-led effort to develop a tool based on the NAICS/SOC code set and believe that it can provide a much-needed authoritative standard that can enable the detailed recording of I/O titles. We intend to monitor the development of such a tool and will consider it and the additional comments we received regarding structured capture of I/O information for future rulemaking.

- U.S. Uniformed/Military Service Data – Request for Comment

To improve coding of military and all uniformed history, we stated in the Proposed Rule that a promising path forward would be to add codes to the U.S. Extension of SNOMED-CT®. Therefore, we requested comment on the following:

- Whether a potential certification criterion should be focused solely on U.S. military service or all uniformed service members (e.g., commissioned officers of the USPHS and NOAA);
- Whether the U.S. Extension of SNOMED-CT® is the most appropriate vocabulary code set or whether other vocabulary code sets may be appropriate; and
- The concepts/values we should use to capture U.S. military service or all uniformed service status. We ask commenters to consider the work of NIOSH on I/O information as it relates to capturing military service.

Comments. A large number of commenters suggested that we adopt certification to capture military service. Commenters stated that capturing information on military service could identify significant occupational exposure risks unique to military service, including overseas

deployment and combat environments. Commenters stated that capturing a patient's military service could also ensure that a patient receives all the applicable health care benefits (e.g., military and veteran's benefits), s/he is entitled to by alerting medical professionals to the patient's service history. Commenters stated that capturing military service information could also enable the assembly of a complete longitudinal record of care for a U.S. service member, including merging of health care data from different sources.

Some commenters supported and opposed the collection of non-military service uniformed service status (e.g., service data for U.S. Public Health Service and National Oceanic and Atmospheric Administration uniformed officers) as part of military/uniformed service data or collected separately.

In regard to vocabulary standards for collecting military service information, commenters submitted mixed comments on whether SNOMED CT® codes were sufficiently detailed and captured the right types of military service information. Commenters pointed out that SNOMED CT® contains some concepts to capture high-level military history, including current or past active military service and combat zone service. However, other commenters expressed concern that current SNOMED CT® codes for military history are not detailed enough to be of clinical value. As an example, commenters noted that while SNOMED CT® can document general information about whether the person served in the military, it does not allow for the capture of the individual's specific occupation.

Commenters stated that the NIOSH work on developing a tool for industry and occupation codes as described in the "Work Information – Industry/Occupation Data – Request for Comment" section above would include detailed codes for military service branch; service status; commissioned, warrant officer, non-commissioned and enlisted service; and many

occupational areas. Commenters noted, however, that the NIOSH tool is not expected to be able to capture Military Occupational Specialty (MOS) codes maintained by the Armed Forces or areas of service (such as ships, stations, and combat theaters).

Response. We thank commenters for the thoughtful feedback. As stated in the 2015 Edition proposed rule (80 FR 16830), we continue to believe in the value of capturing patient military service and other uniformed service information. We believe recording U.S. uniformed/military service information can have many benefits. It can help in identifying epidemiological risks for patients such as those noted above. It can assist in ensuring that a patient receives all the health care benefits he or she is entitled to by alerting medical professionals to the patient's service history, which can facilitate the coordination of benefits. This information can also increase the ability to assemble a longitudinal record of care for a U.S. service member, such as by requesting or merging of a patient's electronic health record stored by the Department of Defense, Veteran's Health Administration, and/or another health care provider.

Our long-term goal is for health care providers to use military service information to provide better care for our nation's veterans. However, given the feedback about SNOMED CT and the NIOSH tool under development, we have not adopted a 2015 Edition certification criterion for military service. We plan to continue to work with the appropriate stakeholders to develop the appropriate values and code sets that would enable consideration of a relevant certification criterion in a future rulemaking.

- Pharmacogenomics Request for Comment

Pharmacogenomics data identifies genetic variants in individuals that alter their metabolism or other interactions with medications and can lead to serious adverse events. This

information is being included in an increasing number of FDA-approved drug labels. Health IT that can capture pharmacogenomics information could be used to improve patient safety and enhance patient outcomes. In the Proposed Rule, we stated that to our knowledge, in general, health IT has not yet captured genomic and genetic patient information – the presence of clinically significant genomic variants – in a structured manner such as exists for other categorical clinical findings or laboratory-derived data.[156]

In collaboration with the National Institutes of Health, we solicited comment on whether:

- the 2015 Edition "medication allergy list" certification criterion should include the capability to integrate genotype-based drug metabolizer rate information;
- the 2015 Edition "drug-drug, drug-allergy interactions checks for CPOE" certification criterion or as a separate certification criterion should include pharmacogenomic CDS for "drug-genome interactions;"
- we should offer 2015 Edition certification for CDS that incorporate a patient's pharmacogenomic genotype data into the CPOE prescribing process with the goal of avoiding adverse prescribing outcomes for known drug-genotype interactions;
- there are certification approaches that could enhance the end-user's (provider's) adoption and continued use of health IT implementations that guide prescribing through CDS using pharmacogenomic data; and
- there are existing or developing standards applicable to the capture, storage, display, and exchange of potentially clinically relevant genomic data, including the pharmacogenomic subset.

[156] http://www.genomebc.ca/education/articles/genomics-vs-genetics/; and http://www.who.int/genomics/geneticsVSgenomics/en/

Comments. Most commenters agreed on the value of pharmacogenomics data as an integral part of medicine in the future, but indicated that the standards were currently not mature enough to support this functionality and that it was premature to attempt to include it in certification. Commenters noted that the inclusion of pharmacogenomics data can link variants to changes in drug metabolism or response, especially when clinical guidelines exist about dosing for variant carriers and how it can enable pharmacogenomic-based therapeutic recommendations integrated into computerized systems for drug prescription, automated medication surveillance, and EHRs.

In certain instances, commenters supported inclusion of the pharmacogenomic variant causing the allergy if such information is known for the patient. However, other commenters suggested that studies are needed to prove effectiveness and support inclusion of such data. Some commenters cited drug-drug and drug-allergy interaction alerts without an appropriate filter as the largest source of alert fatigue in relation to the value. Many other commenters also cited concerns over other CDS alert fatigue, poor return on investment, high costs of testing, and the staff resources needed to maintain the CDS in a rapidly evolving area with little evidence to show that it improves overall outcomes or reduces costs. A few commenters noted the existence of third-party web services that provide drug-genome interaction checking functionality that are easily integrated with EHRs.

Response. While we believe in the value of CDS including drug-drug/drug-allergy interaction checks for improving patient safety, we agree that standards are not mature to support incorporating pharmacogenomics data into health IT certification at this point in time. We encourage the industry to continue its work on developing standards for incorporating this information into health IT. We note that we view the use of pharmacogenomics data in health IT

as one of the early tangible products of the Precision Medicine Initiative,[157] and intend to monitor and consider developments in this field for future rulemaking.

Privacy and Security Considerations for Pharmacogenomics

We solicited comment on whether:

- we should offer certification for health IT functionality that could facilitate HIPAA-compliant sharing of discrete elements of a patient's genomic information from their record to the family history section of a relative's record;
- the proposed "data segmentation for privacy" criteria would provide needed health IT functions with respect to the storage, use, transmission, and disclosure of genetic, genomic, and pharmacogenomics information that is subject to protections under HIPAA and additional state and federal privacy and protection laws such as the Genetic Information Nondiscrimination Act (GINA)[158];
- the proposed "data segmentation for privacy" criteria adequately balance complex genetic privacy issues, such as those related to behavioral health, with the clinical value of context-appropriate availability of a patient's actionable genetic and genomic information;
- health IT should be required to apply different rules for the use and exchange of genetic, genome, and pharmacogenomics data based on different groupings of diseases or conditions based on the sensitivity of the information, such as those related to behavioral health; and

[157] http://www.nih.gov/precisionmedicine/
[158] http://ghr.nlm.nih.gov/spotlight=thegeneticinformationnondiscriminationactgina

- there are other factors we should consider for health IT that allows the user to use or disclose genetic information in a manner compliant with federal and state privacy laws.

Comments. Many commenters noted privacy concerns stating it is essential to understand and implement proper privacy and security requirements associated with certified functionalities. Commenters indicated certified functionalities must not lead to discrimination against individuals or their families who may be at risk of developing future health issues. These commenters were concerned that there is not sufficient technical maturity to support privacy protections for genetic data, segmented to the genetic data atom. In particular, commenters were concerned about behavioral health implications, the risk of revealing latent conditions and providing information on close relatives, and the effect on insurance coverage. In addition to privacy concerns, select comments noted ethical and legal implications of any gene-related functionality. Some commenters suggested that the features of the "data segmentation for privacy" criteria should be incorporated into any inclusion of pharmacogenomic data.

Response. We thank commenters for sharing their concerns and feedback. As noted above, standards are not mature to support incorporating pharmacogenomics data into health IT certification at this point in time. We will continue to consider privacy and security implications and stakeholder concerns as they relate to any potential future rulemaking for pharmacogenomics data. To note, we have adopted the proposed "data segmentation for privacy" criteria (see section III.3 of this preamble) and will further assess and consider its value in the segmentation of individually identifiable genetic information that is protected by federal and state privacy laws as part of any future rulemaking related to pharmacogenomics data.

B. Definitions

1. Base EHR Definitions

We proposed to adopt a Base EHR definition specific to the 2015 Edition (i.e., a 2015 Edition Base EHR definition) at § 170.102 and rename the current Base EHR definition at § 170.102 as the 2014 Edition Base EHR definition. We proposed a 2015 Edition Base EHR definition that would differ from the 2014 Edition Base EHR definition in the following ways:

- It would not include privacy and security capabilities and certification criteria.
- It would only include capabilities to record and export CQM data (§ 170.315(c)(1)) and not the other CQM capabilities such as import, calculate, and "report to CMS."
- It would include the 2015 Edition "smoking status" certification criterion as patient demographic and clinical health information data consistent with statutory requirements.[159]
- It would include the 2015 Edition "implantable device list" certification criterion as patient demographic and clinical health information data consistent with statutory requirements.[160]
- It would include the 2015 Edition "application access to Common Clinical Data Set" certification criterion as a capability to both capture and query information relevant to health care quality and exchange electronic health information with, and integrate such information from other sources.[161]

[159] A Base EHR is the regulatory term we have given to what the HITECH Act defines as a "qualified EHR." Our Base EHR definition(s) include all capabilities found in the "qualified EHR." Please see the 2014 Edition final rule (77 FR 54262) for further explanation.
[160] A capability included in the Base EHR definition, which originates from the "qualified EHR" definition found in the HITECH Act.
[161] These are capabilities included in the Base EHR definition, which originate from the "qualified EHR" definition found in the HITECH Act.

- It would include the proposed 2015 Edition certification criteria that correspond to the remaining 2014 Edition certification criteria referenced in the "2014 Edition" Base EHR definition (i.e., CPOE, demographics, problem list, medication list, medication allergy list, CDS, transitions of care, data portability, and relevant transport certification criteria). On the inclusion of transport certification criteria, we proposed to include the "Direct Project" criterion (§ 170.315(h)(1)) as well as the "Direct Project, Edge Protocol and XDR/XDM" criterion (§ 170.315(h)(2)) as equivalent alternative means for meeting the 2015 Edition Base EHR definition.

Comments. A commenter recommended removing the Base EHR definition from the 2015 Edition rulemaking and including it in the EHR Incentive Programs rulemaking. Several commenters suggested that we modify the Base EHR definition to accommodate use of health IT that is certified to the 2014 Edition and the 2015 Edition, stating that this will give providers flexibility as they upgrade to 2015 Edition and begin to achieve Stage 3.

Commenters provided varying recommendations for the criteria that should be included in the Base EHR definition. Some commenters stated that separating privacy and security certification criteria from the Base EHR definition is overly burdensome or confusing, or may create security gaps. A commenter recommended that the "data export" and "application access to Common Clinical Data Set" criteria are more appropriate as "modular" certification, rather than as part of the Base EHR definition. A commenter suggested that "drug-drug, drug-allergy interaction checks for CPOE" criterion be included in the Base EHR definition as it is specifically for CPOE, which is part of the Base EHR definition. Some commenters rejected the idea of including the "implantable device list" criterion in the Base EHR definition, while other commenters supported inclusion of this criterion and noted that this capability would improve

care coordination. A few commenters voiced support for the inclusion of the Direct Edge Protocol as an alternative to Direct Project. Some commenters recommended that sexual orientation and gender identity data be included in the Base EHR definition.

Response. We have renamed the current Base EHR definition at § 170.102 as the 2014 Edition Base EHR definition and adopted the 2015 Base EHR definition largely as proposed. In Table 7 below, we list the 2015 Edition certification criteria included in the 2015 Edition Base EHR definition. Many of the proposed criteria have been revised in response to comments and we refer readers to section III.A.1 of this preamble for a detailed discussion of those criteria and revisions.

Since the establishment of the 2014 Edition Base EHR definition (77 FR 54263-64), we have tried to limit the criteria included in the Base EHR definition to those necessary to meet the HITECH Act requirements and our policy goals. In this regard, we have not included "drug-drug, drug-allergy interaction checks for CPOE" criterion in the 2015 Edition Base EHR definition just as we did not for the 2014 Edition Base EHR definition (see 77 FR 54264). We have, however, included the "implantable device list" criterion in this 2015 Edition Base EHR definition for the reasons stated in the Proposed Rule (80 FR 16825) and discussed under the "implantable device list" criterion in section III.A.1 of this preamble. We have also included the Direct transport alternatives for the reasons discussed in the Proposed Rule (80 FR 16862) and under "transport methods and other protocols" in section III.A.1 of this preamble. In response to comments and other considerations, the "demographics" certification criterion (§ 170.315(a)(5)) now includes sexual orientation and gender identity as data elements, thus including this data in the 2015 Edition Base EHR definition. We discuss this further under the "demographics" certification criterion in section III.A.1 of this preamble. We also note that given our decision to

split the "application access to Common Clinical Data Set" criterion into three separate criteria, we have accordingly modified the 2015 Edition Base EHR definition to include these three criteria.

In regard to the lack of inclusion of privacy and security criteria in the 2015 Edition Base EHR definition, we believe commenters are confused by our approach. As discussed in more detail under the "privacy and security" heading in section IV.C.1 of this preamble, Health IT Modules presented for certification to criteria listed in the 2015 Base EHR definition and other 2015 Edition certification criteria will be subject to the applicable privacy and security criteria for the purposes of certification. Our new privacy and security certification approach places responsibility more clearly on the health IT developer presenting its product for certification to ensure that its health IT has the applicable privacy and security capabilities in order to be certified. This is counter to the approach under the 2014 Edition Base EHR definition, which puts the onus on the provider to ensure he/she has health IT certified to the privacy and security criteria included in the Base EHR definition.

The CQM capabilities noted above as not included in the 2015 Edition Base EHR definition have, however, been included the Certified EHR Technology (CEHRT) definition under the EHR Incentive Programs. We refer readers to the next section ("2. Certified EHR Technology Definition") and Table 4 found in section III.A.3 ("2015 Edition Health IT Certification Criteria Associated with the EHR Incentive Programs Stage 3") of this preamble for further information and guidance on the relationship of the 2015 Edition Base EHR definition and the 2015 Edition certification criteria with the CEHRT definition. We also refer readers to the CEHRT definition finalized in the EHR Incentive Programs Stage 3 and Modifications final

rule published elsewhere in this issue of the **Federal Register** as the authoritative source for the requirements to meet the CEHRT definition.

We seek to clarify the 2015 Base EHR definition in response to comments. First, the Base EHR definition is just a definition not a single certified product. As noted in 2014 Edition final rule (77 FR 54263), the Base EHR definition may be met using multiple Health IT Modules. Therefore, to the commenter's point, Health IT Modules separately certified to the "data export," "application access" criteria, and other criteria included in the 2015 Edition Base EHR definition can be combined to meet the definition. Second, we believe the defining of the Base EHR definition should remain in the rulemaking as the Base EHR definition is only one part of the CEHRT definition and may serve other purposes beyond its inclusion in the CEHRT definition and supporting the EHR Incentive Programs. Third, with the 2014 and 2015 Base EHR definitions' inclusion in the CEHRT definition and the CEHRT definition's included flexibility to use both health IT certified to the 2014 and 2015 Editions for the specified EHR reporting periods, we do not believe there would be a benefit to developing a single Base EHR definition that referenced both the 2014 and 2015 Editions. Rather, we believe this would cause confusion, particularly in relationship to the CEHRT definition.

Table 7. Certification Criteria Required to Satisfy the 2015 Edition Base EHR Definition

Base EHR Capabilities	**Certification Criteria**
Includes patient demographic and clinical health information, such as medical history and problem lists	Demographics § 170.315(a)(5) Problem List § 170.315(a)(6) Medication List § 170.315(a)(7) Medication Allergy List § 170.315(a)(8) Smoking Status § 170.315(a)(11) Implantable Device List § 170.315(a)(14)
Capacity to provide clinical decision support	Clinical Decision Support § 170.315(a)(9)
Capacity to support physician order entry	Computerized Provider Order Entry § 170.315(a)(1), (2) or (3)
Capacity to capture and query information relevant to health care quality	Clinical Quality Measures – Record and Export § 170.315(c)(1)

Capacity to exchange electronic health information with, and integrate such information from other sources	Transitions of Care § 170.315(b)(1) Data Export § 170.315(b)(6) Application Access – Patient Selection § 170.315(g)(7) Application Access – Data Category Request § 170.315(g)(8) Application Access – All Data Request § 170.315(g)(9) Direct Project § 170.315(h)(1) or Direct Project, Edge Protocol, and XDR/XDM § 170.315(h)(2)

Marketing

In the Proposed Rule, we noted that we would continue the same marketing policy that we adopted for the 2014 Edition as it relates to the 2015 Edition Base EHR definition (i.e., health IT developers would have the ability to market their technology as meeting the 2015 Edition Base EHR definition when their Health IT Module(s) is/are certified to all the 2015 Edition certification criteria included in the 2015 Edition Base EHR definition) (see also 77 FR 54273).

Comments. A commenter requested clarification regarding how we anticipate ONC-ACBs will monitor the use of the term "Base EHR definition."

Response. We will maintain this policy with the 2015 Edition. We anticipate that ONC-ACBs will continue to monitor health IT developers and their certified health IT as they do now with regard to the 2014 Edition Base EHR definition. ONC-ACBs have various oversight responsibilities for certified health IT, including ensuring the public disclosure of certain information for certified health IT (see § 170.523(k)); the proper use of the Certified HIT certification mark (see § 170.523(l)); and responsibilities under ISO/IEC 17065 (2012) (ISO 17065)[162], to which they are accredited. In regard to ISO 17065, section 4.1.3.2 states "incorrect references to the certification scheme or misleading use of licenses, certificates, marks, or any other mechanism for indicating a product is certified, found in documentation or other publicity, shall be dealt with by suitable action." Consistent with the performance of these responsibilities,

[162] This standard is incorporated by reference in 45 CFR 170.599.

we anticipate ONC-ACBs will be able to identify any improper marketing association of certified health IT with the "Base EHR definition." We also note that any purchaser or other stakeholder may inform us of any alleged improper marketing association of certified health IT with the "Base EHR definition."

2. Certified EHR Technology Definition

We proposed to remove the Certified EHR Technology (CEHRT) definition from § 170.102, effective with this final rule. We explained that the CEHRT definition has always been defined in a manner that supports the EHR Incentive Programs and would more appropriately reside solely within the EHR Incentive Programs regulations to be consistent with our approach in this final rule to make the ONC Health IT Certification Program more open and accessible to other types of health IT beyond EHR technology and for health IT that supports care and practice settings beyond those included in the EHR Incentive Programs. We noted that this removal of the definition should add administrative simplicity in that regulatory provisions, which EHR Incentive Programs participants must meet (e.g., the CEHRT definition), would be defined within the context of rulemakings for those programs. We further noted that, as proposed in the EHR Incentive Programs Stage 3 proposed rule (80 FR 16767), CMS would adopt a CEHRT definition in 42 CFR 495.4 that would cover all relevant compliance timelines (i.e., specify the CEHRT definition applicable for each year/EHR reporting period) and EHR Incentive Programs requirements. We explained that the CEHRT definition proposed by CMS would also continue to point to the relevant Base EHR definitions[163] adopted or proposed by ONC and to other ONC-adopted and proposed certification criteria relevant to the EHR Incentive Programs.

[163] This is required by the HITECH Act under the term "Qualified EHR" and references a foundational set of certified capabilities all EPs, eligible hospitals, and CAHs need to adopt.

Comments. The overwhelming majority of commenters were supportive of moving the CEHRT definition into the EHR Incentive Programs. One commenter requested that we and CMS identify which certification criteria are required for to meet the CEHRT definition and be a meaningful user. Many commenters suggested that the CEHRT definition should accommodate use of health IT certified to the 2014 Edition and health IT certified to the 2015 Edition as this approach would give providers flexibility as they upgrade to 2015 Edition. Many commenters also requested that we work closely with CMS and other organizations to align any changes to the CEHRT definition or adoption of proposed criteria for inclusion in programs beyond the EHR Incentive Programs.

Response. We have finalized our proposal to remove the CEHRT definition for 2015 certification. As proposed in the EHR Incentive Programs Stage 3 proposed rule, a combination of health IT certified to the 2014 Edition and 2015 Edition may be used during EHR reporting periods through calendar year 2017. Table 4 found in section III.A.3 ("2015 Edition Health IT Certification Criteria Associated with the EHR Incentive Programs Stage 3") provides guidance on the relationship of the 2015 Edition certification criteria with the CEHRT definition and Stage 3 of the EHR Incentive Programs. We also refer readers to the EHR Incentive Programs Stage 3 and Modifications final rule published elsewhere in this issue of the **Federal Register** as the authoritative source for the requirements to meet the CEHRT definition (and meaningful use objectives and measures). We note that supplemental guidance documents we intend to issue with this final rule will also identify the 2015 Edition certification criteria necessary to meet the CEHRT definition and are associated with meaningful use objectives and measures. We further note that we intend to work closely with CMS and other stakeholders to ensure alignment of the

2015 Edition and CEHRT definition to support settings, use cases, and programs beyond the EHR Incentive Programs.

3. Common Clinical Data Set Definition

We received general comments on our overall proposal and comments on the data and vocabulary standards included in the proposed definition. We have divided and responded to the comments in a similar manner.

Name Change

We proposed to revise the "Common MU Data Set" definition in § 170.102 and change the name to "Common Clinical Data Set," which aligned with our proposed approach to make the ONC Health IT Certification Program more open and accessible to other types of health IT beyond EHR technology and for health IT that supports care and practice settings beyond those included in the EHR Incentive Programs. We explained the procedural requirement to remove the previous name from the CFR and add the new name. We also proposed to change references to the "Common MU Data Set" in the 2014 Edition (§ 170.314) to "Common Clinical Data Set."

Comments. The majority of commenters expressed support for the name change. One commenter did not support the name change stating it would add confusion and lack of continuity. One commenter stated the term "clinical" may be too restrictive.

Response. We thank commenters for the support for the name change and have finalized this proposal and related changes to the CFR. The term "Common Clinical Data Set" aligns with our approach to make the ONC Health IT Certification Program more open and accessible to other types of health IT beyond EHR technology and for health IT that supports care and practice settings beyond those included in the EHR Incentive Programs. We believe "clinical" is a suitable descriptor for the purpose and context within which the Common Clinical Data Set has

been defined (i.e., for the certification of health IT under the ONC Health IT Certification Program).

We refer readers to Table 8 below for a complete listing of the data included in the Common Clinical Data Set and the associated standards.

Vocabulary Standards

We proposed to revise the definition to include new and updated standards and code sets (HL7 Version 3 for sex; "Race & Ethnicity – CDC" code system in PHIN VADS and the OMB standard for race and ethnicity; RFC 5646 for preferred language, the September 2014 Release of the U.S. Edition of SNOMED CT® for problems and procedures; the February 2, 2015 monthly version of RxNorm for medications and medication allergies; and LOINC® version 2.50 for laboratory tests). We noted that for race and ethnicity a Health IT Module must be able to express both detailed races and ethnicities according to the "Race & Ethnicity – CDC" code system and the aggregate OMB code for each race and ethnicity identified by the patient.

We emphasized that the proposed revisions would not change the standards, codes sets, and data requirements specified in the Common Clinical Data Set for 2014 Edition certification and would only apply to a Health IT Module certified to the 2015 Edition certification criteria that reference the Common Clinical Data Set.

Comments. The majority of commenters expressed support updating the definition to reflect new and updated standards and code sets. Some commenters stated that specific versions of vocabulary standards may become obsolete or superseded and systems should be permitted to use later versions.

Response. We thank commenters for their support. We have adopted the proposed data elements and referenced standards for the Common Clinical Data Set definition. We note that we

have adopted newer versions of SNOMED CT®, RxNorm, and LOINC® than we proposed as the baseline versions for certification. We have also more specifically identified the CDC Race and Ethnicity code set (CDC Race and Ethnicity Code Set Version 1.0 (March 2000)) as compared to the identification in the Proposed Rule. We note this code set remains part of the PHIN Vocabulary Access and Distribution System (VADS) Release 3.3.9. We refer readers to section III.A.2.c ("Minimum Standards" Code Sets) for further discussion of our adoption of minimum standards code sets and our decision to adopt these newer versions. We also remind readers that health IT developers may seek certification to newer versions than the adopted baseline versions of minimum standards code sets, unless the Secretary specifically prohibits it.

Comments. One commenter requested clarification regarding which codes for race and ethnicities are included in the Common Clinical Data Set.

Response. Both the CDC Race and Ethnicity code set in PHIN VADS and the OMB standard for race and ethnicity are included for certification to the 2015 Edition, but only the OMB standard for certification to the 2014 Edition.

Comments. One commenter requested clarification if the C-CDA Release 1.1 will be applicable for certification to the "Common MU Data Set" or the Common Clinical Data Set.

Response. For the 2014 Edition certification criteria that reference the Common Clinical Data Set (formerly the "Common MU Data Set"), the C-CDA Release 1.1 is the referenced standard.

Immunizations

We proposed to include immunizations in the Common Clinical Data Set for 2015 Edition certification. We noted that the C–CDA Release 2.0 could support NDC codes as a translational data element, but the CVX code is required to accompany it. We stated that it would

not be a heavy burden to map from an NDC code to a CVX code because a mapping from NDC codes to CVX codes is publicly available. Therefore, for the purposes of including immunizations in the Common Clinical Data Set for 2015 Edition certification, immunizations would be required to be coded according to the CVX code set (HL7 Standard Code Set CVX—Vaccines Administered, updates through February 2, 2015) and the NDC code set (NDC—Vaccine NDC Linker, updates through January 15, 2015).

Comments. Multiple commenters expressed concerns with mapping burden. One commenter stated that the inclusion of immunizations mapped to NDC codes may be problematic as most providers may not include NDC codes when documenting immunizations particularly for historical immunizations and immunizations received outside the practice setting. Some commenters commented that IIS transmission doesn't seem to align since IIS transmission is based on HL7 V2 and not C-CDA R2.

Response. We have included immunizations in the definition according to the standards proposed. We note that we have adopted newer versions of NDC and CVX than we proposed as the baseline versions for certification. We refer readers to section III.A.2.c ("Minimum Standards" Code Sets) for further discussion of our adoption of minimum standards code sets and our decision to adopt these newer versions. We do not believe this creates an undue mapping burden as CDC provides a publicly available mapping of NDC codes for vaccines to CVX codes.[164] We also note that these requirements are to test and certify a Health IT Module's capabilities; and they do not require a provider to send an immunization using a certain code. IIS transmission based on HL7 V2 serves a different use case than the Common Clinical Data Set

[164] http://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=ndc. See also: http://www2a.cdc.gov/vaccines/iis/iisstandards/ndc_tableaccess.asp.

and the C-CDA, which support transitions of care, data export, API access, and a patient's ability to view, download, and transmit their health information.

Vital Signs

We proposed to include vital signs in the Common Clinical Data Set according to specific LOINC® codes, metadata, and relevant UCUM unit of measures. We also proposed to offer optional certification to pediatric vital signs as part of the Common Clinical Data Set.

We have not adopted the proposed vital signs criterion as discussed in section III.A.5 above.

Comments. Commenters generally supported the expanded list of proposed vital signs for the Common Clinical Data Set with concerns on a few items. For systolic and diastolic blood pressure, a few commenters did not support the separating out of these from blood pressure generally as their systems allow both to be collected in one field with a delineator (e.g., a comma or forwards-slash) that can be used to parse the two fields. A few commenters suggested that "body weight measured" specifies the method of measurement and noted that there are other ways that body weight is collected, such as self-reporting. There was a lot of concern over the choice of "oxygen saturation in arterial blood by pulse oximetry" and a few commenters suggested there are multiple ways of collecting pulse oximetry. Commenters noted that BMI is typically a calculated value from height and weight, and were concerned that users should not be allowed to manually enter in a BMI as it could be incorrectly calculated. Last, commenters were concerned that mean blood pressure is not a vital sign typically collected in all provider settings, and is more specific to surgery, ED, and ICU settings.

Response. We thank commenters for their feedback. While we have not adopted the proposed 2015 Edition "vital signs" criterion as discussed in section III.A.5 above, we have

included vital signs in the Common Clinical Data Set for certification to the 2015 Edition consistent with the same vocabulary standards as specified by the C-CDA Release 2.1 standard (i.e., vital signs are exchanged using a LOINC® code, and with a Unified Code of Units of Measure (UCUM) code for the unit of measure associated with the vital sign measurement). We discuss the list of vital signs that must be exchanged in this manner below, including changes made in comparison to our proposals.

We continue to differentiate between systolic and diastolic blood pressure as two distinct vital signs, but note that Health IT Modules may store and display the two values in one field as long as they are exchanged as two separate fields. We have revised "body weight measured" to "body weight." We have revised "oxygen saturation in arterial blood by pulse oximetry" to "pulse oximetry" and will allow implementers, for the purposes of testing and certification, to choose the LOINC® code with "pulse oximetry" in its name that best represents the method of measurement for exchange. We note that we believe that inhaled oxygen concentration is a necessary measurement in order to correctly interpret the pulse oximetry measurement, and are including it in the list of vital signs for exchange. This does not mean that providers are required to capture this measurement every time, only that certified Health IT Modules are able to exchange the value if present. Last, we have removed BMI and mean blood pressure from the list of vital signs.

In summary, we require that the following vital signs must be exchanged as part of the Common Clinical Data Set using a LOINC® code and with a UCUM code for the unit of measure associated with the vital sign measurement:

- Systolic blood pressure;
- Diastolic blood pressure;

- Body height;
- Body weight;
- Heart rate;
- Respiratory rate;
- Body temperature;
- Pulse oximetry; and
- Inhaled oxygen concentration.

We believe this list represents vital signs commonly collected across provider settings today and is a start at defining a minimum set of vital signs, but note that we will continue to work with stakeholders to determine and consider if this list should be revised through a future rulemaking.

Comments. A number of commenters were concerned that UCUM does not allow for mixing of units, and were therefore concerned that a height of 5 feet and 6 inches (5'6") could not be represented with an associated UCUM code for the unit of measure.

Response. We note that systems have the flexibility to choose how to display the vital sign measurement. Our requirement only specifies that the vital sign measurement must be exchanged using an applicable unit of measurement with a UCUM code. Therefore, systems could exchange a height of 5'6" as 66 inches or 5.5 feet or 167.64 centimeters using the appropriate UCUM code to represent the unit of measure for the measurement. Note that we provide this as an example only, and leave the decision on the appropriate unit of measure to the developers and providers. As noted in the 2015 Edition proposed rule (80 FR16818), LOINC

provides a translation table[165] that enumerates UCUM syntax for a subset of UCUM codes that are commonly used in health IT that may be a useful reference for stakeholders. We would also suggest that health IT developers and providers follow the guidance provided in C-CDA Release 2.1 for exchanging vital signs.

Comments. Commenters were generally supportive of the proposed optional pediatric vital signs.

Response. We have adopted the pediatric vital signs as proposed for inclusion in the Common Clinical Data Set definition as optional for exchange. We note that as discussed in the 2015 Edition proposed rule, CDC recommends the use of these pediatric vital signs for settings of care in which pediatric and adolescent patients are seen (80 FR 16818-16819) as part of best practices. The availability of a reference range/scale or growth curve can help with proper interpretation of the measurements for the BMI percentile per age and sex and weight for age per length and sex. Thus, we are including the reference range/scale or growth curve for each of these two pediatric vital signs as part of the Common Clinical Data Set definition for certification, and would suggest that providers include this information as appropriate. We note that the C-CDA Release 2.1 standard does allow for including additional clinically relevant information with vital signs.

Unique Device Identifier(s)

We proposed to include the Unique Device Identifier(s) of a patient's Implantable Device(s) for certification to the 2015 Edition.

[165] https://loinc.org/downloads/usage/units

Comments. Some commenters were in agreement with including UDIs, while other commenters suggested removing UDIs until more progress has been made with medical device identifier manufacturers and utilization among providers.

Response. We have included UDIs in the definition and require it be recorded in accordance with the "Product Instance" in the "Procedure Activity Procedure Section" of the C-CDA 2.1. This specificity within the C-CDA will make this information more easily retrievable. As discussed in more detail under the ''implantable device list'' certification criterion in section III.A.3 of this preamble, this information leads to improved patient safety when available to providers. By including this information in the Common Clinical Data Set, a Health IT Module certified to criteria referencing the Common Clinical Data Set would be capable of exchanging this information and further facilitating improvements in patient safety.

Assessment and Plan of Treatment, Goals, and Health Concerns

We proposed to include the "assessment and plan of treatment," "goals," and "health concerns" in the "Common Clinical Data Set" for certification to the 2015 Edition to replace the concept of the "care plan field(s), including goals and instructions" which is part of the "Common MU Data Set" in the 2014 Edition. We clarified that we intend "care plan field(s), including goals and instructions" to be a single provider's documentation of their assessment, plan of treatment, goals, and health concerns for the patient, and we stated that this clarification applies for 2014 Edition certification. We proposed this clarification to better align with the terms used in the C-CDA Release 2.0, which includes the "Assessment and Plan Section (V2)," "Assessment Section (V2)," "Plan of Treatment Section (V2)," "Goals Section," and "Health Concerns Section." In previous iterations of the C-CDA, we explained that the "Plan of Treatment Section" was called the "Plan of Care Section," which resulted in confusion on

whether the information was intended to represent a single encounter or the synthesis of multiple encounters. For that reason, the "Plan of Care Section" was proposed to be called the "Plan of Treatment Section" to indicate that it is intended to represent a single encounter and not to be confused with the "Care Plan document template."

For certification to the 2015 Edition, we proposed to include in the Common Clinical Data Set "assessment and plan of treatment," "goals," and "health concerns" data in accordance with the C-CDA Release 2.0 "Assessment and Plan Section (V2)" or both the "Assessment Section (V2)" and "Plan of Treatment Section (V2);" the "Goals Section;" and the "Health Concerns Section." We encouraged health IT developers to allow for structured documentation or tagging that would allow a provider to choose relevant pieces of assessment, plan of treatment, goals, and health concerns data that could be synthesized into a comprehensive care plan. We noted that all proposed 2015 Edition certification criteria that reference the "Common Clinical Data Set" (e.g., the "ToC" criterion) would therefore also require a Health IT Module to be able to capture "assessment and plan of treatment," "goals," and "health concerns" data.

Comments. A couple of commenters expressed concern regarding whether this proposal aligned with the C-CDA standard. One commenter found this inclusion to be duplicative since it is captured under "Care Plan Field(s)" and "Problems." A few commenters noted that we should clarify the intent of the "Goals Section" and "Health Concerns Section." These commenters noted that the "Goals Section" and "Health Concerns Section" of the C-CDA Care Plan document template provide more structure and were originally designed to be used with the Care Plan document template. However, other C-CDA document templates, like CCD, allow for health concerns and goals to be included as a narrative within the "Assessment Section (V2)," "Plan of Treatment Section (V2)," or "Assessment and Plan Section (V2)."

Response. We have reviewed the C-CDA 2.1 standard and believe there is no misalignment with our proposal and that it provides the requisite specificity we described in the Proposed Rule (80 FR 16872). Therefore, we have adopted the specific data elements as proposed (i.e., "Assessment Section (V2)" and "Plan of Treatment Section (V2)" or "Assessment and Plan Section (V2);" "Goals Section;" and "Health Concerns Section"). We clarify that we will certify Health IT Modules to the "Goals Section" and the "Health Concerns Section" from the Care Plan document template for the purposes of meeting the Common Clinical Data Set definition. Thus, other C-CDA document templates such as CCD, Referral Note, and Discharge Summary would need to be able to exchange the structured "Goals Section" and "Health Concerns Section" in order to meet the Common Clinical Data Set definition.

Sexual Orientation, Gender Identity, and Other Data

We received recommendations for the inclusion of data in Common Clinical Data Set that we did not propose.

Comments. Commenters recommended that we include sexual orientation and gender identity (SO/GI), military history, and nutritional data in the Common Clinical Data Set definition.

Response. We have not included any of this data in the definition as this was outside the scope of our proposal and, more importantly, inclusion at this time would not give full consideration to the maturity of related standards, the readiness of health IT developers to exchange this data, the clinical relevance of the data, and other considerations for some of the data such as any potential privacy and security concerns. We note, however, that we have taken the intermediate step of including SO/GI data in the 2015 Edition "demographics" criterion, which is a criterion included in the 2015 Edition Base EHR definition. We refer readers to

section III.A.3 of this preamble for more information on the 2015 Edition "demographics" criterion and SO/GI data.

Table 8. Common Clinical Data Set

Data	2014 Edition Standard	2015 Edition Standard
Patient Name	No associated standard.	No associated standard.
Sex	No associated standard.	The standard specified in § 170.207(n)(1) – Birth sex must be coded in accordance with HL7 Version 3 (V3) Standard, Value Sets for AdministrativeGender and NullFlavor attributed as follows: (1) Male. M (2) Female. F (3) Unknown. nullFlavor UNK
Date of Birth	No associated standard.	No associated standard.
Race	The standard specified in § 170.207(f)(1) – The Office of Management and Budget Standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity, Statistical Policy Directive No. 15, as revised, October 30, 1997 (see "Revisions to the Standards for the Classification of Federal Data on Race and Ethnicity").	The standard specified in § 170.207(f)(2) - CDC Race and Ethnicity Code Set Version 1.0 (March 2000); and The standard specified in § 170.207(f)(1) for each race identified in accordance § 170.207(f)(2).
Ethnicity	The standard specified in § 170.207(f)(1) - The Office of Management and Budget Standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity, Statistical Policy Directive No. 15, as revised, October 30, 1997 (see "Revisions to the Standards for the Classification of Federal Data on Race and Ethnicity").	The standard specified in § 170.207(f)(2) - CDC Race and Ethnicity Code Set Version 1.0 (March 2000); and The standard specified in § 170.207(f)(1) for each ethnicity identified in accordance § 170.207(f)(2).
Preferred Language	The standard specified in § 170.207(g)(1) – As specified by the Library of Congress, ISO 639-2 alpha-3 codes limited to those that also have a corresponding alpha-2 code in ISO 639-1.	The standard specified in § 170.207(g)(2) – Request for Comments (RFC) 5646.
Smoking Status	The standard specified in § 170.207(h) – Smoking status must be coded in one of the following SNOMED CT® codes:	The standard specified in § 170.207(h) – Smoking status must be coded in one of the following SNOMED CT® codes:

	(1) Current every day smoker. 449868002 (2) Current some day smoker. 428041000124106 (3) Former smoker. 8517006 (4) Never smoker. 266919005 (5) Smoker, current status unknown. 77176002 (6) Unknown if ever smoked. 266927001 (7) Heavy tobacco smoker. 428071000124103 (8) Light tobacco smoker. 428061000124105	(1) Current every day smoker. 449868002 (2) Current some day smoker. 428041000124106 (3) Former smoker. 8517006 (4) Never smoker. 266919005 (5) Smoker, current status unknown. 77176002 (6) Unknown if ever smoked. 266927001 (7) Heavy tobacco smoker. 428071000124103 (8) Light tobacco smoker. 428061000124105
Problems	At a minimum, the standard specified in § 170.207(a)(3) – IHTSDO SNOMED CT® International Release July 2012 and US Extension to SNOMED CT® March 2012 Release.	At a minimum, the standard specified in § 170.207(a)(4) - IHTSDO SNOMED CT®, U.S. Edition, September 2015 Release.
Medications	At a minimum, the standard specified in § 170.207(d)(2) – RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine, August 6, 2012 Release.	At a minimum, the standard specified in § 170.207(d)(3) – RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine, September 8, 2015 Release.
Medication Allergies	At a minimum, the standard specified in § 170.207(d)(2) – RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine, August 6, 2012 Release.	At a minimum, the standard specified in § 170.207(d)(3) – RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine, September 8, 2015 Release.
Laboratory Test(s)	At a minimum, the standard specified in § 170.207(c)(2) – Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.40, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc.	At a minimum, the standard specified in § 170.207(c)(3) – Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.52.
Laboratory Value(s)/Result(s)	No associated standard.	No associated standard.
Vital Signs	Height/length, weight, blood pressure, and BMI (no associated	The patient's diastolic blood pressure, systolic blood pressure, body height,

	vocabulary standard).	body weight, heart rate, respiratory rate, body temperature, pulse oximetry, and inhaled oxygen concentration must be exchanged in numerical values only; and in accordance with the standard specified in § 170.207(c)(3) and with the associated applicable unit of measure for the vital sign measurement in the standard specified in § 170.207(m)(1). § 170.207(c)(3) – Logical Observation Identifiers Names and Codes (LOINC®) version 2.52. § 170.207(m)(1) – The Unified Code of Units of Measure, Revision 1.9, October 23, 2013. Optional. The patient's BMI percentile per age and sex for youth 2-20 years of age, weight for age per length and sex for children less than 3 years of age, and head occipital-frontal circumference for children less than 3 years of age must be recorded in numerical values only in accordance with the standard specified in § 170.207(c)(3) and with the associated applicable unit of measure for the vital sign measurement in the standard specified in § 170.207(m)(1). For BMI percentile per age and sex for youth 2-20 years of age and weight for age per length and sex for children less than 3 years of age, the reference range/scale or growth curve should be included as appropriate.
Care Plan Field(s), including Goals and Instructions	No associated standard.	Not applicable (replaced with Assessment and plan of treatment, goals, and health concerns – see below).
Procedures	At a minimum, the version of the standard specified in § 170.207(a)(3), or § 170.207(b)(2). § 170.207(a)(3) - IHTSDO SNOMED CT® International Release July 2012 and US Extension to SNOMED CT® March 2012 Release § 170.207(b)(2) – The code set	At a minimum, the version of the standard specified in § 170.207(a)(4), or § 170.207(b)(2). § 170.207(a)(4) - IHTSDO SNOMED CT®, U.S. Edition, September 2015 Release § 170.207(b)(2) – The code set specified in 45 CFR 162.1002(a)(5) – The combination of Health Care Financing

	specified in 45 CFR 162.1002(a)(5) – The combination of Health Care Financing Administration Common Procedure Coding System (HCPCS), as maintained and distributed by HHS, and Current Procedural Terminology, Fourth Edition (CPT-4), as maintained and distributed by the American Medical Association, for physician services and other health care services. These services include, but are not limited to, the following: (1) Physician services. (2) Physical and occupational therapy services. (3) Radiologic procedures. (4) Clinical laboratory tests. (5) Other medical diagnostic procedures. (6) Hearing and vision services. (7) Transportation services including ambulance. For technology primarily developed to record dental procedures, the standard specified in § 170.207(b)(3) - The code set specified in 45 CFR 162.1002(a)(4) – *Code on Dental Procedures and Nomenclature*, as maintained and distributed by the American Dental Association, for dental services.	Administration Common Procedure Coding System (HCPCS), as maintained and distributed by HHS, and Current Procedural Terminology, Fourth Edition (CPT-4), as maintained and distributed by the American Medical Association, for physician services and other health care services. These services include, but are not limited to, the following: (1) Physician services. (2) Physical and occupational therapy services. (3) Radiologic procedures. (4) Clinical laboratory tests. (5) Other medical diagnostic procedures. (6) Hearing and vision services. (7) Transportation services including ambulance. For technology primarily developed to record dental procedures, the standard specified in § 170.207(b)(3) - The code set specified in 45 CFR 162.1002(a)(4) – *Code on Dental Procedures and Nomenclature*, as maintained and distributed by the American Dental Association, for dental services.
Care Team Member(s)	No associated standard.	No associated standard.
Immunizations	Immunization data not included for 2014 Edition certification.	In accordance with, at a minimum, the standards specified in § 170.207(e)(3) and (4). § 170.207(e)(3) - HL7 Standard Code Set CVX—Vaccines Administered, updates through August 17, 2015 § 170.207(e)(4) - National Drug Code Directory (NDC) – Vaccine NDC Linker, updates through August 17, 2015
Unique Device Identifier(s) (UDIs) for a Patient's	UDI data not included for 2014 Edition certification.	In accordance with the "Product Instance" in the "Procedure Activity Procedure Section" of the standard specified in § 170.205(a)(4).

Implantable Device(s)		§ 170.205(a)(4) - HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes, Draft Standard for Trial Use, Release 2.1. <u>Unique device identifier</u> is defined as it is in 21 CFR 801.3 - means an identifier that adequately identifies a device through its distribution and use by meeting the requirements of 830.20 of this chapter. A unique device identifier is composed of: (1) A device identifier --a mandatory, fixed portion of a UDI that identifies the specific version or model of a device and the labeler of that device; and (2) A production identifier --a conditional, variable portion of a UDI that identifies one or more of the following when included on the label of the device: (i) The lot or batch within which a device was manufactured; (ii) The serial number of a specific device; (iii) The expiration date of a specific device; (iv) The date a specific device was manufactured; (v) For an HCT/P regulated as a device, the distinct identification code required by 1271.290(c) of this chapter. <u>Implantable device</u> is defined as it is in 21 CFR 801.3 – means a device that is intended to be placed in a surgically or naturally formed cavity of the human body. A device is regarded as an implantable device for the purpose of this part only if it is intended to remain implanted continuously for a period of 30 days or more, unless the Commissioner of Food and Drugs determines otherwise in order to protect human health.
Assessment and Plan of Treatment	Not applicable (refer to care plan field(s), including goals and instructions – see above).	§ 170.205(a)(4) - HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for

		Clinical Notes, Draft Standard for Trial Use, Release 2.1.
Goals	Not applicable (refer to care plan field(s), including goals and instructions – see above).	In accordance with the "Goals Section" of the standard specified in § 170.205(a)(4). § 170.205(a)(4) - HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes, Draft Standard for Trial Use, Release 2.1.
Health Concerns	Not applicable (refer to care plan field(s), including goals and instructions – see above).	In accordance with the "Health Concerns Section" of the standard specified in § 170.205(a)(4). § 170.205(a)(4) - HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes, Draft Standard for Trial Use, Release 2.1.

Alignment with Clinical Practice

We requested comment in the Proposed Rule on ways in which we can engage the public to keep the Common Clinical Data Set relevant to clinical practice as the data included in the Common Clinical Data Set may change over time.

Comments. A commenter suggested we limit the use of highly prescriptive criteria, permitting innovation and clinical appropriateness to exist within "guardrails." Another commenter encouraged us to seek input from provider specialty societies and organizations to ensure the interests of clinicians are properly represented, including concerns about clinical workflows.

Response. We thank commenters for their feedback. We will take these comments under consideration for further development and uses of the Common Clinical Data Set to support interoperability, program alignment, and patient care.

4. Cross-referenced FDA Definitions

We proposed to adopt in § 170.102 new definitions for "Implantable Device," "Unique

Device Identifier," "Device Identifier," and "Production Identifier" as discussed in the Proposed Rule's sections for the "implantable device list" certification criterion. We proposed to adopt the same definitions already provided to these phrases at 21 CFR 801.3 and emphasized that capitalization was purposefully applied to each word in these defined phrases in order to signal to readers that they have specific meanings.

Comments. Commenters expressed unanimous support for our proposed approach to cross-reference relevant FDA definitions. One commenter recommended that we use the term "identifiers" when referring to Device Identifier and Product Identifier instead of the term "UDI data." The commenter contended that this would align better with FDA terminology.

Response. We thank commenters for their support. We are adopting the cross-referenced FDA definitions as proposed. In regard to the recommendation to use the term "identifiers," we agree that our terminology related to UDIs should more closely align with FDA terminology and the UDI final rule to prevent any unnecessary confusion. Therefore, we have revised our terminology use within this final rule and refer readers to the "implantable device list" certification criterion discussed earlier in this preamble for further details.

IV. Provisions of the Proposed Rule Affecting the ONC Health IT Certification Program

A. Subpart E – ONC Health IT Certification Program

We proposed to replace the term "HIT" with the term "health IT" and to change the name of the "ONC HIT Certification Program" to the "ONC Health IT Certification Program" wherever these references occur in subpart E. In referring to the certification program, we noted that the term "health" is capitalized. We also proposed to remove § 170.553 "Certification of health information technology other than Complete EHRs and EHR Modules" as no longer

relevant due to proposals in the Proposed Rule for the ONC Health IT Certification Program that would make the program more open and accessible to health IT beyond EHR technology.

Comments. Commenters were broadly supportive of these proposals.

Response. We have adopted these proposals as proposed.

B. Modifications to the ONC Health IT Certification Program

In the Voluntary Edition proposed rule (79 FR 10929-30) we recited our authority and the history of the ONC Health IT Certification Program. The history includes multiple requests for comment and significant stakeholder feedback on making the certification program more accessible to health IT beyond EHR technology and health care settings and practices not directly tied to the EHR Incentive Programs. With consideration of stakeholder feedback and our policy goals, we attempted to make the ONC Health IT Certification Program more open and accessible through a proposal in the Voluntary Edition proposed rule (79 FR 10918-20) to create "meaningful use" (MU) and non-MU EHR Modules. We determined that our proposal was not the best approach in a subsequent final rule (79 FR 54472-73). Since that rulemaking, the HITPC issued recommendations supporting certification for care/practice settings beyond the ambulatory and inpatient settings.[166] In response, we reconsidered how best to structure the program and make it open and accessible to more types of health IT, health IT that supports a variety of care and practice settings, and programs that may reference the ONC Health IT Certification Program, including Medicaid and Medicare payment programs and various grant programs. In the Proposed Rule, we proposed revisions to the ONC Health IT Certification Program to achieve these goals, including new certification criteria for use cases and health care settings beyond the EHR Incentive Programs.

[166] http://www.healthit.gov/facas/sites/faca/files/TransmittalLetter_LTPAC_BH_Certification.pdf and http://www.healthit.gov/facas/sites/faca/files/HITPC_LTPAC_BH_Certification_Recommendations_FINAL.pdf

Comments. Most commenters supported the increase in scope of technologies and health care settings to include lab information systems, HISPs, HIEs, LTPAC, behavioral health, and pediatrics. Commenters supported opening the certification program to greater accessibility to more health IT, allowing for greater flexibility and use of a variety of health IT products and services, and advancing interoperability beyond narrowly defined EHR technology. Some commenters, however, opposed a more open ONC Health IT Certification Program and the use of certified health IT beyond the EHR Incentive Programs, including linking forms of Medicare and Medicaid reimbursement to the use of certified health IT.

Response. We disagree with the commenters that do not support a more open ONC Health IT Certification Program and the use of certified health IT beyond the EHR Incentive Programs. We believe the ONC Health IT Certification Program should be open and accessible to more types of health IT, health IT that supports a variety of care and practice settings, and programs beyond the EHR Incentive Programs. We have finalized provisions and adopted 2015 Edition certification criteria to support these goals. As discussed in more detail below in regard to referencing the use of certified health IT, ONC and HHS continue to encourage the use of certified health IT to support interoperability and health information exchange across diverse care and practice settings, including the linking of certified health IT to reimbursement under HHS payment programs.

1. Health IT Modules

We proposed to rename EHR Modules as Health IT Modules by removing the EHR Module definition from the CFR at § 170.102 and adding the "Health IT Module" definition. We proposed this change to be effective with this final rule, and we proposed to make this change applicable for certification to the 2014 Edition and 2015 Edition. We stated that the proposed

change would have no substantive impact on the technologies that might be, or have been, certified under the ONC Health IT Certification Program. We also noted that technologies already certified to the 2014 Edition as EHR Modules, and their use to meet the CEHRT definition, would not be affected by this proposal.

Comments. Many commenters strongly supported the removal of "Complete EHR" certification in favor of modular certification. A couple of commenters requested that we clarify what exactly constitutes a Health IT Module, saying that deviations in this definition will lead to inaccurate assessments of workload requirements and scope of impact to implement a specific certification criterion.

Response. We thank commenters for their feedback. The 2014 Edition Release 2 final rule discontinued the "Complete EHR" certification concept (see 79 FR 54443-45). "Complete EHR" certification will not be available to the 2015 Edition.

The definition of a Health IT Module is any service, component, or combination thereof that can meet the requirements of at least one certification criterion adopted by the Secretary (see § 170.102). This essentially means any type of technology that could be certified to one or more certification criteria under the ONC Health IT Certification Program. For example, a Health IT Module could be certified to only the 2015 Edition "CPOE – medications" criterion and the other required mandatory and conditional criteria (i.e., the 2015 Edition "safety-enhanced design," "quality management system," "accessibility-centered design," and applicable privacy and certification criteria). Alternatively, a Health IT Module could be certified to practically all the 2015 Edition certification criteria. While we appreciate commenters' requests for further specificity for the Health IT Module definition, we believe that this definition affords flexibility for health IT developers and providers in terms of what technologies are presented for

certification and to what certification criteria (e.g., technology provided by a HISP that is presented for certification to the 2015 Edition "Direct Project, Edge Protocol, and XDR/XDM" certification criterion (§ 170.315(h)(2)) or an EHR technology presented by a developer for certification to the 2015 Edition "CDS" certification criterion (§ 170.315(a)(9)).

2. "Removal" of Meaningful Use Measurement Certification Requirements

We proposed to not require ONC-ACBs to certify Health IT Modules to the 2015 Edition "meaningful use measurement" certification criteria (§ 170.315(g)(1) "automated numerator recording" and § 170.315(g)(2) "automated measure calculation"). We explained that we believe this will make the ONC Health IT Certification more accessible to the certification of health IT for other purposes beyond the EHR Incentive Programs. We also emphasized that this proposed approach would not preclude health IT developers from seeking certification to § 170.315(g)(1) or (2) in support of their customers' and providers' needs related to the EHR Incentive Programs.

Comments. A commenter stated that these criteria and their functionality have been well-established through certification to the 2014 Edition "automated measure calculation" and "automated numerator recording" certification criteria; and therefore, their removal should have minimal effect. Several commenters voiced support for removal of these requirements. One commenter noted that this change will not reduce the requirements for accredited testing laboratories to test nor ONC-ACBs to certify these criteria when a health IT developer elects to certify a product for use in the EHR Incentive Programs. A commenter disagreed with removal of these criteria, stating that this functionality is important for EPs and EHs to meet requirements under the EHR Incentive Programs and for purposes of their own quality improvement efforts.

Response. We have adopted our proposed approach in that we will not require ONC-ACBs to certify Health IT Modules to the 2015 Edition "meaningful use measurement"

certification criteria. However, the EHR Incentive Program Stage 3 and Modifications final rule includes a CEHRT definition that will require EPs, eligible hospitals, and CAHs to have health IT certified to these criteria in order to meet the CEHRT definition. Accordingly, we encourage health IT developers supporting providers participating in the EHR Incentive Programs or providers' quality improvement needs to seek certification to these criteria as appropriate for their Health IT Modules (e.g., a Health IT Module is presented for certification to a criterion that supports a Stage 3 objective with a percentage-based measure and the Health IT Module can meet the "automated numerator recording" criterion or "automated measure calculation" criterion).for their Health IT Module (e.g., the Health IT Module is presented for certification to a criterion that supports a Stage 3 objective percentage-based measure and the Health IT Module can meet the "automated numerator recording" criterion or "automated measure calculation" criterion).

3. Types of Care and Practice Settings

We commented in the Proposed Rule that we had proposed a diverse edition of health IT certification criteria with capabilities included that could support a wide range of providers practicing in various settings. We stated that we anticipated that we would issue general interoperability guidance for the 2015 Edition when it became final, but that we had no plans to independently develop and issue certification "paths" or "tracks" by care or practice setting (e.g., a "LTPAC certification") because it would be difficult to independently devise such "paths" or "tracks" in a manner that was sure to align with other relevant programs and specific stakeholder needs. We explained that we are best suited for supporting the development of standards for specific settings/use cases and providing technical assistance to both health IT developers and providers about the certification criteria, the standards and capabilities they include, and the

processes of the ONC Health IT Certification Program. We stated that we would welcome working with HHS agencies, other agencies, or provider associations, in identifying the appropriate functionality and certification criteria to support their stakeholders, including jointly developing specialized certification "paths" or "tracks." We noted that such an approach would be consistent with stakeholder feedback we received through rulemaking (79 FR 54473-74) and the HITPC recommendations for us to work with HHS agencies and other agencies.

We sought comment on potential future certification criteria that could include capabilities that would uniquely support LTPAC, behavioral health, or pediatrics care\practice settings, as well as other settings. In particular, we sought comment on whether certification criteria focused on patient assessments for certain settings would be of value to health IT developers and health care providers.

Comments. A commenter suggested that patient assessments should not be included in future certification criteria. A commenter requested that EHR certification standards adequately capture and address data elements necessary to support the home care setting – specifically for durable medical equipment prosthetics, orthotics, and supplies (collectively, DMEPOS). The HITPC listed several entities that may find certification requirements applicable to them, including pharmacy information systems, long-term services and support providers (transport, meals, care management services, etc.), ambulance providers, blood banks, end-stage renal disease facilities, free-standing cancer hospitals, visiting nurse services, outpatient surgical centers, telehealth and monitoring, personal health devices (e.g. bands, watches, monitors), biomedical tech devices (e.g. pacemakers), personal health record systems, health and fitness centers, free-standing weight-loss centers. One commenter recommended including standards and capabilities to include e-signatures to the Home Health and Hospice Plans of Treatment.

Multiple commenters suggested that modular certification should follow "tracks" or "pathways" for specialists to identify what they need. Some commenters requested that we publish guidelines as to which criteria are applicable to which care settings. These commenters suggested that "certification tracks" could be established for each different segment of the provider market (laboratories, behavioral health, long-term care, etc.) looking for alignment and interoperability across certification "tracks." A commenter questioned how we and stakeholders would monitor claims that a set of independently certified Health IT Modules meet the requirements of the path or track.

Response. We appreciate the breadth and diversity of comments on potential future certification criteria that could include capabilities to support different care settings and use cases. Consistent with our request for comment in the Proposed Rule, we will carefully consider these suggestions for future certification criteria.

As mentioned in the Proposed Rule and recited above, we do not intend to develop certification "tracks" or "pathways" for particular provider specialties or settings within this final rule because it would be difficult for us to independently devise such "paths" or "tracks" in a manner that was sure to align with other relevant programs and specific stakeholder needs. We are, however, working with our colleagues within HHS to identify capabilities and certification criteria that support other programs and use cases. We also continue to welcome the opportunity to collaborate with representatives from different provider and specialties societies as well as health IT developers to determine what certification criteria and "tracks" could be identified and developed to support various care and practice settings and particular use cases. We do not anticipate monitoring any developed certification "tracks." Rather, we anticipate that a program or association, as applicable, would develop any necessary compliance requirements.

4. Referencing the ONC Health IT Certification Program

We stated in the Proposed Rule that the adoption of proposed criteria that support functionality for different care and practice settings and the proposals to make the ONC Health IT Certification Program open and accessible to more types of health IT and health IT that supports a variety of care and practice settings, would permit further referencing and use of certified health IT. We proceeded to cite other HHS programs that reference certification criteria and the ONC Health IT Certification Program (80 FR 16874).

Comments. One commenter recommended that we not over-specify or over-bundle a singular certification criterion that could cause a mismatch between what a federal program requires and what is defined as a single criterion. Another commenter recommended that we allow for at least 18 months in advance of any compliance dates for providers and health IT developers to successfully test and deploy required certified health IT, stating that an 18-month minimum timeframe is important to ensure that the process provides good design while reducing risks to care and safety.

Response. We agree with the commenter that it is important to try to properly scope a certification criterion so that the capabilities included are consistent with current health IT technologies and design practices. In this regard, we have separated out capabilities that have once been proposed or adopted in a single criterion (e.g., see the "CPOE" criteria or the "application access" ("API") criteria).

We also agree with the commenter that sufficient lead time must be provided for development, testing, certification, and implementation before certified health IT is required for use. With this final rule and the EHR Incentive Programs Stage 3 and Modifications final rule, providers and health IT developers have 27 months before health IT certified to the 2015 Edition

must be used to meet the CEHRT definition adopted in the EHR Incentive Programs Stage 3 and Modifications final rule published elsewhere in this issue of the **Federal Register**. This timeframe should provide sufficient time for development, testing, certification, and implementation of certified health IT. We plan to continue to work with our colleagues in HHS to ensure that proper lead time is considered with respect to the required use of certified health IT.

We continue to support the use of certified health IT and the ONC Health IT Certification Program to support interoperability and health information exchange across diverse care and practice settings. To note and building on the references we cited in the Proposed Rule, the HHS interoperability strategy and the encouraged use of certified health IT are mentioned in the Prospective Payment System and Consolidated Billing for Skilled Nursing Facilities for FY 2015 proposed rule (79 FR 45652), the Conditions of Participation for Home Health Agencies proposed rule (79 FR 61185), the CY 2016 Home Health Prospective Payment System Rate Update; Home Health Value-Based Purchasing Model; and Home Health Quality Reporting Requirements proposed rule (80 FR 39844), and the End-Stage Renal Disease Prospective Payment System, and Quality Incentive Program proposed rule (80 FR 37852). The required use of certified health IT continues to be referenced for chronic care management services in CY 2016 Physician Fee Schedule final rule (80 FR 41796). Further, the Mechanized Claims Processing and Information Retrieval Systems (MMIS) proposed rule (80 FR 20464) requires that state MMIS systems align with adopted standards and allow for interoperability with health information exchanges.

C. Health IT Module Certification Requirements

1. Privacy and Security

We proposed a new approach for privacy and security (P&S) certification to the 2015 Edition. In our past rulemakings, we discussed and instituted two different policy approaches and sought comment on others for ensuring that health IT and providers have privacy and security capabilities while also trying to minimize the level of regulatory burden imposed on health IT developers. With the 2011 Edition, we included an upfront requirement that required Health IT Modules to meet all P&S certification criteria as a condition of certification unless the health IT developer could demonstrate that certain P&S capabilities were either technically infeasible or inapplicable. With the 2014 Edition, we eliminated the upfront requirement for each Health IT Module to be certified against the P&S criteria in favor of what we thought would better balance the burden potentially posed by our rulemaking. Thus, the P&S criteria were made part of the 2014 Edition Base EHR definition that all EPs, eligible hospitals, and CAHs participating in the EHR Incentive Programs must meet in order to satisfy the CEHRT definition (meaning each provider needed post-certification to ultimately have technology certified to the P&S criteria).

Based on recommendations from the HITSC, in the Proposed Rule, we proposed a revised P&S certification approach for the 2015 Edition so that each certification criterion has a set of appropriate P&S "safeguards" that must be in place. We proposed to require that an ONC-ACB must ensure that a Health IT Module presented for certification to any of the certification criteria that fall into each regulatory text "first level paragraph" category of § 170.315 (e.g., § 170.315(a)) identified below would be certified to either Approach 1 (technically demonstrate) or Approach 2 (system documentation) as follows:

Table 9. Proposed 2015 Edition Privacy and Security Certification Framework		
If the Health IT Module includes capabilities for certification listed under:	**It will need to be certified to Approach 1 or Approach 2 for each of the P&S certification criteria listed in the "Approach 1" column**	
	Approach 1	**Approach 2**
§ 170.315(a)	§ 170.315(d)(1) (authentication, access control, and	For each applicable P&S certification criterion not

	authorization), (d)(2) (auditable events and tamper resistance), (d)(3) (audit reports), (d)(4) (amendments), (d)(5) (automatic log-off), (d)(6)(emergency access), and (d)(7) (end-user device encryption)	certified for approach 1, there must be system documentation sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces for each applicable privacy and security certification criterion that enable the Health IT Module to access external services necessary to meet the privacy and security certification criterion.
§ 170.315(b)	§ 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8) (integrity)	
§ 170.315(c)	§ 170.315(d)(1) through (d)(3)	
§ 170.315(e)	§ 170.315(d)(1) through (d)(3), (d)(5), and (d)(7)	
§ 170.315(f)	§ 170.315(d)(1) through (d)(3) and (d)(7)	
§ 170.315(h)	§ 170.315(d)(1) through (d)(3)	
§ 170.315(i)	§ 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8)	

We explained that under the P&S certification framework we proposed, a health IT developer would know exactly what it needed to do in order to get its Health IT Module certified and a purchaser of a Health IT Module would know exactly what privacy and security functionality against which the Health IT Module had to be tested in order to be certified. We further explained that, because we explicitly proposed which P&S certification criteria would be applicable to the associated criteria adopted in each regulatory text "first level paragraph" category and also proposed Approach 2, we did not propose to permit the 2011 Edition policy of allowing for a criterion to be met through documentation that the criterion is inapplicable or would be technically infeasible for the Health IT Module to meet.

Comments. Most commenters were supportive of our proposed P&S certification framework, including the HITSC. One commenter recommended that we keep the option for a health IT developer to attest that a certain security criterion is inapplicable or infeasible. Another commenter was concerned that a health IT developer would have to redundantly certify products that have a shared security infrastructure.

Response. We appreciate the broad support expressed for the proposed framework. We have adopted the P&S certification framework as proposed. As recited above and stated in the Proposed Rule, we continue to believe it is not necessary to permit health IT developers to attest that certain P&S criteria are inapplicable or infeasible because we have specified which P&S certification criteria are applicable to a Health IT Module based on the other adopted 2015 Edition certification criteria for which it is presented for certification to as well as also permitting certification through Approach 2. We clarify that Approach 2 provides health IT developers with the ability to demonstrate through system documentation that products share a security infrastructure, giving developers the option to certify the security infrastructure only once.

Comments. Several commenters provided feedback suggesting which 2015 Edition P&S certification criteria should apply to each grouping of 2015 Edition certification criteria in Table 9 above. Commenters recommended that we should add the:

- "Integrity" certification criterion (§ 170.315(d)(8)) to the clinical certification criteria (§ 170.315(a)) due to transmissions of laboratory data per the proposed "CPOE – laboratory" certification criterion (§ 170.315(a)(2));
- "Amendments" certification criterion (§ 170.315(d)(4)) to the care coordination criteria (§ 170.315(b)) to support patient requested amendments; and
- "Automatic access time-out" certification criterion (§ 170.315(d)(5)) to the clinical quality measures criteria (§ 170.315(c)) since patient health information is evident in many quality measurement implementations.

Response. We have not adopted the commenter's recommendation to apply the "integrity" certification criterion (§ 170.315(d)(8)) to the clinical certification criteria because we have not adopted the proposed content exchange functionality for the "CPOE – laboratory"

certification criterion. By not adopting the content exchange functionality (LOI standard), testing and certification will not involve the preparation of patient laboratory data for transmission consistent with the proposed standards. Therefore, the "integrity" certification criterion (§ 170.315(d)(8)) does not need to be applied to the category of criteria (i.e., § 170.315(a)).

The application of the "amendment" criterion is not necessary for care coordination. We have made the "amendment" criterion applicable to the "clinical care" category of criteria (i.e., § 170.315(a)). The functionality certified under the "clinical care" category focuses on data capture and is more appropriate for application of the "amendment" criterion, while the "care coordination" category focuses on the transmission of health information and not patient interaction related to amending the record.

We agree with commenters that the "automatic access time-out" criterion should apply to the clinical quality measures criteria for the reasons provided by the commenters and have included it as applicable to § 170.315(c) under the P&S certification framework. As discussed in the "application access to Common Clinical Data Set" section of this preamble, we have adopted and applied new P&S criteria ("trusted connection" (§ 170.315(d)(9) and "auditing actions on health information" (§ 170.315(d)(10)) to the three "API" certification criteria as part of the P&S certification framework. These new criteria are derived from the security requirements included in the proposed "API" criterion in the Proposed Rule and have been applied back to the "API" criteria adopted in this final rule.

We have separated out the "patient engagement" category (§ 170.315(e)) by criterion to provide clarity and appropriate application of privacy and security capabilities. In this regard, we do not apply "end-user device encryption" to the "secure messaging" and "patient health information capture" criteria as that was not our intention. We have added the new "trusted

connection" criteria to the "patient engagement" category (§ 170.315(e)) to compliment the revisions we made to the "VDT" and "secure messaging" criteria as part of the overall P&S certification framework and to support the functionality included in the "patient health information capture" criterion. Please see the discussions of these criteria earlier in this preamble for further details.

In this final rule, we require that an ONC-ACB must ensure that a Health IT Module presented for certification to any of the certification criteria that fall into each regulatory text "first level paragraph" category of § 170.315 (e.g., § 170.315(a)) identified in Table 10 below is certified to either Approach 1 (technically demonstrate) or Approach 2 (system documentation) as follows:

Table 10. Final 2015 Edition Privacy and Security Certification Framework		
If the Health IT Module includes capabilities for certification listed under:	**It will need to be certified to approach 1 or approach 2 for each of the P&S certification criteria listed in the "approach 1" column**	
	Approach 1	**Approach 2**
§ 170.315(a)	§ 170.315(d)(1) (authentication, access control, and authorization), (d)(2) (auditable events and tamper resistance), (d)(3) (audit reports), (d)(4) (amendments), (d)(5) (automatic log-off), (d)(6) (emergency access), and (d)(7) (end-user device encryption)	For each applicable P&S certification criterion not certified for approach 1, the health IT developer may certify for the criterion using system documentation sufficiently detailed to enable integration with external services necessary to meet the criterion.
§ 170.315(b)	§ 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8) (integrity)	
§ 170.315(c)	§ 170.315(d)(1) through (d)(3) and (d)(5)*	
§ 170.315(e)(1)	§ 170.315(d)(1) through (d)(3), (d)(5), (d)(7), and (d)(9)(trusted connection)*	
§ 170.315(e)(2) and (3)	§ 170.315(d)(1) through (d)(3), (d)(5), and (d)(9)*	
§ 170.315(f)	§ 170.315(d)(1) through (d)(3) and (d)(7)	
§ 170.315(g)(7), (8) and (9)*	§ 170.315(d)(1) and (d)(9); and (d)(2) or (d)(10) (auditing actions on health information)*	
§ 170.315(h)	§ 170.315(d)(1) through (d)(3)	
*Emphasis added to identify additions to the framework as compared to the Proposed Rule.		

We clarify that of the adopted 2015 Edition certification criteria, only the privacy and security criteria and the criteria specified in § 170.315(g)(1) through (6) are exempt from the P&S certification framework due to the capabilities included in these criteria, which do not implicate privacy and security concerns.

In order to be issued a certification, a Health IT Module would only need to be tested once to each applicable privacy and security criterion identified as part of Approach 1 or Approach 2 so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification, except for the certification of a Health IT Module to § 170.315(e)(1) "VDT" and (e)(2) "secure messaging." For each criterion, a Health IT Module must be separately tested to § 170.315(d)(9) because of the specific capabilities for secure electronic transmission and secure electronic messaging included in each criterion, respectively.

Comments. We received several comments requesting clarification on our proposal to allow a health IT developer to certify for P&S criteria using system documentation sufficiently detailed to enable integration with external services necessary to meet P&S certification criteria (Approach 2). One commenter requested clarification regarding how an ONC-ACB would verify that documentation was sufficient to implement the interface. Another commenter pointed out that interfaces to external systems may carry an additional cost. Other commenters questioned whether the lack of standardized interfaces will lead to security gaps or be an impediment to information sharing.

Response. System documentation for Approach 2 requires a clear description of how the external services necessary to meet the applicable P&S criteria would be deployed and used. We note that Approach 2 is one of two options that provide health IT developers more certification

flexibility. Health IT developers and their customers have the discretion to seek certification to the approach (Approach 1 or 2) that best meets their needs, taking into account efficiencies, costs, and security concerns. We further note that the actual implementation of privacy and security capabilities is outside the scope of certification, but in most instances, is guided by applicable federal and state privacy and security laws. We are supportive of the unencumbered exchange of health information and note that certified capabilities should not be implemented in a way that precludes health information sharing.

Comments. A commenter requested clarification on how a health IT developer could guarantee certain functionality, particularly end-user device encryption.

Response. Certification ensures that a Health IT Module can meet the capabilities of a certification criterion. However, it does not ensure the appropriate implementation of the capabilities. For example, in the context of a Health IT Module's certification to the "VDT" criterion (§ 170.315(e)(1)), additional required certification to the "end-user device encryption" criterion is intended to apply to the storage actions that the Health IT Module is programmed to take (i.e., creation of temp files, cookies, or other types of cache approaches) and not an individual or isolated user action to save or export a file to their personal electronic storage media.

Comments. A commenter stated that the P&S certification framework is more specific than the approach prescribed in the HIPAA Security Rule. Another commenter stated that we should not name specific encryption and hashing standards because the information security risk landscape is constantly evolving.

Response. The P&S certification framework focuses on the capabilities of health IT certified to the 2015 Edition. It is not designed nor could it align with each covered entity's

responsibilities under the HIPAA Security Rule, which focus on a risk-based approach to security. We note, however, that the adoption of health IT certified to the 2015 Edition under the P&S framework may support a provider's compliance with the HIPAA Security Rule and other federal and state privacy and security laws. We do not require specific standards for encryption and hashing. Rather, we require any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2, October 8, 2014[167]. For hashing, we require any hashing algorithm with security strength equal to or greater than SHA-2 as identified by NIST as an approved security function in that publication.

2. Design and Performance (§ 170.315(g))

We proposed to revise § 170.550 to add paragraph (g), which would require ONC-ACBs to certify Health IT Modules to certain proposed certification criteria under § 170.315(g). We proposed to require ONC-ACBs to certify Health IT Modules to § 170.315(g)(3) (safety-enhanced design) and § 170.315(g)(6) (Consolidated CDA creation performance) consistent with the requirements included in these criteria. We noted that paragraph (g) also includes a requirement for ONC-ACBs to certify all Health IT Modules presented for certification to the 2015 Edition to § 170.315(g)(4) (quality system management) and (g)(8) (accessibility-centered design). We explained that the proposed certification requirements for § 170.315(g)(3) and (4) maintain the policy approach established with certification to the 2014 Edition (see § 170.550(f)(2) and (3)), which ensures Health IT Modules, as applicable, are certified to these specific safety and quality certification criteria. We also explained that the proposed certification requirement for § 170.315(g)(6) is associated with the new "Consolidated CDA creation

[167] http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf

performance" criterion we proposed for the 2015 Edition. We reiterated that the requirement is similarly designed to ensure that Health IT Modules (with Consolidated CDA creation capabilities within their scope) are also certified to the "Consolidated CDA creation performance" criterion. We noted the proposed certification requirements for § 170.315(g)(8) were associated with the new "accessibility-centered design" criterion we proposed for the 2015 Edition, which patterned the certification approach of the 2014 Edition "quality system management" criterion.

Comments. Commenters supported the proposed revisions to § 170.550.

Response. We thank commenters for their support. We have added paragraph (g) to § 170.550 as proposed with a minor cross-reference revision that points to the 2015 Edition "accessibility-centered design" criterion codified in § 170.315(g)(5) instead of proposed paragraph (g)(8).

D. Principles of Proper Conduct for ONC-ACBs

1. "In-the-Field" Surveillance and Maintenance of Certification

We proposed new requirements for "in-the-field" surveillance and maintenance of certification under the ONC Health IT Certification Program. The requirements would clarify and expand ONC-ACBs' existing surveillance responsibilities, including the responsibility to perform surveillance of certified capabilities "in the field." We explained that in-the-field surveillance is necessary to provide assurance to customers, implementers, and users that health IT certified on behalf of ONC will continue to meet the requirements of its certification when it is implemented and used in a production environment. Through our proposal, we sought to promote greater consistency, transparency, and rigor in the surveillance of certified capabilities

and to provide stakeholders with greater clarity and predictability regarding this important aspect of the ONC Health IT Certification Program.

Our proposal defined in-the-field surveillance and specified certain conditions and procedures under which ONC-ACBs would be required to initiate in-the-field surveillance of certified Complete EHRs and certified Health IT Modules. We delineated separate requirements for surveillance based on complaints or other information about potential non-conformities ("reactive surveillance") and for surveillance based on a random sampling approach ("randomized surveillance"). In addition, we specified certain corrective action plan requirements and procedures that would apply in the context of randomized surveillance. ONC-ACBs would also be required to report the results of their in-the-field surveillance to the National Coordinator on at least a quarterly basis and, separately, to report corrective action plan information to the publicly accessible open data CHPL detailed in our separate proposal "Open Data Certified Health IT Product List (CHPL)."

To implement the new requirements for in-the-field surveillance outlined in the Proposed Rule, we proposed to add § 170.556 (In-the-field surveillance and maintenance of certification for health IT) and amend § 170.503 (ONC-AA Ongoing Responsibilities) and § 170.523 (ONC-ACB Principles of Proper Conduct).

Definition and Principles for In-the-field Surveillance

We proposed to explicitly define in-the-field surveillance to mean an ONC-ACB's assessment of whether a certified Complete EHR or certified Health IT Module to which it has issued a certification continues to conform to the certification's requirements when the health IT is implemented and in use in the field. This assessment would require an ONC-ACB to assess the technology's capabilities in a production environment and, where applicable, would be based on

the use of the capabilities with protected health information (PHI), unless the use of test data were specifically approved by the National Coordinator. We explained that such surveillance could be performed through an in-person site visit or by remote observation. We solicited comments on these and other approaches to in-the-field surveillance.

Comments. We received mixed comments on our focus on "in-the-field" surveillance. The commenters who supported our focus on surveillance of certified health IT capabilities "in the field" expressed strong support for our proposal to define and establish clear and explicit expectations for in-the-field surveillance. Commenters stated that clearer and more rigorous requirements for in-the-field surveillance would promote confidence in certifications issued on behalf of ONC and significantly improve the reliability and performance of certified health IT. One ONC-ACB specifically endorsed these requirements and our commitment to ensure that certified health IT capabilities function for providers in their local offices and hospitals in the same manner demonstrated by the health IT developer in a controlled testing environment. Another ONC-ACB specifically supported the concept of in-the-field surveillance in the context of complaint-based surveillance, which has been a focus of the current approach to in-the-field surveillance developed through our annual surveillance guidance.

Several commenters described specific challenges they or their members had encountered with certified health IT capabilities that failed to perform in an acceptable manner when implemented in the field. For example, one commenter stated that it had witnessed several instances in which certified health IT that had successfully demonstrated the ability to send a single standards-compliant continuity of care document in a controlled testing environment could not "scale" and send multiple standards-compliant continuity of care documents when deployed

in a production environment. Commenters stated that our proposed in-the-field surveillance requirements would help identify and address these kinds of apparent non-conformities.

Response. We thank these commenters for their feedback. They underscore our view of the importance of in-the-field surveillance for ensuring that providers and other stakeholders can rely on certifications issued on behalf of ONC. This basic assurance protects the integrity of the ONC Health IT Certification Program and federal health IT investments because it enables customers, implementers, and users to select appropriate technologies and capabilities; identify potential implementation or performance issues; and implement certified health IT in a predictable, reliable, and successful manner.

While ONC-ACBs are already required to conduct in-the-field surveillance as part of their overall surveillance approaches, we agree with these commenters that establishing more explicit and more rigorous requirements will promote greater consistency and clarity regarding ONC-ACBs' responsibilities for conducting in-the-field surveillance, which will in turn improve the reliability and performance of certified health IT and help identify and address potential non-conformities.

Comments. Other commenters, mostly health IT developers, were less supportive of in-the-field surveillance. They cautioned that some factors that may affect the performance of certified health IT—such as how the health IT is configured, implemented and adopted by users and integrated with other health IT components as part of complex, local implementations—may be challenging for ONC-ACBs to evaluate or could in some cases be beyond the scope of a health IT's certification. Some commenters asserted that ONC-ACBs may lack the sophistication or expertise to distinguish certification non-conformities from other factors that may cause certified health IT to perform differently in the field than in a controlled testing environment. In

particular, current certification requirements may be tested with an established workflow (often the health IT developer's "optimal workflow") but made available to users with additional workflow and implementation options. According to these commenters, an ONC-ACB unfamiliar with a particular variation could incorrectly regard it as a non-conformity. Separately, a few commenters asserted that end-users with whom an ONC-ACB would conduct in-the-field surveillance may lack the necessary skill and knowledge to properly demonstrate certified health IT capabilities, or may be susceptible to "leading questioning" (presumably by the ONC-ACB conducting the surveillance).

Response. We appreciate the concerns raised by commenters and acknowledge that in-the-field surveillance presents unique challenges. However, we disagree with the suggestion that ONC-ACBs lack the sophistication or expertise to perform in-the-field surveillance or to do so in a reliable and objective manner.

Under the ONC Health IT Certification Program, ONC-ACBs' surveillance approaches must include the use of consistent, objective, valid, and reliable methods, subject to the ongoing supervision of the ONC-AA. (§ 170.503(e)(2)). In addition, the requirements for in-the-field surveillance established by this final rule build on those with which ONC-ACBs are already familiar, including the requirements for in-the-field surveillance that have existed since the establishment of the Permanent Certification Program in 2011.[168] Since that time, it is our experience that ONC-ACBs have become increasingly adept at analyzing the performance of certified health IT in the field, including working with developers and end-users to identify the causes of reported problems and to distinguish certification issues from other factors that may

[168] 76 FR 1282 (clarifying our expectation under the Permanent Certification Program that an "ONC-ACB would focus its surveillance activities on whether the Complete EHRs and/or EHR Modules it has certified continue to perform 'in the field' … as they did when they were certified."); see also ONC, ONC Health IT Certification Program, Program Policy Guidance #13-01.

affect the performance of certified health IT. For all of these reasons, we are confident that ONC-ACBs will be able to meet their responsibilities for conducting in-the-field surveillance.

Comments. Given the unique challenges associated with in-the-field surveillance, some commenters suggested that, in addition to observing how certified capabilities operate in a production environment, ONC-ACBs should be permitted to use other methods to inform their evaluation of technology in the field. For example, the ONC-AA stated that attempting to replicate reported problems in a controlled testing environment may provide a better basis for identifying a suspected non-conformity than relying on in-the-field observations. Separately, several commenters, including the ONC-AA, suggested that ONC-ACBs should work closely with health IT developers in analyzing complaints and other information about potential non-conformities. The commenters stated that including developers in the surveillance process would be important because ONC-ACBs may not be familiar with a developer's particular technology and implementations. Moreover, health IT developers may have internal complaint and quality management programs that could be leveraged to provide insight into problems and their causes.

Response. We appreciate these suggestions, which are consistent with the approach to in-the-field surveillance we envisioned in the Proposed Rule. We agree with commenters that the assessment of certified health IT in a production environment may require ONC-ACBs to employ a variety of methodologies and approaches. While these must include, they need not be limited to, observing the performance of certified capabilities in the field. Thus in addition to observing how capabilities function in the field, an ONC-ACB might supplement its field observations with information related to the certified technology gleaned from other sources of surveillance, such as user surveys, reviewing developers' complaint logs and defect tickets (including the developer's root cause analysis and resolution of tickets), and attempting to

replicate reported problems in a controlled environment. These and other appropriate investigative and diagnostic techniques may help ONC-ACBs more effectively target and conduct their field assessments and inform their overall assessments of certified health IT capabilities in the field.

We also agree that ONC-ACBs should, where appropriate, involve health IT developers in their surveillance activities. For example, an ONC-ACB could require a health IT developer to provide technical assistance to the ONC-ACB in understanding and analyzing variations not seen during the testing and certification process and other complexities. ONC-ACBs could also require or permit health IT developers to assist in analyzing and determining the causes of issues, provided such assistance does not compromise the ONC-ACB's independence or the requirements of its accreditation.

Comments. Several commenters requested additional clarity regarding the precise standards that would govern an ONC-ACB's assessment of certified capabilities in the field. Some commenters stated that the standards articulated in the Proposed Rule did not provide a sufficiently objective basis for determining that certified health IT, once implemented, no longer conforms to the requirements of its certification. Some commenters requested that we provide detailed guidance and bright-line rules to guide ONC-ACBs in making these determinations.

Response. While we understand the desire for bright-line rules, we do not think it practicable or a useful exercise to attempt to anticipate and prescribe detailed rules for every conceivable situation in which an ONC-ACB may discover a non-conformity during its surveillance of technology in the field. In practice, certified health IT may be integrated with a wide range of other systems, processes, and people and may be customized and used in many

different ways. These circumstances, which are inherent to the production environment, are too numerous and varied to anticipate or to reduce to simple rules of universal application.

In light of these complexities, we identified the basic principles that would guide an ONC-ACB's surveillance of certified health IT in the field. (80 FR 16877). In response to commenters' requests for additional clarity, we further elaborate on these principles below. We believe that with these additional clarifications, the principles we have identified will provide ONC-ACBs with clear and predictable guidance and ensure that in-the-field surveillance is conducted in a fair, reliable, and consistent manner across all health IT products and implementations.

Analysis and Examples of Non-Conformities in the Field

Comments. Some commenters asked us to clarify whether an ONC-ACB's evaluation of certified health IT capabilities in the field must be limited to those aspects of the health IT that were tested in a controlled environment. In this connection, a few commenters stated that certain factors—such as how certified capabilities are made available to and implemented by users in the field—are beyond the scope of certification under the ONC Health IT Certification Program and therefore cannot give rise to a "non-conformity."

Response. An ONC-ACB's assessment of certified health IT in the field is not limited to aspects of the technology that were tested in a controlled environment. Rather, an ONC-ACB must consider the unique circumstances and context in which the certified health IT is implemented and used in order to properly assess whether it continues to perform in a manner that complies with its certification.

Testing is an important part of an ONC-ACB's overall analysis of health IT under the ONC Health IT Certification Program. For practical reasons, however, testing focuses on

particular use cases and necessarily reflects assumptions about how capabilities will be implemented and used in practice. Thus while test results provide a preliminary indication that health IT meets the requirements of its certification and can support the capabilities required by the certification criteria to which the technology was certified, that determination is always subject to an ONC-ACB's ongoing surveillance, including the ONC-ACB's evaluation of certified capabilities in the field. Indeed, a fundamental purpose of in-the-field surveillance is to identify deficiencies that may be difficult to anticipate or that may not become apparent until after certified health IT is implemented and used in a production environment. That purpose would be entirely frustrated if an ONC-ACB's assessment of technology in the field were confined to those aspects of the technology's performance specifically delineated in test procedures.

Comments. Several commenters stated that, depending on the circumstances, certified health IT that has been implemented in the field may be unable to demonstrate certified capabilities for reasons that are beyond the health IT developer's control. For example, users may customize certified health IT capabilities in ways that could not be anticipated by the developer or that conflict with the developer's explicit instructions regarding the proper implementation and configuration of its technology. These and other factors beyond the control of a developer should not, according to these commenters, be grounds for a determination of non-conformity.

Response. We recognize there may be instances in which certified health IT cannot successfully demonstrate implemented capabilities for reasons that the developer cannot reasonably influence or control. We clarify that, as discussed below, these circumstances would be beyond the scope of the health IT's certification and would not give rise to a non-conformity.

A non-conformity arises when certified health IT fails to conform to the requirements of its certification under the ONC Health IT Certification Program. Those requirements take several forms and may apply to aspects of the design and performance of technology as well as the responsibilities of health IT developers. In particular, certified health IT must be able to support the capabilities and uses required by applicable certification criteria, and developers must make such capabilities available in ways that enable them to be implemented and used in production environments for their intended purposes.[169] Developers must also comply with additional program requirements as a condition of certification.[170]

While these requirements vary based on the specific certification criteria or program requirements at issue, all of them focus on the responsibilities of health IT developers and those aspects of their technology that they can reasonably influence or control. Accordingly, if an ONC-ACB finds that health IT, as implemented in the field, cannot demonstrate required capabilities in a compliant manner, the ONC-ACB must determine the reasons for the failure, including the roles of the technology as well as the health IT developer, users, and other parties. If the ONC-ACB finds that the developer or its technology were a substantial cause of the failure, the ONC-ACB would conclude that the health IT does not meet the requirements of its certification. By contrast, if the ONC-ACB finds that the failure was caused exclusively by

[169] Most certification criteria permit technology to be designed and made available to users in any way that meets the outcomes required by the criteria. Several certification criteria, however, also prescribe specific requirements for how certified capabilities are designed or made available to users. For example, the safety-enhanced design criterion (§ 170.315(g)(3)) requires developers to apply user-centered design processes to the capabilities referenced in that criterion during the design and development of certified health IT. Other certification criteria require developers to identify specific design or performance characteristics of their technology, such as the quality management system (§ 170.315(g)(4)) and accessibility-centered design standard or law (§ 170.315(g)(5)) used in the development, testing, implementation, and maintenance of the capability.

[170] In addition to the requirements established by adopted certification criteria, a Complete EHR or Health IT Module's certification is also conditioned on the health IT developer's compliance with certain program requirements that are necessary to the basic integrity and effectiveness of the ONC Health IT Certification Program. These requirements include, for example, the mandatory disclosure requirements (§170.523(k)(1)) and the requirements related to displaying the ONC Certified HIT Certification and Design Mark (§170.523(l)).

factors far removed from the control or responsibility of the developer, the ONC-ACB would regard those factors as beyond the scope of the health IT's certification and would not find a non-conformity. The following contrasting scenarios provide an example of these requirements in practice.

- Scenario A: An ONC-ACB initiates in-the-field surveillance of a Health IT Module certified to the clinical decision support certification criterion at § 170.315(a)(9). The ONC-ACB observes the use of the capability at a location at which it has been implemented. The ONC-ACB observes as a user unsuccessfully attempts to access user diagnostic or therapeutic reference information for a patient as required by the criterion. The ONC-ACB then performs a series of troubleshooting and diagnostic exercises with the provider and the developer of the certified Health IT Module. After additional fact-finding and analysis, the ONC-ACB concludes that the failure of the technology to perform as expected was caused by the failure to implement a routine update of the linked referential clinical decision support component of the Health IT Module. Under the terms of the provider's agreement with the developer, the developer was solely responsible for implementing routine updates in return for an annual maintenance fee, which the provider had paid in full.

Based on these facts, the ONC-ACB would find a non-conformity because the failure of the certified health IT to function as expected was due solely to the actions of the developer that prevented the user from accessing capabilities to which the health IT was certified.

- Scenario B: An ONC-ACB initiates in-the-field surveillance of a Health IT Module certified to the clinical decision support certification criterion § 170.315(a)(9). The ONC-ACB observes the use of the capability at a location at which it has been implemented.

The ONC-ACB observes as a user unsuccessfully attempts to view user diagnostic or therapeutic reference information for a patient as required by the criterion. Upon further evaluation, the ONC-ACB learns that the provider had notified the developer that it did not wish to purchase or sublicense the standard clinical reference information bundled with the developer's clinical decision support technology and requested instead that the developer integrate its technology with the provider's preferred third-party database of clinical reference information. The developer agreed to integrate the third-party database information as requested, but in writing advised the provider that, because the developer did not have a sublicensing agreement in place with the third-party vendor, the provider would be responsible for obtaining and maintaining the necessary licenses for access to the third-party vendor's database. The developer successfully integrated the third-party database information as requested, and the certified capabilities performed as expected using the third-party database information for several months prior to the ONC-ACB's surveillance. However, at the time of the surveillance, access to the third-party database information had been temporarily suspended because of the provider's failure to pay several outstanding invoices from the third-party vendor—the result of an oversight in the provider's accounting department. Because of the suspension in service, the technology, which was otherwise performing as certified, was unable to retrieve and display user diagnostic and therapeutic reference information.

Based on these facts, the ONC-ACB would not find a non-conformity because, while the technology was unable to perform required capabilities in the field, the failure was caused by factors far removed from the control or responsibility of the developer. Indeed, the developer took care to warn the provider that, while the technology could be customized to support third-

party database information, the provider would be responsible for maintaining any necessary licenses for access to the third party database information.

Comments. Some commenters stated that contractual restrictions or other limitations on the use of a developer's certified health IT should be treated as a non-conformity, while several other commenters asked for additional guidance on this issue.

Response. As the scenarios above illustrate, because developers sell and license certified technology in many different ways and often in conjunction with many other related products and services, an ONC-ACB's evaluation of technology in the field will necessarily require a consideration of the manner in which the developer makes its certified technology and associated capabilities available to customers and users, including a consideration of implementation options, contractual terms, and other factors that could affect the performance of the capabilities in the field. For example, an ONC-ACB would find a non-conformity were it to determine that a developer had imposed restrictions or limitations[171] on its technology (or the use of its technology) that substantially interfered with users' ability to access or use certified capabilities for any purpose within the scope of the technology's certification, as in the following scenarios.

- Scenario C: An ONC-ACB initiates in-the-field surveillance of a Health IT Module certified to the data export criterion at § 170.315(b)(6). The ONC-ACB observes the use of the capability at a location at which it has been implemented. The ONC-ACB observes as a user unsuccessfully attempts to create a set of export summaries using the required standard for patients whose information is stored in the technology. The ONC-ACB contacts the health IT developer, which explains that to utilize the data export capability, a user must load a series of coded instructions into the technology using the developer's

[171] Potential restrictions and limitations are discussed in detail in section IV.D.2 of this preamble, "Transparency and Disclosure Requirements."

proprietary scripting language. However, the developer restricts the ability of users to access training materials or instructions that would allow them to acquire the necessary knowledge and expertise to perform this function.

Based on these facts, the ONC-ACB would find a non-conformity. Specifically, the developer has restricted access to training materials and instructions that are needed to access and capability and successfully use it to achieve the technical outcomes contemplated by § 170.315(b)(6). Indeed, as the scenario illustrates, the restriction effectively prevents a user from using the data export capability at all. As such, the technology no longer conforms to the requirements of its certification.

- Scenario D: An ONC-ACB initiates in-the-field surveillance of a Health IT Module certified to the data export criterion at § 170.315(b)(6). The ONC-ACB observes the use of the capability at a location at which it has been implemented. The user is able to successfully create a set of export summaries for patients in real time but is unable to configure the technology to create a set of export summaries based on a relative time and date (e.g., the first of every month at 1:00 am). The ONC-ACB contacts the health IT developer, which explains that the ability to create export summaries based on a relative time and date is an "advanced functionality" that the developer has disabled by default. The developer will only enable the functionality if a customer specifically requests it.

Based on these facts, the ONC-ACB would find a non-conformity. Specifically, the developer has placed a technical limitation on its technology by disabling and thus preventing users from accessing functionality within the scope of the technology's certification to the data export capability. Indeed, the ability to create a set of export summaries based on a relative time

and date is expressly required by § 170.315(b)(6)(iii)(B)(2). That a customer must specifically request that the developer turn on the functionality is a substantial interference with a user's ability to access and use this aspect of the certified capability. As such, the technology no longer conforms to the requirements of its certification.

Comments. Some commenters asked whether a developer's failure to disclose known material limitations or types of costs associated with its certified health IT would give rise to a non-conformity. Several commenters assumed that it would and stated that, together with the more meaningful transparency and disclosure requirements we proposed, assessing the effect of developers' disclosures on the performance of certified health IT in the field would promote greater transparency and reliability of certified health IT capabilities and help mitigate business practices that limit or interfere with access to certified health IT capabilities.

Response. Under the expanded transparency and disclosure requirements at § 170.523(k)(1), which are discussed in section IV.D.2 of this preamble, a health IT developer must disclose all known material limitations and types of costs associated with its certified health IT. The failure to disclose this information is a violation of an explicit certification program requirement (§ 170.523(k)(1)) and thus constitutes a non-conformity. The disclosure violation may also give rise to a separate non-conformity in the event that the failure to disclose the required information has substantially impaired, or would be likely to substantially impair, the ability of one or more users (or prospective users) to implement or use the developer's certified health IT in a manner consistent with its certification.

As an example, if the developer in Scenario D above failed to disclose the technical limitation described in that scenario, the ONC-ACB would find a non-conformity to the disclosure requirements at § 170.523(k)(1). This determination would be warranted because the

developer's failure to disclose the limitation could substantially interfere with the ability of a user or prospective user to implement the data export capability in a manner consistent with the technology's certification to § 170.315(b)(6).[172]

Given the risk of non-conformity created by the failure of a developer to disclose the kinds of material information described above, and the concomitant requirement for ONC-ACBs to evaluate such disclosures in order to properly evaluate certified technology in the field, we have finalized elsewhere in this final rule our proposal to expand and clarify the types of information that developers are required to disclose as a condition of certification under the ONC Health IT Certification Program. We discuss these disclosure requirements in detail in section IV.D.2 of this preamble, "Transparency and Disclosure Requirements."

For the foregoing reasons, and with the clarifications discussed above, we have finalized as proposed the definition of in-the-field surveillance at § 170.556(a).

Reactive Surveillance

We proposed to clarify and add to ONC-ACBs' responsibilities for conducting "reactive surveillance"—that is, surveillance of certified health IT initiated on the basis of complaints or other indications that the health IT does not conform to the requirements of its certification. We proposed to create an explicit duty for an ONC-ACB to initiate such surveillance whenever it becomes aware of facts or circumstances that call into question the continued conformity of a certified Complete EHR or certified Health IT Module to the requirements of its certification (including conformity both to applicable certification criteria as well as to other requirements of certification, such as the disclosure requirements at § 170.523(k)(1)). Further, we proposed that whenever an ONC-ACB initiates reactive surveillance, it would be required, as a matter of

[172] The ONC-ACB would also find a separate non-conformity to § 170.315(b)(6), for the reasons explained in connection with Scenario D.

course, to assess the health IT developer's compliance with the disclosure requirements at § 170.523(k)(1).

Comments. Many commenters agreed with the proposed requirements for reactive surveillance. Commenters stated that strengthening surveillance, including in-the-field surveillance, based on complaints and other information about the real-world performance of capabilities would provide greater assurance to providers that they will in fact be able to implement and use the capabilities to which health IT has been certified. The ONC-AA and ONC-ACBs largely supported our proposed reactive surveillance requirements and urged us to focus primarily on refining this aspect of in-the-field surveillance and not the proposed randomized surveillance requirements.

Some commenters, mostly ONC-ACBs, sought greater clarity regarding the interaction between the proposed reactive surveillance requirements and ONC-ACBs' existing responsibilities for conducting reactive and other forms of surveillance pursuant to the requirements of their accreditation to ISO/IEC 17065 and authorization to issue certifications under the ONC Health IT Certification Program. Relatedly, several commenters noted that the proposed duty to initiate reactive surveillance would require in all cases that such surveillance take place in the field; these commenters regarded this as an overly broad requirement that could unnecessarily supplant other forms of "traditional" surveillance that, depending on the circumstances, may be more effective and less burdensome.

Response. We thank commenters for their thoughtful comments on this aspect of our proposal. In consideration of these comments and the additional comments summarized below, we are finalizing the reactive surveillance requirements at § 170.556(b), subject to the revisions discussed below. The revisions address the request from commenters for clarification of the

interaction between the proposed reactive surveillance requirements and ONC-ACBs' existing obligations to conduct reactive surveillance.

The proposed reactive surveillance requirements focused primarily on an ONC-ACB's duty to initiate surveillance of certified health IT in the field. Specifically, we stated that an ONC-ACB would be required to initiate in-the-field surveillance whenever it becomes aware of facts or circumstances that call into question health IT's continued conformity to the requirements of its certification (80 FR 16878). However, we agree with the observation of several commenters that requiring ONC-ACBs to initiate in the field surveillance in all cases would be unnecessarily prescriptive. In some cases, an ONC-ACB will be able to investigate and evaluate a putative non-conformity just as effectively by using traditional forms of surveillance that do not depend on observing certified health IT capabilities in the field. For example, an ONC-ACB may identify and substantiate non-conformities through conventional desk-audits followed by re-testing of Health IT Modules in a controlled environment. As another example, an ONC-ACB may perform an audit of a developer's complaint processes to identify potential non-compliance with the requirements of ISO/IEC 17065. Similarly, an ONC-ACB may audit a developer's website and other communications to identify potential non-compliance with the disclosure requirements (§ 170.523(k)(1)), the Criteria and Terms of Use for the ONC Certified HIT Certification and Design Mark (§ 170.523(l)), or other certification requirements.

Because our intent was to build upon—not supplant—these traditional forms of surveillance, we have revised the requirements at § 170.556(b) as follows. Under § 170.556(b), an ONC-ACB has a duty to initiate reactive surveillance—including, as necessary, in-the-field surveillance—whenever it becomes aware of facts or circumstances that would cause a reasonable person to question a certified Complete EHR or certified Health IT Module's

continued conformity to the requirements of its certification. Such conformity includes both ongoing conformity to applicable certification criteria as well as compliance with other requirements of certification, including the disclosure requirements for health IT developers at § 170.523(k)(1).

Whether reactive surveillance must include in-the-field surveillance or may employ other methods is governed by the definition and principles for in-the-field surveillance described earlier in this preamble and codified at § 170.556(a), including the nature of the suspected non-conformity and the adequacy of other forms of surveillance under the circumstances. In most cases, the need to evaluate the certified health IT in the field will be obvious from the nature of the suspected non-conformity. For example, if a problem with a certified health IT capability is reported to arise only in connection with a specific local implementation option, an ONC-ACB would likely need to observe the relevant capabilities in the field in order to fully analyze the cause of the problem and determine whether it is the result of a non-conformity. In other cases, the need for in-the-field surveillance may become apparent only after other surveillance methods and techniques have failed to isolate the cause of the problem.

In-the-field surveillance may also be necessary to determine a developer's compliance with certification program requirements, such as the mandatory disclosure requirements at § 170.523(k)(1). While non-compliance with these requirements may often be established from complaints and a review of a developer's disclosures, certain kinds of undisclosed limitations on the capabilities of certified health IT may need to be confirmed through in-the-field surveillance of the technology, or may not be discovered at all except upon observing the operation of certified capabilities in the field.

Comments. A number of commenters asked us to articulate more precise standards for when an ONC-ACB would be required to initiate reactive surveillance. Some of these commenters stated that ONC-ACBs would not be able to consistently apply the standard set forth in the Proposed Rule, which would require an ONC-ACB to initiate reactive surveillance whenever it becomes aware of facts or circumstances that would cause a reasonable person to question a certified Complete EHR or certified Health IT Module's continued conformity to the requirements of certification.

Response. As requested by commenters, we provide the following additional guidance on the circumstances that would trigger an ONC-ACB's duty to initiate reactive surveillance under the requirements at § 170.556(b).

In determining whether to initiate reactive surveillance, an ONC-ACB must consider and weigh the volume, substance, and credibility of complaints and other information received against the type and extent of the alleged non-conformity, in light of the ONC-ACB's expertise and experience with the particular capabilities, health IT, and certification requirements at issue. For example, if an ONC-ACB receives a number of anonymous complaints alleging general dissatisfaction with a particular certified Health IT Module, the ONC-ACB is not be required to initiate surveillance (though it would not be precluded from doing so). In contrast, if an ONC-ACB receives several complaints alleging, for example, that a particular certified Health IT Module is unable to electronically create a set of export summaries in accordance with the data export certification criterion at § 170.315(b)(6), the ONC-ACB must initiate surveillance of the Health IT Module unless a reasonable person in the ONC-ACB's position would doubt the credibility or accuracy of the complaints. A reasonable basis for doubt might exist if the ONC-ACB had recently responded to the very same issue and determined through in-the-field

surveillance of the Health IT Module at several different locations that the reported problem was due to a "bug" arising from an unsupported use of the Health IT Module that the developer had specifically cautioned users about in advance.

An ONC-ACB's decision to initiate reactive surveillance must also take into account complaints and other information indicating whether a health IT developer has disclosed all known material information about certified capabilities, as required by § 170.523(k)(1). The failure to disclose this information calls into question the continued conformity of those capabilities because it creates a substantial risk that existing and prospective users will encounter problems implementing the capabilities in a manner consistent with the applicable certification criteria. Thus in the example above, if the complaints received by the ONC-ACB suggested that the developer knew about but failed to disclose the data export issue to users, the ONC-ACB would be required to initiate in-the-field surveillance of the certified Health IT Module to verify whether the developer had failed to disclose known material information and, if so, whether the failure to disclose that information prevented users from reasonably implementing and using the data export capability in accordance with the requirements of the certification criterion at § 170.315(b)(6).

We believe the foregoing principles and examples will provide sufficient clarity and practical guidance for ONC-ACBs regarding their responsibilities for conducting reactive surveillance pursuant to § 170.556(b). If necessary, we will issue additional guidance to ONC-ACBs to assist them in conducting such surveillance in a consistent, objective, and reliable manner.

Comments. A commenter suggested that reactive surveillance should be based solely on complaints submitted directly to ONC-ACBs. The commenter stated that ONC-ACBs "can't be

expected to keep ears to the ground" to monitor the trade press, user group message boards, blogs, analyst reports, and other sources of information, which may not be credible. Another commenter asked us to clarify that in determining whether to initiate reactive surveillance, ONC-ACBs would be required to consider complaints from persons other than providers and users of certified health IT (such as public health agencies and other recipients of electronic health information that may not themselves use certified health IT).

Response. Under the requirements adopted in this final rule, an ONC-ACB has a duty to initiate reactive surveillance whenever it becomes aware of facts or circumstances that call into question the continued conformity of health IT to which it has issued a certification. We do not prescribe new requirements for ONC-ACBs to proactively monitor any particular source of information (such as the trade press or user forums), as ONC-ACBs are already required obtain and synthesize information about certified health IT from multiple sources.

Regardless of the form of the information or how it comes to an ONC-ACB's attention, if the information suggests that health IT the ONC-ACB has certified may no longer conform to the requirements of its certification, the ONC-ACB is required to initiate surveillance. For example, an ONC-ACB may become aware of a potential non-conformity through user surveys and other "behind-the-scenes" surveillance of users and products. Or an ONC-ACB may become aware of a potential non-conformity while auditing a developer's website and other disclosures. ONC will also share information with ONC-ACBs, which may well come from the trade press and other sources. And, of course, an ONC-ACB will receive complaints from a variety of sources, including, as one commenter suggested, entities such as public health agencies that may not be certified health IT users. All of this information would compose the facts and

circumstances of which an ONC-ACB is aware and is required to consider in determining whether to initiate surveillance.

Randomized Surveillance

In addition to reactive surveillance, we proposed to require ONC-ACBs to initiate in-the-field surveillance on a "randomized" basis for the certification criteria prioritized by the National Coordinator. For those prioritized certification criteria, an ONC-ACB would be required each calendar year to randomly select at least 10% of the Complete EHRs and Health IT Modules to which it has issued a certification. The ONC-ACB would then be required to initiate in-the-field surveillance of each such certified Complete EHR or certified Health IT Module at the lesser of 10 or 5% of locations at which the technology is implemented and in use in the field. The locations would be selected at random, subject to certain sampling considerations and limited exclusions described in the Proposed Rule.

We stated that randomized surveillance would enable ONC-ACBs to identify non-conformities that are difficult to detect through complaint-based or other reactive forms of surveillance. Randomized surveillance would also enable an ONC-ACB to detect patterns of non-conformities that indicate a more widespread or recurring problem requiring a comprehensive corrective action plan. We proposed that a pattern of non-conformity would exist if an ONC-ACB found that a certified Complete EHR or certified Health IT Module failed to demonstrate conformity to any prioritized certification criterion at 20% or more of the locations surveilled. Upon such a finding, the ONC-ACB would deem the certified Complete EHR or certified Health IT Module "deficient" and impose a corrective action plan on the developer of the certified Complete EHR or certified Health IT Module. We specified certain elements and procedures that would be required for such corrective action plans.

Comments. We received strong support for our proposal to require ONC-ACBs to perform "randomized" surveillance as part of their in-the-field surveillance approach. Several commenters who supported our proposal urged us to minimize the associated disruption and other burdens for providers who participate in randomized surveillance.

A number of commenters—including the ONC-AA and the ONC-ACBs—raised concerns regarding this aspect of our proposal. The ONC-ACBs estimated that performing randomized surveillance on 10% of certified products, even at the relatively small number of locations specified in the Proposed Rule, would as much as double the total cost of certification and divert an inordinate amount of time and resources away from other important certification and surveillance activities. Meanwhile, commenters including the ONC-AA doubted that the proposed sample size would be sufficient to detect patterns of non-conformities or to determine with any degree of confidence how widespread a particular non-conformity may be. In this connection, commenters pointed out that surveilling a randomly selected certified Complete EHR or certified Health IT Module at the lesser of 10 or 5% of locations at which the technology is installed may not yield a statistically significant result. For example, if an ONC-ACB were to randomly select a Health IT Module installed at 40 locations, the ONC-ACB would only be required to perform in-the-field surveillance at 2 locations. The ONC-AA stated that performing surveillance of certain certified capabilities, such as interoperability or privacy and security, at only 2 locations would be insufficient to identify all but the grossest non-conformities.

Some commenters felt that it was premature to codify a specific approach to randomized surveillance and that we should instead create a "pilot study" or allow ONC-ACBs to continue to experiment with approaches to randomized surveillance in order to gauge the willingness of

providers to participate, potential methodologies, and the costs and benefits of this type of surveillance.

Response. Randomized surveillance is an important aspect of an ONC-ACB's overall approach to in-the-field surveillance. In addition to exposing problems that may not surface through complaints and other forms of surveillance, randomized surveillance will encourage developers to proactively address issues and will also encourage providers to participate in and become familiar with in-the-field surveillance of certified health IT. However, we acknowledge that the proposed randomized surveillance requirements could place a significant burden on ONC-ACBs and divert resources and energy away from other equally important aspects of our proposal, including more rigorous in-the-field surveillance of certified health IT based on complaints and other evidence of potential non-conformities. Balancing these considerations, we are persuaded that starting with a less ambitious approach to randomized surveillance will allow us to refine this aspect of surveillance over time and will provide the best path to achieving our overall goal of strengthening in-the-field surveillance and making it more meaningful.

Accordingly, we have revised the proposed randomized surveillance requirements as follows. First, we have reduced the annual sample size for randomized surveillance. Instead of 10% of all certified Complete EHRs and certified Health IT Modules, an ONC-ACB must perform randomized surveillance on 2% of certified Complete EHRs or certified Health IT Modules each year. Based on current data on the CHPL, we estimate this could require ONC-ACBs to perform randomized surveillance of up to 24 products per calendar year (depending on the total number of products the ONC-ACB has certified, which we expect will increase with the addition of Health IT Modules certified to the 2015 Edition). We believe this new minimum threshold will provide additional insight and experience related to randomized surveillance. This

specific baseline will establish a randomized surveillance program that advances our policy aims while reducing the burden of randomized surveillance for all stakeholders and making this initial approach more manageable for ONC-ACBs. That being said, we intend to continually review surveillance results and experiences to determine whether and how to increase this threshold over time (e.g., whether an incrementally rising threshold over time would be appropriate and effective). We also intend to pursue and investigate other avenues that could add feedback to (and be combined with) this surveillance process. For example, we will explore other kinds of tools, such as those that may be able to be used directly by health care providers to test and report how their products performed. Overall, and over the long-term, we believe that other approaches can and should be included to complement the randomized in-the-field surveillance performed by ONC-ACBs.

Second, while an ONC-ACB must perform surveillance of randomly selected certified Complete EHRs and certified Health IT Modules in the field, we no longer specify a minimum number of locations at which the ONC-ACB will be required to conduct such surveillance. This revision reflects commenters' insight that requiring an ONC-ACB to surveil the technology at the lesser of 5% or 10 locations, as we had proposed, could be simultaneously both burdensome and yet unlikely to yield statistically significant or generalizable results. It also reflects our recognition, underscored by the comments, that well-established methodologies and standards for post-market surveillance used in other industries typically focus on conformity testing of discrete products or components in isolation and thus provide little guidance for formulating appropriate sampling and statistical methods under the ONC Health IT Certification Program. Given the lack of suitable reference models in other industries, we agree with commenters that this particular aspect of an ONC-ACB's randomized surveillance approach would benefit from

additional experience and piloting. Thus we intend to work with ONC-ACBs and the ONC-AA and issue guidance as necessary to refine these aspects and ensure the use of consistent and reliable methods across ONC-ACBs and their surveillance approaches.

Finally, we have eliminated the concept of "deficient surveillance results" and instead applied the proposed corrective action plan requirements across-the-board to all types of surveillance and confirmed non-conformities. Thus, if an ONC-ACB performs randomized surveillance for a certified Complete EHR or certified Health IT Module and confirms a non-conformity, it must institute a corrective action plan under § 170.556(d) and report related information to the open data CHPL, as required by § 170.556(e)(3). This requirement applies regardless of whether the non-conformity meets the 20% "deficiency threshold" described in the Proposed Rule. These changes are described in more detail below in our responses to the comments on these aspects of our proposal.

We have finalized these revisions at § 170.556(c)–(e).

Comments. A number of commenters suggested that we specify additional details regarding the random sampling approach that ONC-ACBs must follow when selecting certified Complete EHRs and certified Health IT Modules for randomized surveillance and, separately, when selecting the locations at which the technology will be surveilled in the field. Commenters noted that under a purely random sampling approach, an ONC-ACB would be equally likely to select a Complete EHR or Health IT Module with relatively few installations or users as one with many installations or users. To maximize the value of randomized surveillance for providers and other stakeholders, commenters suggested that we require ONC-ACBs to weigh the selection of products based on the number of installed locations, users, or other factors.

Commenters also suggested we clarify or specify additional requirements related to the number and types of locations at which an ONC-ACB must surveil certified Complete EHRs and certified Health IT Modules that it has randomly selected for in-the-field surveillance. One commenter stressed the importance of ensuring random selection of and diversity in the providers and locations selected for surveillance. Another commenter suggested that an ONC-ACB's approach to selecting locations would need to vary depending on the type of implementation (e.g., local versus hosted systems).

Response. We thank commenters for their feedback on potential random sampling and other considerations for randomized surveillance. While we do not explicitly adopt any additional sampling or methodological constraints beyond those we proposed, we agree with many of the commenters' suggestions and intend to work with ONC-ACBs and the ONC-AA to incorporate these and other elements in their approaches to randomized surveillance, consistent with the basic parameters established by this final rule and discussed in more detail below.

In consideration of the comments provided, we have determined that an ONC-ACB's selection process under randomized surveillance will adhere to the following requirements. On an annual basis the ONC-ACB must ensure that it meets the threshold sample size, which is initially being established at 2% of all of the Complete EHRs and Health IT Modules to which the ONC-ACB has issued a certification. The ONC-ACB must randomly select products from those to which it has issued a certification, but is permitted to implement appropriate weighting and sampling considerations. After an ONC-ACB has randomly selected a product for surveillance, for each product selected, the ONC-ACB must select a random sample of one or more locations at which the ONC-ACB will initiate in-the-field surveillance of the certified Complete EHR or certified Health IT Module's prioritized capabilities. At both stages of the

selection process, an ONC-ACB must ensure that every product selected and every provider location at which the product is in use has a chance of being randomly selected for in-the-field surveillance (unless a product is excluded from selection because it was already selected for randomized surveillance within the last 12 months). This prospect, that any product and location may be selected at random, is the essence of a "random sampling" approach and is a central feature of randomized surveillance because it ensures that all health IT developers' products and implementations are potential candidates for in-the-field surveillance. The possibility that any product may be surveilled at any provider location will encourage developers to proactively address issues and improve the real-world performance and reliability of health IT capabilities across all customers.

Consistent with these principles, we clarify that an ONC-ACB's selection of products and locations need not be random in the absolute sense of assigning an equal probability of selection to every product or location in the pool. Indeed, for the reasons stated by commenters, there may be strong justifications for assigning different probabilities or "weights" to products or locations based on a variety of factors that are relevant to maximizing the value and impact of randomized surveillance activities for providers and other stakeholders. For example, when selecting products for randomized surveillance, the ONC-ACB could assign greater weight to products that are more widely adopted and used so as to increase the likelihood that the products surveilled will include at least some products with a large number of installations and users. This would increase the overall impact of the ONC-ACB's surveillance activities by increasing the likelihood of discovering and addressing non-conformities that affect a large number of providers and users. As another example, when randomly selecting locations at which to perform in-the-field surveillance for any particular product, an ONC-ACB might ensure that no two

locations selected are under the common ownership or control of a single person or entity, thereby addressing the concerns raised by commenters regarding the diversity of providers and locations selected for randomized surveillance.

To avoid any misinterpretation of the phrases "randomly select" and "selected at random," we have clarified the regulation text at § 170.556(c)(2) and § 170.556(c)(4)(ii) to allow for appropriate weighting and sampling considerations in the random selection of products and locations, respectively.

Finally, we note that under the ONC Health IT Certification Program, it is an ongoing responsibility of the ONC-AA to ensure that the surveillance approaches used by ONC-ACBs, including the selection processes and methodologies for randomized surveillance discussed above, include the use of consistent, objective, valid, and reliable methods. (§ 170.503(e)(2)). We intend to work closely with the ONC-AA and the ONC-ACBs to ensure that such methods are in place and to identify and incorporate appropriate best practices and elements that serve the policies of this final rule.

Comments. Commenters pointed out that while ONC-ACBs may be able to randomly select locations at which to conduct in-the-field surveillance, they cannot compel a provider to grant access to its health care facility or to cooperate in the surveillance of its certified health IT. At the same time, providers may be reluctant to allow ONC-ACBs to perform in-the-field surveillance because of concerns about granting access to PHI. One ONC-ACB stated that it had experienced difficulties securing cooperation from providers in connection with its existing surveillance activities and therefore questioned whether providers would be willing to participate in additional surveillance, especially when conducted at random rather than in response to a complaint or identified issue.

Given these concerns, some commenters suggested that ONC-ACBs should not be required to conduct randomized surveillance unless providers are also required to participate in such surveillance as a condition of participation in the EHR Incentive Programs or other programs. Alternatively, other commenters suggested that we provide exceptions and other flexibility for ONC-ACBs in the event that a provider is selected for but does not cooperate with an ONC-ACB's in-the-field surveillance of the provider's certified health IT. Several commenters requested clarity on our expectations for providers' role as participants in in-the-field surveillance, especially randomized surveillance.

Response. We appreciate commenters' concerns and acknowledge that randomized surveillance presents unique challenges. In particular, we recognize that some providers who are selected for randomized surveillance may not cooperate with an ONC-ACB's efforts. Moreover, depending on the number of locations at which a particular product is in use, a lack of cooperation from providers or end-users could prevent the ONC-ACB from conducting in-the-field surveillance of that product altogether.

Because we agree that an ONC-ACB should not be penalized in such situations, we clarify that where an ONC-ACB makes a good faith effort but is nevertheless unable to complete in-the-field surveillance at a particular location for reasons beyond its control, the ONC-ACB may exclude the location and substitute another location that meets the random selection requirements described above. Similarly, in the event that the ONC-ACB exhausts all available locations for a particular certified Complete EHR or certified Health IT Module, the ONC-ACB may exclude that Complete EHR or Health IT Module and substitute another randomly selected Complete EHR or Health IT Module. In the case of exhaustion, we clarify that the excluded certified Complete EHR or Health IT Module would be counted towards the minimum number

of products an ONC-ACB is required to randomly surveil during the calendar year surveillance period. We emphasize, however, that an ONC-ACB must carefully and accurately document its efforts to complete in-the-field surveillance for each product and at each location. The ONC-AA would be expected to review this documentation to ensure that ONC-ACBs have met the required random selection requirement and have made a good faith effort to perform in-the-field surveillance prior to excluding any product or location from randomized surveillance. We believe that these revisions—combined with the reduced minimum sample size for in-the-field surveillance and the clarifications noted above regarding the number of locations at which an ONC-ACB must observe capabilities in the field—will mitigate the concerns raised by commenters and make randomized surveillance more manageable for ONC-ACBs, providers, and developers.

It is our expectation that providers will cooperate with an ONC-ACB's authorized surveillance activities, including the surveillance of certified health IT in the field. While we understand that some providers may be reluctant to grant ONC-ACBs access to PHI, we point out that providers who commented on our proposal overwhelmingly supported and urged us to finalize requirements for the surveillance of certified health IT in the field (i.e., in production environments in which the technology is implemented and used). Such surveillance will only be successful if providers are actively engaged and cooperate with ONC-ACBs' surveillance activities, including by granting access to and assisting ONC-ACBs to observe the performance of production systems. We also note that, in consultation with the Office for Civil Rights, we have clarified that under the "health oversight agency" exception of the HIPAA Privacy Rule, a healthcare provider is permitted to disclose PHI to an ONC-ACB during the course of authorized

in-the-field surveillance activities, without patient authorization and without a business associate agreement.[173]

Comment. One commenter, an ONC-ACB, stated that some health IT developers have resisted providing the ONC-ACB with a complete list of the health IT developers' users. The commenter asked us to clarify that health IT developers have an obligation to abide by and support an ONC-ACB's surveillance requirements, including furnishing complete and up-to-date user lists upon request.

Response. We expect an ONC-ACB to require, as a condition of certification, that health IT developers furnish to the ONC-ACB upon request, accurate and complete customer lists, user lists, and other information that the ONC-ACB determines is necessary to enable it to carry out its surveillance responsibilities. We note that even under ONC-ACB's existing annual surveillance plans, access to accurate customer and user lists is essential to an ONC-ACB's ability to contact users for reactive surveillance and to conduct surveys and other activities necessary to obtain and synthesize information about the performance of certified health IT. Therefore, if a health IT developer refuses to provide this information to an ONC-ACB, the ONC-ACB may regard the refusal as a refusal to participate in surveillance under the ONC Health IT Certification Program and institute appropriate procedures, consistent with the ONC-ACB's accreditation to ISO 17065, to suspend or terminate the health IT developer's certification.

Corrective Action Requirements; Reporting of Surveillance Results and Corrective Action Information

[173] See ONC Regulation FAQ #45 [12-13-045-1], available at http://www.healthit.gov/policy-researchers-implementers/45-question-12-13-045.

In the Proposed Rule, we stated that if an ONC-ACB found a pattern of nonconformity—defined as a failure to demonstrate conformity to any prioritized certification criterion at 20% or more of the locations surveilled—the ONC-ACB would be required to treat the certified Complete EHR or certified Health IT Module as "deficient." This finding would also trigger special requirements for corrective action plans and the reporting of that information to the open data CHPL. Specifically, the ONC-ACB would have to contact the developer of the certified Complete EHR or certified Health IT Module and require the developer to submit a proposed corrective action plan to the ONC-ACB within 30 days of the date that the developer was notified by the ONC-ACB of the "deficient" finding. The ONC-ACB would be responsible for prescribing the form and content of corrective action plans and for developing specific procedures for submission and approval, with guidance from ONC to promote consistency across ONC-ACBs.

Comments. Many commenters supported our proposal to specify certain required elements and procedures for corrective action. Several commenters asked us to clarify whether these requirements would apply to non-conformities confirmed through reactive and other forms of surveillance and, if not, what if any corrective action would be required for those non-conformities. Several commenters urged us to apply the same standards for corrective action to all types of surveillance and non-conformities. Commenters pointed out that the reasons for imposing such requirements apply with equal force to all confirmed non-conformities, not only those identified through randomized surveillance and meeting the proposed 20% threshold. In particular, requiring corrective action plans and related public reporting for only some non-conformities and not others would be difficult to square with our stated goals of improving transparency and accountability for health IT developers and ONC-ACBs. Commenters also

questioned whether the proposed approach would best achieve our patient safety goals. When an ONC-ACB confirms a non-conformity in the context of reactive surveillance, it may not know whether the problem is widespread unless and until it conducts more extensive randomized surveillance of a large sample of the potentially affected certified Complete EHR or certified Health IT Module. For reasons described earlier, ONC-ACBs may have difficulty at this time conducting randomized surveillance on the necessary scale. Applying the corrective action plan and related reporting requirements to all types of surveillance and confirmed non-conformities would alert users to these potential concerns.

Response. Our goal for these requirements was to ensure that health IT users, implementers, and purchasers would be alerted to potential non-conformities in a timely and effective manner, consistent with the patient safety, program integrity, and transparency objectives described in the Proposed Rule. But as the comments make clear, the proposed requirements would only partially serve those goals. As commenters pointed out, there is no principled reason to apply the proposed corrective action plan exclusively to non-conformities identified in the context of the proposed randomized surveillance approach. Moreover, the comments suggest that prescribing different corrective action plan requirements in this context than for other types of non-conformities (which would be governed by an ONC-ACB's general responsibility to require corrective action per its accreditation to ISO 17065) would likely create significant and unnecessary confusion.

Particularly in light of the reduced emphasis on randomized surveillance in comparison to the Proposed Rule, we are persuaded that our policy objectives will be better served by requiring the same approach to corrective action across the board. Thus we have finalized the proposed requirements for corrective action plans for all certified Complete EHRs and certified Health IT

Modules for which an ONC-ACB confirms a non-conformity, whether that non-conformity is confirmed through randomized, reactive, or any other form of surveillance under the ONC Health IT Certification Program.

For similar reasons, we have finalized the proposed reporting requirements for corrective action plans and extended these requirements to all cases in which an ONC-ACB confirms a non-conformity and subsequently approves a corrective action plan. Requiring the uniform submission of this information will promote transparency and alert health IT users, implementers, and purchasers to potential conformity issues in a more timely and effective manner. These reporting requirements are discussed further below in our response to the comments on this aspect of our proposal and also in our discussion of the "Open Data CHPL" requirements found elsewhere in this preamble.

Comment. A commenter suggested that in addition to making information about corrective action plans available on the CHPL, we should require health IT developers to notify affected users of the corrective action, similar to the requirements for breach notification under the HIPAA Rules. The commenter stated that many providers do not regularly check the CHPL and therefore may not be made aware of problems in a timely manner.

Response. We appreciate the commenter's suggestion that health IT developers who are subjected to a corrective action plan should be required to notify affected and potentially affected users of identified non-conformities and deficiencies. We already proposed to require developers to describe in their corrective action plans both an assessment of how widespread an identified non-conformity might be and how the developer planned to address the non-conformity both at the specific locations at which surveillance occurred and more generally at other potentially affected locations (80 FR 16879). Requiring developers to describe how they will notify affected

and potentially affected users of the extent of the problem and their plans to address it is a natural extension of these requirements and will help alert stakeholders to potential non-conformities in a timely and effective manner, which was one of the stated purposes of these requirements (80 FR 16884).

Accordingly, we have added as a requirement of all corrective action plans approved by an ONC-ACB that the developer identify a process for ensuring that all affected and potentially affected customers and users are alerted to identified non-conformities and deficiencies, as applicable. This process must describe in detail: how the developer will assess the scope and impact of the problem, including identifying all potentially affected customers; how the developer will promptly ensure that all potentially affected customers are notified of the problem and plan for resolution; how and when the developer will resolve issues for individual affected customers; and how the developer will ensure that all issues are in fact resolved.

To ensure adherence to these requirements for notification and resolution across a developer's customer base, and to the other requirements of the approved corrective action plan, we have added as an additional requirement of all corrective action plans approved by an ONC-ACB that the developer attest to having completed all required elements of the plan, including the requirements for alerting customers and users described above.

Comments. Many commenters supported our proposals to improve the reporting and submission of surveillance results. Several commenters stated that requiring ONC-ACBs to submit corrective action plan information to the publicly accessible open data CHPL would provide customers and users with valuable information about the performance of certified health IT while significantly enhancing transparency and accountability for health IT developers and ONC-ACBs.

Some commenters, including several health IT developers, objected to the reporting of corrective action plan information to the publicly accessible Open Data CHPL. Some commenters felt that information about non-conformities should not be made public unless and until the developer of the certified Complete EHR or certified Health IT Module at issue has been given a full and fair opportunity to contest the ONC-ACB's determination, including whether the developer was responsible or "at fault" for the non-conformity. Other commenters stated that such information should never be made public because it is bound to lack important context, could be misinterpreted, or would not offer substantial value to health IT customers and users. Separately, some commenters raised concerns regarding the reporting of proprietary or competitively sensitive information.

A few commenters suggested that to reduce reporting burden or improve the efficacy of the open data CHPL, we limit the types of information about corrective action that an ONC-ACB would be required to submit. One commenter suggested that the reporting of corrective action plan information be limited to 2015 Edition certified health IT and that reporting of surveillance results be limited to twice a year instead of quarterly. The commenter stated that these changes would reduce burden and enable us to assess the costs of these reporting requirements.

Response. We agree with commenters that requiring ONC-ACBs to report surveillance results to the National Coordinator on a quarterly basis will significantly improve our ability to respond to problems and provide timely and accurate information stakeholders.

With regard to the reporting of corrective action plan information to the open data CHPL, we understand the concerns raised by some commenters but believe that it is both necessary and appropriate to require ONC-ACBs to submit this information. The public safety, transparency, and program integrity rationales for requiring timely and public reporting of this information are

compelling. In comparison, and contrary to the assertions of some commenters, making this information available is not likely to cause customers and users to draw inaccurate or unfair conclusions about a health IT developer or its certified technology. By definition, this information will only be required when an ONC-ACB has confirmed a non-conformity and required a health IT developer to take corrective action. Thus the ONC-ACB will have completed its review of the relevant facts and circumstances, including those raised by the developer in the course of the surveillance of its certified Complete EHR or certified Health IT Module. ONC-ACBs are required to make such determinations in accordance with their accreditation to ISO 17065 and with the Principles of Proper Conduct for ONC-ACBs, subject to ongoing supervision by the ONC-AA. Moreover, as stated in the Proposed Rule, when the developer has provided an explanation of the deficiencies identified by the ONC-ACB as the basis for its determination, the ONC-ACB must include the developer's explanation in its submission to the open data CHPL. Thus developers will be able to note any objections and provide any additional context or information that may be relevant to interpreting the results of the surveillance and the ONC-ACB's findings and conclusions.

We are confident that the concerns of some commenters regarding disclosure of proprietary or sensitive information will be adequately addressed through appropriate safeguards implemented at the discretion of ONC-ACBs. ONC-ACBs should not submit to the open data CHPL any information that is in fact legally privileged or protected from disclosure. ONC-ACBs may also implement other appropriate safeguards, as necessary, to protect information they believe should not be reported to a publicly available website. However, we caution ONC-ACBs to ensure that such safeguards are narrowly tailored and consistent with our goal of promoting the greatest possible degree of transparency with respect to certified health IT and the business

practices of certified health IT developers. ONC-ACBs are required to accurately report the results of their surveillance and to explain in detail the facts and circumstances on which their conclusions are based. Similarly, health IT developers are required to cooperate with these efforts and may not prevent or seek to discourage an ONC-ACB from reporting the results of its authorized surveillance activities. We note that while the ONC Health IT Certification Program is a voluntary one, developers who choose to participate agree to comply with certification program requirements, including reporting requirements designed to ensure transparency and accountability for all participants and stakeholders.

We decline to limit the requirements for more frequent reporting of surveillance results to the National Coordinator and the submission of corrective action plan information to the open data CHPL to 2015 Edition certified health IT. The public safety, transparency, and program integrity reasons for requiring the reporting of this information apply to all, and not only 2015 Edition, certified health IT. However, we do agree that the reporting of corrective action information should be limited to the types of information that will be useful to customers and users, consistent with the goals of reporting this information to the open data CHPL explained above. We have therefore revised § 170.523(f)(1)(xxii) and (f)(2)(xi) to limit reporting to the following subset of information:

- The specific certification requirements to which the technology failed to conform, as determined by the ONC-ACB;
- A summary of the deficiency or deficiencies identified by the ONC-ACB as the basis for its determination of non-conformity;
- When available, the health IT developer's explanation of the deficiency or deficiencies;
- The dates surveillance was initiated and completed;

- The results of randomized surveillance, including pass rate for each criterion in instances where the Health IT Module is evaluated at more than one location;
- The number of sites that were used in randomized surveillance;
- The date of the ONC-ACB's determination of non-conformity;
- The date on which the ONC-ACB approved a corrective action plan;
- The date corrective action began (effective date of approved corrective action plan);
- The date by which corrective action must be completed (as specified by the approved corrective action plan);
- The date corrective action was completed; and
- A description of the resolution of the non-conformity or non-conformities.

Comments. We proposed that an ONC-ACB would have to require a health IT developer to submit a proposed corrective action plan within 30 days of being notified of an ONC-ACB's non-conformity determination and to complete an approved corrective action plan within 6 months of such notice. One commenter stated that this timeline was much too long and that developers should not be able to market health IT as certified for 6 months while they correct a non-conformity. Another commenter stated that the 30 day timeline was too short because it would not allow sufficient time for the developer to understand and investigate the issues and respond to the ONC-ACB's preliminary findings.

Response. We agree with the commenter that a developer should be able to complete an approved corrective action plan within a substantially shorter timeframe than we proposed.

We clarify that the 30 day period for submitting a proposed corrective action plan would begin to run only after an ONC-ACB has issued a non-conformity determination. In our experience, ONC-ACBs already work with health IT developers and users to investigate

potential non-conformities prior to issuing a final determination. Because this back-and-forth will have occurred prior to the ONC-ACB's non-conformity determination, we believe that a developer should be able to submit a proposed corrective action plan within 30 days of being notified of the ONC-ACB's non-conformity determination under § 170.556(d)(1). Similarly, if after 90 days of notifying the developer of a non-conformity under § 170.556(d)(1), the ONC-ACB cannot approve a corrective action plan because the developer has not submitted a revised proposed corrective action plan in accordance with §170.556(d)(4), the ONC-ACB must initiate suspension procedures. Finally, an ONC-ACB must initiate suspension procedures when it has approved a corrective action plan but the developer fails to comply with all of the requirements of the plan within the time specified therein. We have revised § 170.556(d)–(e) to reflect these requirements.

Effective Date and Applicability of Requirements

At the time of this Proposed Rule, ONC-ACBs had submitted their annual surveillance plans for calendar year 2015, which include their existing approaches and methodologies for randomized surveillance. To minimize disruption to ONC-ACBs' current surveillance activities, we proposed to make the requirements for randomized surveillance effective beginning on January 1, 2016. We said this would provide time for ONC-ACBs to implement these requirements in their annual surveillance plans and incorporate additional guidance and clarification from ONC and the ONC-AA as necessary. All other proposed surveillance requirements would be effective immediately. We requested comment on whether this timeline and plan for implementation was appropriate and on ways to minimize disruption and ensure that the requirements and purpose of this proposal are timely and effectively achieved.

Comments. Some commenters, including the ONC-AA and an ONC-ACB, suggested that we specify a single January 1, 2016 effective date for all proposed surveillance requirements in order to allow ONC-ACBs to effectively and consistently implement these requirements in their annual surveillance plans for the calendar year 2016 surveillance period. Another commenter, also an ONC-ACB, stated that it would have difficulty implementing the randomized surveillance requirements for calendar year 2016 and suggested that the requirements be postponed until January 1, 2017. Yet another commenter felt that the timeline for implementing the proposed requirements should be more aggressive.

One ONC-ACB suggested that the proposed requirements for in-the-field surveillance be applied only to 2015 Edition certified health IT so that ONC-ACBs could implement the requirements prospectively in new contracts with health IT developers.

Response. We believe that the proposed timeline for implementation is reasonable. Given the significantly reduced scope of randomized surveillance in comparison the Proposed Rule, we are confident that ONC-ACBs will be able to complete randomized surveillance requirements over the course of the calendar year 2016 surveillance period. We also believe that ONC-ACBs will be able to implement the other requirements established by this final rule during the 90 days between its publication and effective date. Accordingly, ONC-ACBs must comply with all new requirements by the effective date of this final rule. We will provide guidance to ONC-ACBs regarding updates to their annual surveillance plans for calendar year 2016 and, as necessary, regarding other aspects of surveillance affected by this final rule.[174]

[174] In our annual surveillance guidance to ONC-ACBs for the calendar year 2016 surveillance period, we stated that ONC-ACBs should be aware of the proposals in the 2015 Edition proposed rule that could affect their surveillance responsibilities and indicated that we would update our surveillance guidance as necessary in the event that such proposals were finalized. ONC, ONC Health IT Certification Program, Program Policy Guidance #15-01 (July 16, 2015), http://healthit.gov/sites/default/files/policy/onc-acb_cy16annual_surveillance_guidance.pdf.

We decline to adopt the commenter's suggestion to limit the requirements for in-the-field surveillance and maintenance of certification to only 2015 Edition certified health IT. The need to assure that certified health IT conforms to the requirements of its certification is applicable to all health IT certified under the ONC Health IT Certification Program, not just technology certified to the new 2015 Edition. Thus, as proposed, we have finalized the in-the-field surveillance and maintenance of certification requirements for all Health IT Modules certified to either the 2015 Edition or the 2014 Edition. With respect to Complete EHRs, because we have discontinued Complete EHR certification with the 2015 Edition, we have finalized these requirements for all Complete EHRs certified to the 2014 Edition. We note that Complete EHR certification to the 2014 Edition has and will continue to occur as providers may use health IT certified to the 2014 Edition to meet the CEHRT definition at least through 2017 based on the EHR Incentive Programs Stage 3 and Modifications final rule published elsewhere in this issue of the **Federal Register**.

2. Transparency and Disclosure Requirements

We proposed to revise the Principles of Proper Conduct for ONC-ACBs to require greater and more effective disclosure by health IT developers of certain types of limitations and additional types of costs that could interfere with the ability to implement or use health IT in a manner consistent with its certification. We stated that these additional disclosure requirements were necessary to ensure that existing and potential customers, implementers, and users of certified health IT are fully informed about these implementation considerations that accompany capabilities certified under the ONC Health IT Certification Program.

Our proposal expanded on health IT developers' existing disclosure obligations at §170.523(k)(1). Those obligations were adopted in the 2014 Edition final rule to promote greater

price transparency in certified health IT capabilities required to meet meaningful use objectives and measures; to mitigate confusion in the marketplace; and to reduce the risk that EPs, eligible hospitals, and CAHs would encounter unexpected difficulties in the implementation or use of certified health IT.

As we explained in the Proposed Rule, despite our initial efforts to promote greater transparency and disclosure of information by health IT developers, many providers continue to lack reliable up-front information about health IT products and services. We described reports from providers who have encountered unexpected costs and limitations in connection with their certified health IT that were not disclosed or contemplated when the technology was initially purchased or licensed. (80 FR 16880–81). We said that the failure of developers to disclose "known material information" about limitations or additional types of costs associated with the capabilities of certified health IT diminishes both the reliability of certified health IT and of certifications issued under the ONC Health IT Certification Program. In particular, the failure of developers to disclose such information creates a substantial risk that existing or prospective users of certified health IT will encounter problems implementing and using the health IT in a manner consistent with its certification. Moreover, inadequate or incomplete information about health IT products and services distorts the marketplace by preventing customers from accurately assessing the costs and capabilities of different technologies and selecting the most appropriate solutions to their needs, which increases the likelihood of downstream implementation problems and, ultimately, reduced opportunities to use health IT to improve health and health care. Finally, customers who purchase or license inappropriate or suboptimal technologies may find it difficult to switch to superior alternatives due to the often significant financial and other "switching

costs" associated with health IT.[175] When providers become "locked in" to technologies or solutions that do not meet their needs or the needs of their patients, health IT developers have fewer incentives to innovate and compete on those aspects of health IT that providers and their patients most value and need.

For all of these reasons, we proposed to revise and strengthen our existing transparency and disclosure requirements in three key respects.

First, under our proposal, a health IT developer's obligation to disclose "additional types of costs" would no longer be confined to the use of capabilities to demonstrate a meaningful use objective or measure under the EHR Incentive Programs. Instead, ONC-ACBs would be required to ensure that developers disclose any additional types of costs that a user may incur in order to implement or use capabilities of certified health IT, whether to demonstrate meaningful use objectives or measures or for any other purpose within the scope of the health IT's certification.

Second, in addition to "additional types of costs," we proposed that health IT developers would be required to disclose other factors that may similarly interfere with a user's ability to successfully implement certified health IT, including information about certain "limitations" associated with its certified health IT. We explained that the failure to disclose information about limitations—including contractual, technical, and other restrictions or policies—associated with certified health IT creates a substantial risk that current or prospective users will encounter problems implementing the health IT in a manner consistent with its certification. Thus the

[175] The costs of switching to a new technology include not only the costs of purchasing or licensing the technology itself but of installing and integrating it with other administrative and clinical IT systems, migrating data, redesigning associated workflows and processes, and retraining staff to use the new technology. The transition may also disrupt normal health care and business operations, adding additional costs and strain on provider organizations and staff.

disclosure of this information is no less important than the disclosure of information about additional types of costs.

Third, with regard to both "limitations" and "additional types of costs," we proposed to significantly broaden the types of information and the level of detail that a health IT developer would be required to disclose. In contrast with the price transparency requirements adopted in the 2014 Edition final rule, which required disclosure only of additional types of costs that a user "would pay" to implement certain capabilities, we proposed to require health IT developers to be more proactive in identifying the kinds of limitations and additional types of costs that a user "may" pay or encounter in order to achieve any use of the health IT within the scope of its certification. Specifically, developers would be required to provide, in plain language, a detailed description of any "known material information" about limitations that a purchaser may encounter, and about additional types of costs that a user may be required to pay, in the course of implementing or using the capabilities of health IT to achieve any use within the scope of its certification. We also provided an extensive discussion of the types of information that would be deemed "material" and of the types of information that developers would and would not be required to disclose. Further, we described the manner in which the information would need to be disclosed as well as safeguards to avoid the disclosure of intellectual property and trade secrets.

Finally, in addition to these three aspects, we proposed one additional element designed to complement the disclosure requirements set forth in the Proposed Rule. We proposed that in addition to requiring health IT developers to disclose known material information about their certified health IT, an ONC-ACB would be required to obtain a public attestation from every health IT developer to which it issues or has issued a certification for any edition of certified

health IT. The attestation would take the form of a written "pledge" by the health IT developer to take the additional, voluntarily step of proactively providing information (which it would already be required to disclose via its website and in marketing and other materials) to all current and prospective customers as well as to any other persons who request such information. While adherence to the attestation would be strictly voluntary, we explained that requiring developers to make the attestation could encourage a culture of greater transparency and accountability in the health IT marketplace. For example, health IT purchasers, implementers, and users (and organizations that represent them) would be invited to approach developers directly and request information most relevant to their health IT decisions and needs. The expectation that developers will provide this information in a way that is more meaningful for stakeholders, consistent with the attestation, would create greater competitive incentives for developers to do so. Developers would also receive important feedback about the types of information that stakeholders find important, which would assist developers in meeting their disclosure obligations under the ONC Health IT Certification Program. For example, requests for information about a particular cost or capability may alert the developer to a material limitation or additional type of cost that it is required to disclose.

Comments. Most commenters strongly supported our proposal to require the disclosure of additional information about certified health IT. Many of these commenters agreed with our assessment that providers and other stakeholders often lack reliable information about certified health IT products and services and, as a result, may encounter unexpected costs and limitations that interfere with their ability to successfully implement and use certified health IT capabilities. Several commenters cited examples of providers encountering unexpected fees to license, implement, upgrade, or use health IT; to exchange or export electronic health information stored

in certified health IT; or to integrate certified health IT capabilities and data with other technologies, organizations, and applications. Similarly, commenters cited examples of providers encountering unanticipated contractual, technical, or other limitations on their ability to implement and use certified health IT capabilities in the manner they anticipated when they purchased or licensed the technology. Some commenters stated that small providers are especially vulnerable to these unexpected challenges because they lack the resources and time to study and understand the complexities associated with developer contracts.

Many commenters stated that the proposed transparency and disclosure requirements would help ensure that providers are informed of these and other considerations and enable them both to more reliably estimate the resources needed to successfully implement certified health IT capabilities and to arrive at a realistic expectation of how those capabilities will perform in the field. Commenters also noted that this increased ability of customers to assess and compare certified health IT products and services could reduce the problems of "lock in" and "unfair surprise" described in our proposal and put pressure on developers to compete to innovate and deliver better and more affordable technologies and solutions based on provider and consumer preferences. Commenters also stated that greater transparency in health IT products and services would help to expose and discourage information blocking and other business practices that frustrate interoperability and prevent the effective sharing of electronic health information. A number of commenters cited our discussion of these issues in our recent Report to Congress on Health Information Blocking.[176]

Response. We thank commenters for their detailed and thoughtful feedback on this proposal. As that feedback overwhelmingly demonstrates, the lack of transparency and access to

[176] ONC, Report to Congress on Health Information Blocking (April 2015), http://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf (hereinafter "Blocking Report").

reliable information about health IT products and services is a persistent and pervasive problem that undermines the reliability of certifications issued on behalf of ONC and creates substantial risks that users will be unable to successfully implement and derive the benefits of certified health IT. For this and the additional reasons discussed below in our responses to comments on specific aspects of our proposal, we have finalized the transparency and disclosure requirements at § 170.523(k). We have finalized these requirements as proposed, except for the attestation requirement, which we have revised. To complement these new requirements, we have also finalized additional reporting requirements to the open data CHPL, which we have added to §§ 170.523(f)(1) and (f)(2). We discuss these revisions below in our response to the comments on this aspect of our proposal.

Comments. Several commenters specifically agreed with our proposal to require health IT developers to disclose known material information about the capabilities of certified health IT, including limitations and additional types of costs. Many commenters also specifically endorsed our proposal to apply these requirements uniformly to all capabilities and uses within the scope of a health IT's certification—not just those required to meet a specific meaningful use objective or measure. Commenters stated that applying clear and uniform standards for the disclosure of this information will be necessary to help customers understand and use an increasing array of certified health IT products, services, and capabilities.

In contrast, some commenters, mostly health IT developers, strongly opposed all of the proposed disclosure requirements. These commenters stated, among other objections, that requiring the disclosure of this information is unnecessary; would be burdensome for developers; and could limit developers' flexibility to design and market their products and services in ways that their customers value. Several commenters stated that the proposed disclosure requirements

would be unfair to developers because developers may not be aware of capabilities or uses of their technology that are not specifically required to demonstrate the meaningful use of certified health IT under the EHR Incentive Programs. Some commenters also stated that developers should not be expected to know about—or required to disclose—limitations or additional types of costs that may apply to third-party components or that may flow from local implementation decisions.

Response. While we appreciate the concerns raised by some commenters, we believe they are outweighed by the need to promote greater and more meaningful disclosure of information by developers of health IT certified on behalf of ONC.

First, we respectfully disagree with the assertion that these transparency and disclosure requirements are unnecessary. Our conclusion is based on the overwhelming support for this proposal from providers and other customers of certified health IT, whose comments and first-hand accounts of the health IT marketplace affirm our assessment in the Proposed Rule. Those comments suggest that many customers lack access to reliable information about certified health IT products and services and, as a result, are more likely to encounter unexpected costs and limitations that interfere with their ability to successfully implement and use certified health IT capabilities. The comments also provide insight into other deleterious consequences that flow from a lack of basic transparency in the marketplace, including the increased risk that developers will engage in information blocking and other business practices that undermine the goals of certification and the ONC Health IT Certification Program.

Second, we disagree that the transparency and disclosure requirements are burdensome or unfair to health IT developers. We note that developers are not required to disclose information of which they are not and could not reasonably be aware, nor to account for every conceivable

cost or implementation hurdle that a customer may encounter in order to successfully implement and use the capabilities of a developer's certified health IT. Indeed, we recognized in the Proposed Rule that certified health IT often functions in combination with many third party technologies and services whose specific costs and limitations may be difficult for a health IT developer to precisely predict or ascertain. Local implementation factors and other individual circumstances also vary substantially among customers and impact the cost and complexity of implementing certified health IT. In addition, the costs of upgrading health IT to meet new regulatory requirements or compliance timelines, which are subject to change, may make some particular types of additional costs especially difficult to forecast.

Nevertheless, it is reasonable to assume that health IT developers are experts on their own products and services and possess sophisticated technical and market knowledge related to the implementation and use of health IT in a variety of settings in which their products are used. Through their accumulated experience developing and providing health IT solutions to their customers, health IT developers should be familiar with the types of costs and limitations that most users encounter, and therefore must describe these in sufficient detail so as to provide potential customers with the information they need to make informed purchasing or licensing and implementation decisions.

Finally, we disagree that the transparency and disclosure requirements will limit developers' flexibility to design and market their products and services in ways that their customers value. To the contrary, greater transparency in health IT developers' business practices will provide customers with the basic information they need to make informed decisions in the marketplace, which will in turn encourage and enable developers to experiment,

innovate, and compete to deliver products and services that customers demand and on such prices and terms that meet their individual needs and requirements.

Comments. Several commenters stated that ONC-ACBs and developers may have difficulty complying with the proposed disclosure requirements because we had not specified with sufficient clarity or detail the types of information that developers would be required to disclose. Two ONC-ACBs indicated that additional guidance may be needed to fully implement the requirements. However, another ONC-ACB that commented extensively on the proposal did not raise these concerns. In addition, the ONC-AA supported our approach and noted that the criteria and examples described in the Proposed Rule provided sufficient guidance to ONC-ACBs and developers. The ONC-AA stated that while ONC-ACBs and developers would inevitably need to exercise some degree of judgment regarding the precise form and content of the required disclosures, comparisons across developers' disclosures would promote consistency and provide additional clarity to ONC-ACBs, developers, and other stakeholders as to the types of information and level of detail that must be disclosed.

Response. We understand the desire for clear and predictable rules governing these expanded disclosure requirements under the ONC Health IT Certification Program. We note that our ability to issue guidance is limited by the problem we are trying to solve; that is, the lack of transparency in the marketplace means we lack detailed information about many types of limitations and additional types of costs that customers and users may encounter in the course of implementing and using certified health IT and that developers would be required to disclose.

Nevertheless, based on the comments and in particular the feedback of the ONC-AA, we believe that the principles and examples provided in the Proposed Rule provide a workable starting point for ONC-ACBs to apply, and developers to comply with, the disclosure

requirements. As stated by the ONC-AA, while these principles inevitably involve the exercise of some discretion, comparisons across developers' disclosures over time will provide consistency and additional clarity regarding the types of information and level of detail that developers must disclose. In addition, as our visibility into these practices improves, we stand ready to issue additional guidance.

For the sake of additional clarity, we clarify that to comply with the disclosure requirements, a developer must disclose in plain language—on its website and in all marketing materials, communications statements, and other assertions related to its certified health IT—a detailed description of all known material information concerning limitations and additional types of costs that a person may encounter or incur to implement or use certified health IT capabilities, whether to meet meaningful use objectives and measures or to achieve any other use within the scope of the health IT's certification. Such information is "material" (and its disclosure therefore required) if the failure to disclose it could substantially interfere with the ability of a user or prospective user to implement certified health IT in a manner consistent with its certification. Certain kinds of limitations and additional types of costs will always be material and thus, if known, must be disclosed. These include but are not limited to:

- Additional types of costs or fees (whether fixed, recurring, transaction-based, or otherwise) imposed by a developer (or any third-party from whom the developer purchases, licenses, or obtains any technology, products, or services in connection with its certified health IT) to purchase, license, implement, maintain, upgrade, use, or otherwise enable and support the use of capabilities to which health IT is certified; or in connection with any data generated in the course of using any capability to which health IT is certified.

- Limitations, whether by contract or otherwise, on the use of any capability to which technology is certified for any purpose within the scope of the technology's certification; or in connection with any data generated in the course of using any capability to which health IT is certified.
- Limitations, including but not limited to technical or practical limitations of technology or its capabilities, that could prevent or impair the successful implementation, configuration, customization, maintenance, support, or use of any capabilities to which technology is certified; or that could prevent or limit the use, exchange, or portability of any data generated in the course of using any capability to which technology is certified.

As already noted, developers are not required to disclose information of which they are not and could not reasonably be aware, nor to account for every conceivable type of cost or implementation hurdle that a customer may encounter in order to successfully implement and use the capabilities of the developer's certified health IT. Developers are required, however, to describe with particularity the nature, magnitude, and extent of the limitations or types of costs. A developer's disclosure possesses the requisite particularity if it contains sufficient information and detail from which a reasonable person under the circumstances would, without special effort, be able to reasonably identify the specific limitations he may encounter and reasonably understand the potential costs he may incur in the course of implementing and using capabilities for any purpose within the scope of the health IT's certification.

Comments. A commenter asked whether a developer would be required to disclose known material limitations of its certified health IT where the limitations are due to the actions of a third-party from whom the developer purchases, licenses, or obtains technology, products, or services in connection with its own certified health IT. The commenter noted that in describing

certain kinds of presumptively material information that a developer would be required to disclose, we mentioned third parties only in connection with types of costs and not limitations.

Response. We clarify that a developer must disclose known material limitations of its certified health IT, including limitations caused by a third party that the developer should be aware of under the circumstances.

A developer's disclosure obligations are limited to material information that the developer knows or should know about under the circumstances. The reference to third parties at § 170.526(k)(1)(iv)(A) and above is intended to limit the material types of costs a developer will be presumed to know about to those that the developer itself imposes or that are imposed by a third party from whom the developer purchases, licenses, or obtains any technology, products, or services in connection with its certified health IT. This reflects the reality that developers are unlikely to know about types of costs imposed by third parties with whom they do not have a contractual relationship. In contrast, because limitations include not only contractual restrictions but also technical and practical limitations of a developer's technology, developers will often be aware of material limitations notwithstanding the existence of a contractual relationship, and there is therefore no reason to expressly qualify the types of material limitations for which a developer may, in appropriate circumstances, be presumed to have knowledge.

Comments. Several commenters who supported our proposal urged us to require the disclosure of more specific information about prices and cost structures for health IT products and services. Some of these commenters suggested that developers be required to disclose specific prices for each service a user may need and provide guidance on how relevant factors—such as the volume of transmissions, geography, interfaces, and exchange partner technology—may impact the costs of those services. One commenter stated that developers should be required

to disclose more detailed and specific cost structures that include costs and fees not covered by the provider's service contract. Another commenter stated that developers should be required to disclose costs that could arise from common end-user customizations and implementations of the developer's health IT. Commenters believed that requiring the disclosure of this information would enable customers to more easily and accurately estimate their likely total cost of ownership and other costs.

In contrast, several health IT developers and a few other commenters strongly objected to a requirement to disclose any additional information about prices or costs. One commenter stated that this information and other "commercial terms and conditions" are too varied and complex to be disclosed in a useful manner to customers. Other commenters worried that requiring disclosure of this information could expose intellectual property, trade secrets, or other sensitive information.

Response. We thank commenters for their extensive input regarding the types of costs and price information health IT developers should be required to disclose.

We understand the importance of ensuring that health IT developers' disclosures provide meaningful information to customers and users of certified health IT. We believe it is important for developers to provide the kind of information and level of detail that will enable ordinary purchasers, licensees, and users to understand and make informed health IT purchasing and implementation decisions.

At the same time, we appreciate that the disclosure of certain kinds of proprietary or confidential information may not be necessary to achieve these goals and may also lead to undesirable consequences. Requiring developers to disclose trade secrets and other confidential information, for example, could dampen innovation by making it difficult for developers to

license and make their technologies available on terms that protect their research and investments.[177] And requiring the disclosure of detailed price information could lessen price competition or even lead to price coordination among competitors, at least for certain kinds of products and services in highly concentrated markets.

We believe the approach described in the Proposed Rule accommodates these concerns by ensuring that developers' disclosures are comprehensive, and thus meaningful, while also providing certain safeguards against the unnecessary disclosure of proprietary or confidential information.

Consistent with that approach, and to comply with this final rule, a developer must make a comprehensive disclosure of all known material information regarding its certified health IT—including limitations and additional types of costs. With respect to types of costs, the disclosure must identify and describe the types of costs with particularity, from which a potential customer or user would be able to reasonably understand his potential costs to implement and use the health IT for any purpose within the scope of the health IT's certification. The disclosure must also describe the factors that impact additional types of costs, including but not limited to geographical considerations, volume and usage, costs associated with necessary interfaces or other licenses or technology, and costs associated with exchange partner technology and characteristics, among other relevant factors. Since certified technical capabilities may be bundled with non-certified capabilities, any disclosure would need to include an explanation of any limitations such other non-certified capabilities may have on the use or implementation of the certified capabilities.[178] Developers have substantial flexibility as to the content of their

[177] See M. Jager, 1 Trade Secrets Law § 1.1; Restatement (Third) of Unfair Competition § 39, cmt. a.
[178] Health IT includes "hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services . . . ." 42 U.S.C. § 300jj(5).

disclosures, including how they choose to describe the particular limitations and additional types of costs associated with their certified health IT products and services. As such, developers should be able to comply with the disclosure requirements without publishing their prices or cost structures or unnecessarily disclosing information that they deem confidential.

The following scenario and discussion further illustrate these requirements.

- Scenario: A Health IT Module is certified to the 2014 Edition transitions of care certification criterion at § 170.314(b)(1). The developer of the Health IT Module charges a yearly "subscription fee" for the use of the capability. In making the capability available, the developer bundles it with its own HISP. Because the developer is not a member of any trust network, users can only exchange transitions of care summaries with other users of the developer's own HISP and with users of third-party HISPs with which the developer has negotiated or is willing to negotiate a trust agreement. The developer also charges a "transaction fee" for each transitions of care summary sent or received via a third-party HISP (the transaction fee does not apply for transitions of care summaries exchanged among users of the developer's own HISP).

Under these facts, the developer must disclose the existence of the subscription fee and the transaction fee—each of which is a known material type of cost associated with the transitions of care capability. In addition, the developer must disclose the known material limitation (and any associated additional types of costs) presented by its HISP policy. The developer must describe each of these additional types of costs and limitations with particularity to the extent they impact the implementation and use of the transitions of care capability for any purpose to which it is certified.

Beginning with the "subscription fee," the developer must disclose that there is such a fee along with any factors that impact the amount a customer would have to pay. Examples include number of licenses or limitations on the number of workstations where the software is deployed, additional types of costs related to the volume of transactions, or usage, or associated bandwidth costs for a customer's transactions. Such factors would need to be described with particularity. For example, for additional types of costs related to the volume of transactions, the developer would need to explain how the volume of transactions would be measured and if variations in volume or types of transactions may trigger additional fees or variations in the subscription fee.

Turning to the developer's HISP policy, the developer must disclose this material limitation and the additional types of costs a user may incur as a result. The developer must explain, for example, that as a result of its policy the transitions of care capability is restricted and users will be unable to exchange transitions of care summaries with users of third-party HISPs with whom the developer does not have a trust agreement. The developer must describe, in plain terms, its current network of HISPs and how such network would enable a user to exchange transitions of care summaries with users of other HISPs servicing a provider's local referral area, including HISPs that participate in trust networks. Further, the disclosure needs to clearly identify any HISPs with whom the developer will not permit exchange or which the developer knows will not agree to a trust agreement with the developer (e.g., because the developer is not a member of a particular trust network). If the developer offers the option to customers to connect to third-party HISPs with whom the developer currently has no relationship, the developer must describe the process for customers to request such connectivity. The developer must also describe any additional types of costs that may apply for this service,

including a description of any factors (e.g., geographical considerations or variability in HISP technologies and trust policies) that impact the amount a customer would have to pay.

Finally, the developer would need to disclose the separate "transaction fee" charged for exchanging transitions of care summaries with users of third-party HISPs. Disclosure of all additional types of costs based on volume, geography, or exchange partner technology would be required. The developer would also be required to provide additional information to assist the customer in realistically understanding additional potential costs of sending and receiving transitions of care summaries via third-party HISPs.

The scenario and discussion above illustrate the substantial flexibility developers have in determining the content of their disclosures, including how they choose to describe the particular limitations and types of costs associated with their certified health IT products and services. We caution, however, that developers are ultimately responsible for effectuating a comprehensive disclosure that satisfies the expanded requirements of this final rule. Because developers have substantial flexibility as to the form and content of their disclosures, it is unlikely that they would have to disclose proprietary or confidential information in order to comply with these requirements. However, the safeguards we have adopted are prophylactic and do not create a substantive basis for a developer to refuse to comply with the requirements. Thus a developer cannot cure a deficient disclosure or avoid a non-conformity finding by asserting that the disclosure of known material limitations or types of costs would require it to disclose trade secrets or other proprietary or confidential information. We note that the ONC Health IT Certification Program is a voluntary program. To the extent that developers choose to seek certification under the Program and to market their products and services as certified health IT, they must comply with the transparency and disclosure requirements in their entirety.

Comments. An ONC-ACB stated that some health IT developers have circumvented the requirement to disclose required information on their websites by omitting discussion of the certification or certified status of their health IT. The ONC-ACB asked us to clarify whether such conduct is permissible or constitutes a violation of the disclosure requirements under § 170.523(k)(1). Relatedly, multiple ONC-ACBs asked whether it would be permissible for a developer to use an abbreviated or alternative disclosure more appropriate to the kind of marketing material and medium at issue. One commenter noted that requiring a detailed disclosure of information in all marketing materials or assertions about certified health IT is impracticable and not helpful to customers. It may also discourage developers from including such assertions in marketing and promotional materials or from using certain kinds of materials or media.

Response. A health IT developer's website is not only one of its most powerful marketing tools but also, for most people, among the most readily available sources of information about a developer's health IT products and services. It is therefore essential that a developer include the information specified by § 170.523(k)(1) on its website. This information must be included and updated on the developer's website regardless of whether the website refers to the certification or certified status of the developer's health IT. The information must also be located in a place that is accessible and obvious to viewers and contextually relevant to the certification criteria to which the disclosures pertain.

For the reasons stated by the commenters, we agree that requiring a comprehensive disclosure in all marketing materials and other assertions may be burdensome and counterproductive to our goal of providing this information to customers in a manner that is meaningful and likely to inform. Therefore, we clarify that a developer may satisfy the

requirement to disclose the information required by § 170.523(k)(1) in its marketing materials, communications statements, and other assertions related to a Complete EHR or Health IT Module's certification by providing an abbreviated disclaimer, appropriate to the material and medium, provided the disclaimer is accompanied by a hyperlink to the complete disclosure on the developer's website. Where a hyperlink is not feasible (for example, in non-visual media), the developer may use another appropriate method to direct the recipient of the marketing material, communication, or assertion to the complete disclosure on its website.

Because of the challenges and accommodations described above, and the need to ensure that customers and users are able to easily locate information about certified health IT products and services, we believe that developers' disclosures should be accessible from a single, authoritative source. Thus, we have included a developer's disclosures as part of the information that an ONC-ACBs must submit to ONC for inclusion in the open data CHPL. We have revised § 170.523(f)(1) and (f)(2) to reflect this requirement.

In keeping with the goal of making developers' disclosures accessible and useful to customers and other stakeholders, we have also revised § 170.523(k)(1)(ii), which requires developers to include in their disclosures certain types of administrative and programmatic information they are required to report to ONC. While the reporting and availability of this information is important and is still required by § 170.523(f)(1) and (2), requiring developers to insert all of this information in their disclosures could add unnecessary clutter and detract from the overall accessibility and clarity of those disclosures. Therefore, under § 170.523(k)(1)(ii), developers must include in their disclosures only a subset of this information that will be valuable to customers in making informed decisions about their certified health IT.

Comments. Several commenters supported our proposal to require developers to attest to voluntarily providing information about their required disclosures to additional persons and in additional circumstances. Other commenters questioned the value of this requirement or stated that it was duplicative of the other requirements we proposed. Some commenters stated that requiring developers to provide such an attestation as a condition of certification would in effect make compliance with the attestation mandatory.

Response. We appreciate the comments in support of the proposed attestation requirement, which we regard as a key feature of the transparency and disclosure requirements adopted in this final rule. In response to the comments questioning the value of this additional requirement, we clarify that the purpose of the attestation is to create market incentives—independent of any regulatory obligations—for health IT developers to be more transparent about their health IT products, services, and business practices. Although the attestation does not create any additional disclosure obligations under the ONC Health IT Certification Program, we believe it will encourage developers to make a good faith effort to ensure that customers and other persons actually receive the information that developers are required to disclose at such times and in such a manner as is likely to be useful in informing their health IT purchasing or licensing, implementation, and other decisions.

In the Proposed Rule, we explained that the attestation would take the form of a written "pledge" by the developer to take the additional, voluntarily step of proactively providing information (which it would already be required to disclose via its website and in marketing and other materials) to all current and prospective customers as well as to any other persons who request such information. While we stated that the attestation would not broaden or change a health IT developer's disclosure obligations under the ONC Health IT Certification Program,

some commenters believed that in practice developers would be forced to comply with the attestation. Because that was and is not our intent, we have revised the attestation requirement. Under the revised approach, which we have codified at § 170.523(k)(2), a developer must either attest that it will voluntarily take the actions described above, or, in the alternative, attest that it will not take these actions. Further, an ONC-ACB will be required to include the developer's attestation in the information submitted to the open data CHPL so that persons can easily identify which attestation the developer has made. We have revised §§ 170.523(f)(1) and (f)(2) accordingly.

3. Open Data Certified Health IT Product List (CHPL)

We proposed to require ONC-ACBs to report an expanded set of information to ONC for inclusion in the CHPL upon its conversion from its present form to an open data file represented in both XML and JSON and with accompanying API functionality. We are converting the CHPL to this new "open data CHPL" in response to feedback from stakeholders regarding the accessibility of information on the CHPL, especially the information contained in the publicly available test reports for certified health IT products.[179] We estimated that the conversion along with the future additional data collection we have proposed for 2015 Edition certifications would occur over the next 12 to 18 months from the date the Proposed Rule was issued.

[179] As the ONC Health IT Certification Program has matured, ONC-ACBs have continued to report the products and information about the products they have certified to ONC for listing on the CHPL. As part of the 2014 Edition final rule (77 FR 54271), we required additional transparency in the ONC Health IT Certification Program in the form of a hyperlink that ONC-ACBs needed to maintain that would enable the public to access the test results that the ONC-ACB used as the basis for issuing a certification. For all 2014 Edition products certified under the ONC Health IT Certification Program, the test results are available in a standardized summary accessible and from the product's detailed information page on the CHPL Web page. The test result summary includes granular detail from ATLs about the testing performed, including, among other information: The certification criteria tested; the test procedure, test data, and test tool versions used during testing for each certification criterion; instances where optional portions of certification criteria were tested; and which standard was used for testing when a certification criterion allowed for more than one standard to be used to meet the certification criterion. The test result summary also includes the user-centered design information and summative tests results applicable to a product in cases where it was required to meet the "safety-enhanced design" certification criterion (§ 170.314(g)(3)) in order to ultimately be certified.

To complement this conversion, we proposed to require ONC-ACBs to report an expanded set of information to ONC for inclusion in the open data CHPL. Specifically, we proposed to revise § 170.523(f) to move the current (f) to (f)(2) and to create a new paragraph (f)(1) that would require ONC-ACBs upon issuing a 2015 Edition (or any subsequent edition certification) to report on the same data elements they report to ONC under § 170.523(f), the information contained in the publicly available test report, and certain additional data listed in the Proposed Rule. We explained that the additional data reported to the open data CHPL would include the information ONC-ACBs would be required to report in connection with corrective action plans under the proposal "'In-the-field' Surveillance and Maintenance of Certification" in the Proposed Rule. Because this data would be required for all, and not only 2015 Edition, certified health IT, we also proposed to revise new § 170.523(f)(2) (former § 170.523(f)) accordingly.

Consistent with ONC-ACBs' current reporting practice required by § 170.523(f), ONC-ACBs would be required to submit the additional data no less frequently than weekly. Because this expanded list of data would largely subsume the data included in the test results summary, we would no longer require for 2015 Edition and subsequent edition certifications that ONC-ACBs provide a publicly accessible hyperlink to the test results used to certify a Health IT Module.

In submitting this data related to corrective action and surveillance, ONC-ACBs would be required to exclude any information that would identify any user or location that participated in or was subject to surveillance (as currently required for ONC-ACBs' annual surveillance results reported to the ONC). ONC-ACBs would not be required and should take care not to submit proprietary information to ONC for inclusion in the open data file. With respect to the

reporting of corrective action plan and surveillance information for health IT, an ONC-ACB would be able to meet the requirement by summarizing the deficiencies leading to its non-conformity determination without disclosing information that the ONC-ACB believes could be proprietary or expose it to liability.

Consistent with these proposals, we also proposed to make a conforming modification to 45 CFR 170.523(k)(1)(ii) which currently cross references § 170.523(f) to cross reference proposed paragraph (f)(2) for 2014 Edition certifications and an equivalent set of data (minus the test results summary) in paragraph (f)(1) for 2015 Edition and subsequent certifications.

Comments. Most commenters supported requiring ONC-ACBs to report an expanded set of information to ONC for inclusion in the open data CHPL. Multiple commenters agreed that information contained in the CHPL has previously been difficult to access and use and supported our proposal and plans to make this information easier to access. Commenters stated that this information and the open data CHPL more generally would provide greater product transparency, with a focus on surveillance, user-centered design, and testing results.

Response. We appreciate these comments in support of our proposal. We have finalized this proposal in its entirety, subject to minor clarifications and revisions discussed below.

Comments. Commenters offered suggestions on operational details of the conversion of the current CHPL to an open data format and on how we should subsequently collect and organize information via the open data CHPL.

Response. We appreciate these suggestions. While the conversion of the CHPL is already underway, we will consider these comments on operational aspects of the open data CHPL as we continue to implement these efforts.

Comments. Some commenters stated that this proposal was unnecessary or that its benefits would be outweighed by associated costs and administrative burden of collecting and reporting an expanded set of information to ONC for inclusion in the new open data CHPL. Commenters asked us to review the proposed reporting requirements to see if they might be clarified and simplified.

Response. While we recognize that the collection and reporting of additional data to the open data CHPL will place a new reporting burden on ONC-ACBs, we believe that the benefit to the public of having all of this data about product certification in granular detail far outweighs the administrative burden it will take to report this information.

Comments. A number of commenters, including several health IT developers, objected to the reporting of corrective action plan information to the publicly accessible open data CHPL. Some commenters felt that information about non-conformities should not be made public unless and until the developer of the certified Complete EHR or certified Health IT Module at issue has been given a full and fair opportunity to contest the ONC-ACB's determination, including whether the developer was responsible or "at fault" for the non-conformity. Other commenters stated that such information should never be made public because it is bound to lack important context, could be misinterpreted, or would not offer substantial value to health IT customers and users. Separately, some commenters raised concerns regarding the reporting of proprietary or competitively sensitive information.

Response. We have addressed the concerns related to the submission of corrective action plan and related information to the open data CHPL in section IV.D.1 of this preamble ("'In-the-field' Surveillance and Maintenance of Certification Criteria"). For the reasons stated there, we have finalized the requirement to submit a corrective action plan and related information to the

open data CHPL. Further, we have revised the specific data elements that must be submitted to accommodate the revised randomized in-the-field surveillance and corrective action plan and related reporting requirements finalized at §§ 170.556(c)–(e).

Comments. Some commenters expressed confusion as to why we proposed to require the submission of corrective action and related information only for randomized surveillance and not for other surveillance activities. Commenters also suggested several technical clarifications to our proposed regulation text to ensure alignment between our "Open Data CHPL" and "'In-the-field' Surveillance and Maintenance of Certification" proposals.

Response. We have responded to these concerns in section IV.D.1 of this preamble ("'In-the-field' Surveillance and Maintenance of Certification Criteria") and refer commenters to that section for a more detailed treatment of these issues. For the reasons stated there, we agree with commenters that the requirement to submit corrective action and related information to the open data CHPL should be applied to all forms of surveillance and all confirmed non-conformities. We have also refined the data elements required to be reported for reasons also set forth in section IV.D.1 of this preamble. To implement these changes we have revised the randomized in-the-field surveillance and corrective action plan reporting requirements at §§ 170.556(c)–(e) and have made conforming revisions to § 170.523(k)(1) and § 170.523(k)(2) to accommodate the revised data elements.

As discussed in section IV.D.2 of this preamble ("Transparency and Disclosure Requirements"), we have also added developers' disclosures required by § 170.523(k)(1) and their attestations required by § 170.523(k)(2) to the data that must be submitted to ONC for inclusion in the open data CHPL.

4. Records Retention

We proposed to change the records retention requirement in § 170.523(g) in two ways. We proposed to require that ONC-ACBs retain all records related to the certification of Complete EHRs and/or Health IT Module(s) (including EHR Modules) for a minimum of 6 years instead of 5 years as was required by regulation. We stated that this proposal would make certification records available for a longer time period, which may be necessary for HHS programmatic purposes such as evaluations or audits. We also proposed that records of certifications performed under the ONC Health IT Certification Program must be available to HHS upon request during the proposed 6-year period that a record is retained. We stated that this would help clarify the availability of certification records for agencies (e.g., CMS) and authorities (e.g., the Office of Inspector General) within HHS.

Comments. A majority of commenters expressed support for the proposed 6-year records retention requirement without additional comment. One commenter suggested a 10-year requirement. Another commenter recommended record retention requirements for the life of the edition of certification criteria. A commenter requested clarification on the start date of the retention period, asking whether the start date was from the first instance of certification for a product or from the last documented date of an activity related to the certification such as surveillance.

Response. We thank commenters for their feedback. We have adopted a records retention provision that requires ONC-ACBs to retain all records related to the certification of Complete EHRs and/or Health IT Module(s) (including EHR Modules) for the "life of the edition" plus an additional 3 years. We have also adopted our proposal to make these records available to HHS upon request during this period of time for the reasons specified above and in the Proposed Rule. We define the "life of the edition" as beginning with the codification of an edition of certification

criteria in regulation and ending when the edition is removed from regulation. This means that certification records for a Complete EHR and/or Health IT Module(s) (including EHR Modules) certified to a specific edition (e.g., the 2015 Edition) must be kept for a minimum of 3 years after the effective date of the removal of that edition from the Code of Federal Regulations (CFR). This approach is responsive to commenters and addresses the goal of ensuring records are available for HHS programs, including evaluations and audits, during a relevant period of time. It provides more clarity and certainty than establishing a term such as 6 or 10 years, which may not be a sufficient period of time or too long a period of time. It also provides consistency and reduced burden for ONC-ACB record keeping. To illustrate this point, establishing a record keeping period based on an event such as an instance of first certification or a surveillance activity would lead to variances in ONC-ACB record keeping for certified health IT, while under our finalized approach all records would be retained until a regulatory certain date (at least 3 years after an edition is removed from the CFR). To note, the record would include all documents related to the issued certification, such as test results and surveillance engagements and results.

5. Complaints Reporting

We proposed that ONC-ACBs provide ONC (the National Coordinator) with a list of complaints received on a quarterly basis. We proposed that ONC-ACB indicate in their submission the number of complaints received, the nature or substance of each complaint, and the type of complainant for each complaint (e.g., type of provider, health IT developer, etc.). We stated that this information would provide further insight into potential concerns with certified health IT and/or the ONC Health IT Certification Program and give ONC a better ability to identify trends or issues that may require action including notification of the public.

Comments. A majority of commenters expressed support for the proposed quarterly complaints reporting requirement. Some commenters, however, expressed opposition or concern with the proposed requirement. These commenters stated that the proposed requirement would add certification cost without value. A few commenters recommended a more robust reporting requirement than proposed, suggesting we require a more comprehensive list of complaint data as well as aggregated and analyzed data. One commenter requested clarification on whether the proposed requirement would apply to any complaint received by an ONC-ACB, such as complaints about an ONC-ACB's services and complaints about certified Health IT Modules.

Response. We have adopted this requirement as proposed with clarifications in response to comments. We continue to believe that this requirement will provide us with insight and situational awareness of issues related to the ONC Health IT Certification Program. We further believe these benefits outweigh the limited reporting burden we have specified, which does not adopt any new reporting requirements as suggested by a few commenters. We clarify that this requirement applies to all complaints received by the ONC-ACB. This includes, but is not limited to, complaints regarding ONC-ACB services, certified health IT, and the ONC Health IT Certification Program in general. To provide ONC-ACBs sufficient time to meet this new requirement, this provision will become effective on April 1, 2016. This means that we expect ONC-ACBs to first provide ONC with a list of complaints received on July 1, 2016.

We intend to provide, as necessary, more specific guidance to ONC-ACBs through the annual ONC Health IT Certification Program surveillance guidance on reporting complaints received regarding certified Health IT Modules.

6. Adaptations and Updates of Certified Health IT

We proposed to require that ONC-ACBs obtain monthly reports from health IT developers regarding their certified health IT. Specifically, we proposed to require that ONC-ACBs obtain a record of all adaptations and updates, including changes to user-facing aspects, made to certified health IT (i.e., Complete EHRs and certified Health IT Modules), on a monthly basis each calendar year, and we requested comment on whether we should require even more frequent reporting. We stated that this new PoPC would apply for all certified Complete EHRs and certified Health IT Modules (which includes "EHR Modules") to the 2014 Edition and all certified Health IT Modules to the 2015 Edition.

We proposed that the PoPC would become effective with this final rule and we would expect ONC-ACBs to begin complying with the PoPC at the beginning of the first full calendar month that is at least 30 days after the effective date of the final rule. We explained that we would not expect the information in these records to be reported to ONC and listed on the CHPL. Rather, we stated that the best course of action would be for ONC-ACBs to retain this information to provide awareness to the ONC-ACB on adaptations and updates made to technologies they certified.

Comments. We received mixed comments in response to the proposal. A number of commenters supported the proposal, but expressed concerns with the volume and frequency of updates to certified health IT. Commenters stated that updates could arise from relatively small changes to software code that do not result in risks to the certified health IT and that the burden to collect a list of these updates would not be worth the effort. Some commenters noted that health IT developers time their major updates with certification to reflect a new product listing on the CHPL whereas others do not. These commenters suggested there is inconsistency in the industry in the versioning of certified products. One commenter recommended that we provide

guidance on consistently distinguishing major from minor updates for products listed on the CHPL.

Response. In response to comments and to balance the ONC-ACBs' burden, we have adopted a more limited requirement than proposed. We agree with commenters that many updates to certified health IT products would not normally pose a risk to certified capabilities or patient safety. As such, we have limited the requirement to only adaptations (all adaptations); and all updates that affect the capabilities included in certification criteria to which the "safety-enhanced design" certification criteria apply.[180] These types of updates, particularly changes to the user-interface, pose the greatest risk to patient safety. The adoption of this requirement will provide ONC-ACBs with more insight and transparency into these kinds of updates and adaptations, which should improve ONC-ACBs' situational awareness and surveillance.

We thank the commenter for the feedback on distinguishing major and minor updates. We first note that, as stated in the 2014 Edition final rule (77 FR 54268), unless adaptations are presented for separate certification, the CHPL would not independently list the adaptation because it is considered part of a previously certified Complete EHR or certified Health IT Module, including EHR Modules. Second, the CHPL does not list updates to products unless they are presented for separate certification. This policy allows a health IT developer to update a product for routine maintenance or to include new or modified capabilities without the need for

[180] 2014 Edition certification criteria: CPOE (§170.314(a)(1)); drug-drug, drug-allergy interaction checks (§170.314(a)(2)); medication list (§170.314(a)(6)); medication allergy list (§170.314(a)(7)); clinical decision support (§170.314(a)(8)); electronic medication administration record (§170.314(a)(16)); CPOE – medications (§170.314(a)(18)); CPOE – laboratory (§170.314(a)(19)); CPOE – diagnostic imaging (§170.314(a)(20)); electronic prescribing (§170.314(b)(3)); clinical information reconciliation (§170.314(b)(4)); and clinical information reconciliation and incorporation (§170.314(b)(9)).
2015 Edition certification criteria: CPOE – medications (§170.315(a)(1)); CPOE – laboratory (§170.315(a)(2)); CPOE – diagnostic imaging (§170.315(a)(3)); drug-drug, drug-allergy interaction checks (§170.315(a)(4)); demographics (§170.315(a)(5)); problem list (§170.315(a)(6)); medication list (§170.315(a)(7)); medication allergy list (§170.315(a)(8)); clinical decision support (§170.315(a)(9)); implantable device list (§170.315(a)(14)); clinical information reconciliation and incorporation (§170.315(b)(2)); and electronic prescribing (§170.315(b)(3)).

recertification. However, in these instances, the product name and version on the CHPL would remain unchanged. We established an attestation process for a product to be approved for inherited certified status to provide a more efficient pathway for certification for a new version of a previously certified product in the Permanent Certification Program final rule (76 FR 1306). As part of this policy, we noted that we do not presume the version numbering schema that a health IT developer may choose to utilize. For compliance with this requirement, the focus on "updates" is for all updates to certified Health IT that affect the capabilities included in certification criteria to which the "safety-enhanced design" criteria apply.

Comments. A commenter requested that we clarify the definition of an "adaptation." Another commenter suggested that ONC-ACBs should only be required to monitor adaptations made by the health IT developer as it would be impractical for an ONC-ACB to monitor all customer-initiated adaptations. A commenter requested clarification as to whether an ONC-ACB is expected to review each report from a health IT developer, which the commenter contended could be time-consuming and costly. Another commenter requested clarification as to whether an ONC-ACB has the authorization to suspend or withdraw a certification if the health IT developer does not provide a report of adaptations and updates within the specified timeframe.

Response. We maintain our previously adopted definition of an "adaptation" as a software application designed to run on a different medium that includes the full and exact same capabilities included in the Complete EHR or certified Health IT Module, including EHR Modules (77 FR 54267). We refer readers to the discussion in the 2014 Edition final rule preamble for more detailed examples of adaptations (77 FR 54267). We also previously stated in the 2014 Edition final rule (77 FR 54268) that a health IT developer can choose to seek certification for adaptations which would lead to it being separately listed on the CHPL and

permit the health IT developer to openly sell the adaptation to all potential purchasers as a separate certified product.

We would expect that ONC-ACBs obtain a record of adaptations of certified health IT made by the health IT developer as those are the adaptations covered by the issued certification. An ONC-ACB has the discretion in determining how much time and resources should be devoted to reviewing the lists provided by health IT developers. As previously noted, we expect this information to inform ONC-ACBs surveillance activities for certified health IT. In terms of non-compliance by a health IT developer in providing the requisite list, we note that an ONC-ACB retains its authority and oversight over the certifications it issues and has the discretion to implement that authority and oversight in a manner that supports its role and responsibilities as well as the integrity of the ONC Health IT Certification Program.

Comments. We received a number of comments on the proposed frequency in which an ONC-ACB would have to obtain a record of all adaptations and applicable updates, with many commenters suggesting quarterly reporting. Another commenter suggested that the reports should be required only when adaptations and updates occur, or alternately weekly.

Response. We have finalized a calendar quarter reporting frequency for this requirement. This approach addresses commenters' concerns about burden, but also ensures that ONC-ACBs receive timely notifications about new adaptations and updates that could affect the safety of certified health IT. In order to provide ONC-ACBs and health IT developers sufficient time to plan and implement this new requirement, this PoPC will not become effective until April 1, 2016. For clarity, we reiterate that this PoPC applies to all certifications issued to the 2014 Edition, 2015 Edition, and future editions of certification criteria. We expect all ONC-ACBs to

receive lists from health IT developers on July 1, 2016, and then every calendar quarter thereafter (e.g., October 1, 2016, January 1, 2017, and so on).

E. "Decertification" of Health IT – Request for Comments

The Proposed Rule proposed and the final rule take certain steps to support the certification of health IT that meets relevant program standards and permits the unrestricted use of certified capabilities that facilitate health information exchange (see the "In-The-Field Surveillance and Maintenance of Certification" and "Transparency and Disclosure Requirements" proposals in section IV.D of this preamble).

In the Proposed Rule, we stated that additional rulemaking would be necessary to implement any approach that would include ONC appropriating an ONC-ACB's delegated authority to issue and terminate a certification, including establishing new program requirements and processes by which ONC or an ONC-ACB would have the grounds to terminate an issued certification. We requested comment on the circumstances, due process, remedies, and other factors that we should consider regarding the termination of a certification. To assist commenters, we provided a brief background of the ONC Health IT Certification Program and examples of the complexities and potential impacts associated with terminating a certification. We asked commenters to account for the potentially profound asymmetric impacts revoking a certification could create, especially if based on the business practices (by health IT developers or their customers) associated with the health IT's use and not necessarily the health IT's performance according to certification requirements.

Comments. Commenters overwhelmingly expressed support for the decertification of health IT products that did not continue to meet certification requirements or proactively blocked the sharing of health information. Of these commenters, the majority supported a clear and

structured approach to "decertification," with some commenters specifically recommending a regulatory approach that could be implemented as soon as possible. However, other commenters opposed changing the current approach or, at a minimum, urged caution in implementing a new "decertification" process. In this regard, commenters recommended clear parameters be established that would lead to decertification; appropriate due processes, including sufficient opportunities to correct deficiencies and non-compliance; and safeguards for non-culpable parties, such as "hold harmless" provisions, hardship exemptions, and "safe harbors" when applicable. A few commenters also suggested that further stakeholder input was needed before considering regulations, particularly to fully understand the "downstream" implications of "decertification."

Response. We thank commenters for their feedback. As noted in the Proposed Rule, additional rulemaking would be necessary to implement any new "decertification" process. We will take the comments received under consideration as we determine whether a new regulatory "decertification" process for health IT is necessary or whether other steps could better support the continued compliance of certified health IT with certification requirements, the unencumbered access and use of certified capabilities of health IT, the unrestricted exchange of health information, and overall interoperability.

V. Incorporation by Reference

The Office of the **Federal Register** has established new requirements for materials (e.g., standards and implementation specifications) that agencies incorporate by reference in the **Federal Register** (79 FR 66267; 1 CFR 51.5). Specifically, § 51.5(b) requires agencies to discuss, in the preamble of a final rule, the ways that the materials they incorporate by reference

are reasonably available to interested parties and how interested parties can obtain the materials; and summarize, in the preamble of the final rule, the material they incorporates by reference.

To make the materials we have incorporated by reference reasonably available, we provide a uniform resource locator (URL) for the standards and implementation specifications. In many cases, these standards and implementation specifications are directly accessible through the URL provided. In instances where they are not directly available, we note the steps and requirements necessary to gain access to the standard or implementation specification. In most of these instances, access to the standard or implementation specification can be gained through no-cost (monetary) participation, subscription, or membership with the applicable standards developing organization (SDO) or custodial organization. In certain instances, where noted, access requires a fee or paid membership.

The National Technology Transfer and Advancement Act (NTTAA) of 1995 (15 U.S.C. 3701 *et seq*.) and the Office of Management and Budget (OMB) Circular A–119[181] require the use of, wherever practical, technical standards that are developed or adopted by voluntary consensus standards bodies to carry out policy objectives or activities, with certain exceptions. The NTTAA and OMB Circular A-119 provide exceptions to selecting only standards developed or adopted by voluntary consensus standards bodies, namely when doing so would be inconsistent with applicable law or otherwise impractical. As discussed in section III.A.2 of this preamble, we have followed the NTTAA and OMB Circular A-119 in adopting standards and implementation specifications , including describing any exceptions in the adoption of standards and implementation specifications. Over the years of adopting standards and implementation specifications for certification, we have worked with SDOs, such as HL7, to make the standards

[181] http://www.whitehouse.gov/omb/circulars_a119

we adopt and incorporate by reference in the **Federal Register** available to interested stakeholders. As described above, this includes making the standards and implementation specifications available through no-cost memberships and no-cost subscriptions.

As required by § 51.5(b), we provide summaries of the standards and implementation specifications we have adopted and incorporated by reference in the **Federal Register**. We also provide relevant information about these standards and implementation specifications throughout section III.3 of the preamble. In particular, in relevant instances, we identify differences between previously adopted versions of standards and implementation specifications and 2015 Edition adopted versions of standards and implementation specifications.

We have organized the following standards and implementation specifications that we have adopted through this final rule according to the sections of the Code of Federal Regulation (CFR) in which they are codified and cross-referenced for associated certification criteria that we have adopted in 45 CFR 170.315.

Transport and other protocol standards – 45 CFR 170.202

- Applicability Statement for Secure Health Transport, Version 1.2.

URL: http://wiki.directproject.org/file/view/Applicability+Statement+for+Secure+Health+Transport+v1.2.pdf. This is a direct access link.

Summary: This document is intended as an applicability statement providing constrained conformance guidance on the interoperable use of a set of Requests for Comments (RFCs) describing methods for achieving security, privacy, data integrity, authentication of sender and receiver, and confirmation of delivery consistent with the data transport needs for health information exchange.

- Implementation Guide for Delivery Notification in Direct, Version 1.0.

URL:

http://wiki.directproject.org/file/view/Implementation+Guide+for+Delivery+Notification+in+Direct+v1.0.pdf. This is a direct access link.

Summary: This document provides implementation guidance enabling Security/Trust Agents (STAs) to provide a high level of assurance that a message has arrived at its destination. It also outlines the various exception flows that result in a compromised message delivery and the mitigation actions that should be taken by STAs to provide success and failure notifications to the sending system.

Functional standards – 45 CFR 170.204

- HL7 Version 3 Standard: Context Aware Knowledge Retrieval Application ("Infobutton"), Knowledge Request, Release 2.

URL: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=208. Access requires a "user account" and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The Context-aware knowledge retrieval specifications (Infobutton) provide a standard mechanism for clinical information systems to request context-specific clinical knowledge from online resources. Based on the clinical context, which includes characteristics of the patient, provider, care setting, and clinical task, Infobutton(s) anticipates clinicians' and patients' questions and provides automated links to resources that may answer those questions.

- HL7 Implementation Guide: Service-Oriented Architecture Implementations of the Context-aware Knowledge Retrieval (Infobutton) Domain, Release 1.

URL: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=283. Access requires a "user account" and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: Context-aware knowledge retrieval (Infobutton) into clinical information systems help deliver clinical knowledge to the point of care as well as patient-tailored education material. This specification enables the implementation of context-aware knowledge retrieval applications through a Service Oriented Architecture based on the RESTful software architectural style.

- HL7 Version 3 Implementation Guide: Context-Aware Knowledge Retrieval (Infobutton), Release 4.

URL: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=22. Access requires a "user account" and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: Context-aware knowledge retrieval (Infobutton) in clinical information systems help deliver clinical knowledge to the point of care as well as patient-tailored education material. This implementation guide provides a standard mechanism for EHR systems to submit knowledge requests over the HTTP protocol through a standard using a URL format.

Content exchange standards and implementation specifications for exchanging electronic health information – 45 CFR 170.205

- HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture – Category I (QRDA I); Release 1, Draft Standard for Trial Use (DSTU) Release 3 (US Realm), Volumes 1 (Introductory Material) and 2 (Templates and Supporting Material).

URL: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=35. Access requires a "user account" and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The Quality Reporting Document Architecture (QRDA) is an electronic document format that provides a standard structure with which to report quality measure data to organizations that will analyze and interpret the data. The Release 3 IG is consistent with the CDA, and Category I is an individual-patient-level quality report. The Release 3 IG includes updates to align with the Quality Data Model version 4.1.2; incorporates appropriate QRDA Category I Release 2 (R2) DSTU comments that were considered as New Feature Requests; and updates of the QRDA I R1 DSTU Release 3 templates to align with the C-CDA R2 templates where applicable.

- Errata to the HL7 Implementation Guide for CDA® Release 2: Quality Reporting Document Architecture – Category III, DSTU Release 1 (US Realm), September 2014.

URL: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=286. Access requires a "user account" and a license agreement. There is no monetary cost for a user account and license agreement. The DSTU package must be downloaded in order to access the errata.

Summary: The September 2014 Errata reflects updates for the implementation of QRDA Category I consistent with the Quality Data Model-based Health Quality Measures Format Release 2.1, an incremental version of harmonized clinical quality measure and CDS standards.

- HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use, Release 2.1, Volumes 1 (Introductory Material) and 2 (Templates and Supporting Material).

URL:

http://www.hl7.org/documentcenter/public/standards/dstu/CDAR2_IG_CCDA_CLINNOTES_R1_DSTUR2.1_2015AUG.zip. Access requires a "user account" and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The Consolidated CDA (C-CDA) IG contains a library of CDA templates, incorporating and harmonizing previous efforts from HL7, IHE, and the Health Information Technology Standards Panel (HITSP). It represents harmonization of the HL7 Health Story guides, HITSP C32, related components of IHE Patient Care Coordination (IHE PCC), and Continuity of Care (CCD). The C-CDA Release 2.1 IG, in conjunction with the HL7 CDA Release 2 (CDA R2) standard, is to be used for implementing the following CDA documents and header constraints for clinical notes: Care Plan including Home Health Plan of Care, Consultation Note, CCD, Diagnostic Imaging Reports, Discharge Summary, History and Physical, Operative Note, Procedure Note, Progress Note, Referral Note, Transfer Summary, Unstructured Document, and Patient Generated Document (US Realm Header). The Consolidated CDA (C-CDA) Release 2.1 IG provides compatibility between Releases 2.0 and 1.1 by applying industry agreed-upon compatibility principles.

- HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1, Part 1: CDA R2 and Privacy Metadata Reusable Content Profile.

URL: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=354. Access requires a "user account" and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: This guide supports segmenting clinical records so that protected health information (PHI) can be appropriately shared as may be permitted by privacy policies or regulations.

- HL7 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5.

URL: http://www.cdc.gov/vaccines/programs/iis/technical-guidance/downloads/hl7guide-1-5-2014-11.pdf. This is a direct access link.

Summary: This document represents the collaborative effort of the American Immunization Registry Association and CDC to improve inter-system communication of immunization records. The guide is intended to facilitate exchange of immunization records between different systems.

- HL7 Version 2.5.1 Implementation Guide for Immunization Messaging (Release 1.5) – Addendum, July 2015.

URL: http://www.cdc.gov/vaccines/programs/iis/technical-guidance/hl7.html.

Summary: This addendum consolidates the HL7 Version 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5 information that clarifies the conformance requirements. This supplement does not specify additional requirements; it just clarifies existing ones. Value set requirements, general clarifications, and Immunization IG errata are also provided in this addendum.

- PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent Care, Inpatient and Ambulatory Settings, Release 2.0, April 21, 2015.

URL:

http://www.cdc.gov/nssp/documents/guides/syndrsurvmessagguide2_messagingguide_phn.pdf. This is a direct access link.

Summary: This document represents the collaborative effort of the International Society for Disease Surveillance, CDC, and NIST to specify a national electronic messaging standard that enables disparate health care applications to submit or transmit administrative and clinical data for public health surveillance and response. The scope of the guide is to provide guidelines for

sending HL7 v.2.5.1 compliant messages from emergency department, urgent and ambulatory care, and inpatient settings to public health authorities.

- Erratum to the CDC PHIN 2.0 Implementation Guide, August 2015; Erratum to the CDC PHIN 2.0 Messaging Guide, April 2015 Release for Syndromic Surveillance: Emergency Department, Urgent Care, Inpatient and Ambulatory Care Settings.

URL: http://www.cdc.gov/nssp/documents/guides/erratum-to-the-cdc-phin-2.0-implementation-guide-august-2015.pdf. This is a direct access link.

Summary: This document contains erratum and conformance clarifications for the PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent Care, Inpatient and Ambulatory Setting, Release 2.0. Value set requirements and errata are also provided in the addendum.

- HL7 CDA© Release 2 Implementation Guide: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, DSTU Release 1.1, Volumes 1 (Introductory Material) and 2 (Templates and Supporting Material).

URL: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=398. Access requires a "user account" and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: As ambulatory health care providers adopt modern EHR systems, the opportunity to automate cancer registry reporting from ambulatory health care provider settings is also increasing and becoming more feasible. This document provides clear and concise specifications for electronic reporting form ambulatory health care provider EHR systems to public health central cancer registries using the HL7 CDA based standards. This document is designed to

guide EHR vendors and public health central cancer registries in the implementation of standardized electronic reporting.

- IHE IT Infrastructure Technical Framework Volume 2b (ITI TF-2b).

URL: http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Rev7-0_Vol2b_FT_2010-08-10.pdf. This is a direct access link.

Summary: This document defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of medical information to support ongoing patient care. The IHE IT Infrastructure Technical Framework identifies a subset of functional components of the health care enterprise, called "IHE actors," and specified their interactions in terms of a set of coordinated, standards-based transactions. Volume 2b corresponds to transactions [ITI-29] through [ITI-57].

- HL7 Implementation Guide for CDA® Release 2 – Level 3: Healthcare Associated Infection Reports, Release 1, U.S. Realm.

URL: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=20. Access requires a "user account" and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: This document specifies a standard for electronic submission of health care associated infection reports (HAI) to the National Healthcare Safety Network of the CDC. This document defines the overall approach and method of electronic submission and develops constraints defining specific HAI report types.

- HL7 Implementation Guide for CDA® Release 2: National Health Care Surveys (NHCS), Release 1 - US Realm, HL7 Draft Standard for Trial Use, Volumes 1 (Introductory Material) and 2 (Templates and Supporting Material), December 2014.

URL: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=385. Access requires a "user account" and license agreement. There is no monetary cost for a user account and license agreement.

Summary: The HL7 Implementation Guide for CDA Release 2: National Health Care Surveys (NHCS), Release 1 - US Realm provides a standardized format for implementers to submit data to fulfill requirements of the Centers for Disease Control and Prevention/National Center for Health Statistics/National Health Care Surveys. This IG supports automatic extraction of the data from a provider's EHR system or data repository. The data are collected through three surveys of ambulatory care services in the United States: the National Ambulatory Medical Care Survey with information from physicians and two national hospital care surveys: the National Hospital Ambulatory Medical Care Surveys and the National Hospital Care Survey with data from hospital emergency and outpatient departments.

Vocabulary standards for representing electronic health information – 45 CFR 170.207

- IHTSDO SNOMED CT®, U.S. Edition, September 2015 Release.

URL: http://www.nlm.nih.gov/research/umls/Snomed/us_edition.html. Access requires a user account and license agreement. There is no monetary cost for a user account and license agreement.

Summary: Systemized Nomenclature of Medicine – Clinical Terms (SNOMED CT®) is a comprehensive clinical terminology, originally created by the College of American Pathologists and, as of April 2007, owned, maintained, and distributed by the International Health Terminology Standards Development Organisation. SNOMED CT® improves the recording of information in an EHR system and facilitates better communication, leading to improvements in the quality of care.

- Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.52, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc.

URL: http://loinc.org/downloads. Access requires registration, a user account, and license agreement. There is no monetary cost for registration, a user account, and license agreement.

Summary: LOINC® was initiated in 1994 by the Regenstrief Institute and developed by Regenstrief and the LOINC® committee as a response to the demand for electronic movement of clinical data from laboratories that produce the data to hospitals, provider's offices, and payers who use the data for clinical care and management purposes. The scope of the LOINC® effort includes laboratory and other clinical observations. The LOINC® database facilitates the exchange and pooling of results for clinical care, outcomes management, and research.

- RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine, September 8, 2015 Release.

URL: http://www.nlm.nih.gov/research/umls/rxnorm/docs/rxnormfiles.html. Access requires a user account and license agreement. There is no monetary cost for a user account and license agreement.

Summary: RxNorm provides normalized names for clinical drugs and links its names to many of the drug vocabularies commonly used in pharmacy management and drug interaction software. By providing links between vocabularies commonly used in pharmacy management and drug interaction software, RxNorm can mediate messages between systems not using the same software and vocabulary. RxNorm now includes the National Drug File – Reference Terminology (NDF-RT) from the Veterans Health Administration, which is used to code clinical drug properties, including mechanism of action, physiologic effect, and therapeutic category.

- HL7 Standard Code Set CVX—Vaccines Administered, updates through August 17, 2015.

URL: http://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=cvx. This is a direct access link.

Summary: CDC's National Center of Immunization and Respiratory Diseases developed and maintains HL7 Table 0292, Vaccine Administered (CVX). CVX includes both active and inactive vaccines available in the U.S. CVX codes for inactive vaccines allow transmission of historical immunization records; when paired with a manufacturer (MVX) code, the specific trade named vaccine may be indicated.

- National Drug Code Directory (NDC) – Vaccine NDC Linker, updates through August 17, 2015.

URL: http://www2a.cdc.gov/vaccines/iis/iisstandards/ndc_tableaccess.asp. This is a direct access link.

Summary: The Drug Listing Act of 1972 requires registered drug establishments to provide the FDA with a current list of all drugs manufactured, prepared, propagated, compounded, or processed by it by commercial distribution. Drug products are identified and reported using a unique, three-segment number, called the National Drug Code (NDC), which services as the universal product identifier for drugs. This standard is limited to the NDC vaccine codes identified by CDC at the URL provided.

- CDC Race and Ethnicity Code Set Version 1.0.

URL: http://www.cdc.gov/phin/resources/vocabulary/index.html. The code set can be accessed through this link.

Summary: The CDC has prepared a code set for use in coding race and ethnicity data. This code set is based on current federal standards for classifying data on race and ethnicity, specifically the minimum race and ethnicity categories defined by the U.S. Office of Management and Budget (OMB) and a more detailed set of race and ethnicity categories maintained by the U.S. Bureau of the Census (BC). The main purpose of the code set is to facilitate use of federal standards for classifying data on race and ethnicity when these data are exchanged, stored, retrieved, or analyzed in electronic form. At the same time, the code set can be applied to paper-based record systems to the extent that these systems are used to collect, maintain, and report data on race and ethnicity in accordance with current federal standards.

- Request for Comments (RFC) 5646, "Tags for Identifying Languages."

URL: http://www.rfc-editor.org/info/rfc5646. This is a direct access link.

Summary: RFC 5646 describes the structure, content, construction, and semantics of language tags for use in cases where it is desirable to indicate the language used in an information object. It also describes how to register values for use in language tags and the creation of user-defined extensions for private interchange.

- International Telecommunication Union E.123: Notation for national and international telephone numbers, e-mail addresses and web addresses.

URL: http://www.itu.int/rec/T-REC-E.123-200102-I/e. This is a direct access link.

Summary: This standard applies specifically to the printing of national and international telephone numbers, electronic mail addresses and Web addresses on letterheads, business cards, bills, etc. Regard has been given to the printing of existing telephone directories. The standard notation for printing telephone numbers, E-mail addresses and Web addresses helps to reduce difficulties and errors, since this address information must be entered exactly to be effective.

- International Telecommunication Union E.164: The international public telecommunication numbering plan.

URL: http://www.itu.int/rec/T-REC-E.164-201011-I/en. This is a direct access link.

Summary: Recommendation ITU-T E.164 provides the number structure and functionality for the five categories of numbers used for international public telecommunication: geographic areas, global services, Networks, groups of countries (GoC) and resources for trials. For each of the categories, it details the components of the numbering structure and the digit analysis required to successfully route the calls.

- Crosswalk: Medicare Provider/Supplier to Healthcare Provider Taxonomy (updated April 2, 2015).

URL: https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/MedicareProviderSupEnroll/Downloads/TaxonomyCrosswalk.pdf. This is a direct access link.

Summary: This crosswalk links the types of providers and suppliers who are eligible to apply for enrollment in the Medicare program with the appropriate Healthcare Provider Taxonomy Codes. This crosswalk includes the Medicare Specialty Codes for those provider/supplier types who have Medicare Specialty Codes. The Healthcare Provider Taxonomy Code Set is available from the Washington Publishing Company (www.wpc-edi.com) and is maintained by the National Uniform Claim Committee (www.nucc.org).

- Public Health Data Standards Consortium Source of Payment Typology Code Set, Version 5.0.

URL: http://www.phdsc.org/standards/pdfs/SourceofPaymentTypologyVersion5.0.pdf. This is a direct access link.

Summary: The Source of Payment Typology was developed to create a standard for reporting payer type data that will enhance the payer data classification; it is also intended for use by those collecting data, or analyzing healthcare claims information. The Payment Typology can be used by any analyst who wishes to code source of payment data, including analysts who code administrative or claims data, survey data, clinical trials data, or any other dataset containing this type of data element.

- The Unified Code of Units of Measure, Revision 1.9.

URL: http://unitsofmeasure.org/trac/. This is a direct access link. The codes can be viewed in html or xml.

Summary: The Unified Code of Units of Measure is a code system intended to include all units of measures being contemporarily used in international science, engineering, and business. The purpose is to facilitate unambiguous electronic communication of quantities together with units.

- HL7 Version 3 (V3) Normative Edition, 2015, AdminstrativeGender Value Set and NullFlavor.

URL: http://www.hl7.org/documentcenter/public_temp_369DCAB9-1C23-BA17-0CAF31D63E2D1A3E/standards/vocabulary/vocabulary_tables/infrastructure/vocabulary/vs_AdministrativeGender.html; and http://www.hl7.org/documentcenter/public_temp_369DCAB9-1C23-BA17-0CAF31D63E2D1A3E/standards/vocabulary/vocabulary_tables/infrastructure/vocabulary/vs_NullFlavor.html. These are direct access links. Compliance with a license agreement is required.

Summary: These HL7 Version 3 (V3) Standard Value Sets for administrativegender and NullFlavor provide means for coding birth sex and nullFlavors.

Standards for health information technology to protect electronic health information created, maintained, and exchanged – 45 CFR 170.210

- Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2, October 8, 2014.

URL: http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf. This is a direct access link.

Summary: Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules, specifies the security requirements that are to be satisfied by the cryptographic module utilized within a security system protecting sensitive information within computer and telecommunications systems. The standard provides four increasing qualitative levels of security that are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed.

- FIPS PUB 180-4, Secure Hash Standard, 180-4 (August 2015).

URL: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf. This is a direct access link.

Summary: This standard specifies secure hash algorithms - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256 - for computing a condensed representation of electronic data (message). Secure hash algorithms are typically used with other cryptographic algorithms, such as digital signature algorithms and keyed-hash message authentication codes, or in the generation of random numbers (bits).

- ASTM E2147-01 (Reapproved 2013) Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems, approved March 1, 2013.

URL: http://www.astm.org/Standards/E2147.htm. This is a direct access link. However, a fee is required to obtain a copy of the standard.

Summary: This specification describes the security requirements involved in the development and implementation of audit and disclosure logs used in health information systems. It specifies how to design an access audit log to record all access to patient identifiable information maintained in computer systems, and includes principles for developing policies, procedures, and functions of health information logs to document all disclosure of confidential health care information to external users for use in manual and computer systems. This specification provides for two main purposes, namely: to define the nature, role, and function of system access audit logs and their use in health information systems as a technical and procedural tool to help provide security oversight; and to identify principles for establishing a permanent record of disclosure of health information to external users and the data to be recorded in maintaining it.

VI. Collection of Information Requirements

Under the Paperwork Reduction Act of 1995 (PRA), agencies are required to provide 60-day notice in the **Federal Register** and solicit public comment on a proposed collection of information before it is submitted to the Office of Management and Budget for review and approval. In order to fairly evaluate whether an information collection should be approved by the Office of Management and Budget, section 3506(c)(2)(A) of the PRA requires that we solicit comment on the following issues:

1. Whether the information collection is necessary and useful to carry out the proper functions of the agency;
2. The accuracy of the agency's estimate of the information collection burden;
3. The quality, utility, and clarity of the information to be collected; and
4. Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

Under the PRA, the time, effort, and financial resources necessary to meet the information collection requirements referenced in this section are to be considered. We sought comment on proposed PRA requirements in the Proposed Rule (80 FR 16893-16895).

Abstract

Under the ONC Health IT Certification Program, accreditation organizations that wish to become the ONC-Approved Accreditor (ONC-AA) must submit certain information, organizations that wish to become an ONC-ACB must submit the information specified by the application requirements, and ONC-ACBs must comply with collection and reporting requirements, records retention requirements, and submit annual surveillance plans and annually report surveillance results.

In the Permanent Certification Program final rule (76 FR 1312-14), we solicited public comment on each of the information collections associated with the requirements described above (and included in regulation at 45 CFR 170.503(b), 170.520, and 170.523(f), (g), and (i), respectively). In the 2014 Edition final rule (77 FR 54275-76), we sought comment on these collection requirements again and finalized an additional requirement at § 170.523(f)(8) for ONC-ACBs to report to ONC a hyperlink with each EHR technology they certify that provides the public with the ability to access the test results used to certify the EHR technology. These collections of information were approved under OMB control number 0955-0013 (previous OMB control number 0990-0378).

In the Proposed Rule, we estimated less than 10 annual respondents for all of the regulatory "collection of information" requirements under Part 170 of Title 45, including those previously approved by OMB and proposed in the Proposed Rule (80 FR 16894). The "collection of information" requirements that apply to the ONC-Approved Accreditor (ONC-

AA) are found in § 170.503(b). The "collection of information" requirements that apply to the ONC-ACBs are found in § 170.520; § 170.523(f)(1) and (2), (g), (i), and (o); and § 170.540(c). As stated in the Proposed Rule, we estimated the number of respondents for § 170.503(b) (applicants for ONC-AA status) at two based on past selection processes for the ONC-AA, which have included no more than two applicants. As also stated in the Proposed Rule, we anticipate that there will be three ONC-ACBs participating in the ONC Health IT Certification Program as this is the current number of ONC-ACBs. Further, since the establishment of the ONC Health IT Certification Program in 2010, ONC has never had more than six applicants for ONC-ACB or ONC-ATCB status or selected more than six ONC-ACBs or ONC-ATCBs.[182]

We concluded that the regulatory "collection of information" requirements under the ONC Health IT Certification Program described above are not subject to the PRA under 5 CFR 1320.3(c). We welcomed comments on this conclusion and the supporting rationale on which it was based.

Comments. We received one comment suggesting that the time we estimated for proposed ONC-ACB surveillance activities may be underestimated in terms of reviewing surveillance guidance, developing plans, and finalizing surveillance results for submission.

Response. We agree with the commenter that our time estimate for surveillance-related activities was an underestimation. We have provided a new estimate as part of the regulatory impact statement.

We continue to estimate fewer than10 respondents for all of the regulatory "collection of information" requirements under Part 170 of Title 45. Accordingly, the "collection of information" requirements/burden that are associated with this final rule are not subject to the

[182] See also: http://www.healthit.gov/policy-researchers-implementers/authorized-testing-and-certifications-bodies and http://www.healthit.gov/policy-researchers-implementers/certification-bodies-testing-laboratories.

PRA under 5 CFR 1320.3(c).

VII. Regulatory Impact Statement

A. Statement of Need

This final rule is being published to adopt the 2015 Edition. Certification criteria and associated standards and implementation specifications would be used to test and certify health IT in order to make it possible for EPs, eligible hospitals, and CAHs to adopt and implement health IT that can be used to meet the CEHRT definition. EPs, eligible hospitals, and CAHs who participate in the EHR Incentive Programs are required by statute to use CEHRT.[183]

The certification criteria and associated standards and implementation specifications would also support the certification of more types of health IT and health IT that supports care and practice settings beyond the scope of the EHR Incentive Programs.

The adoption and implementation of health IT certified to the 2015 Edition promotes interoperability in support of a nationwide health information infrastructure and improves health care quality, safety and efficiency consistent with the goals of the HITECH Act.

B. Overall Impact

We have examined the impact of this final rule as required by Executive Order 12866 on Regulatory Planning and Review (September 30, 1993), Executive Order 13563 on Improving Regulation and Regulatory Review (February 2, 2011), the Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*), section 202 of the Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1532), and Executive Order 13132 on Federalism (August 4, 1999).

[183] Section 1848(o) of the Social Security Act.

1. Executive Orders 12866 and 13563 – Regulatory Planning and Review Analysis

Executive Orders 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). A regulatory impact analysis (RIA) must be prepared for major rules with economically significant effects ($100 million or more in any 1 year). OMB has determined that this final rule is an economically significant rule as we have estimated the costs to develop and prepare health IT to be tested and certified may be greater than $100 million per year.

a. Costs

This final rule adopts standards, implementation specifications, and certification criteria that establish the capabilities that health IT would need to demonstrate to be certified to the 2015 Edition. Our analysis focuses on the direct effects of the provisions of this final rule – the costs incurred by health IT developers to develop and prepare health IT to be tested and certified in accordance with the certification criteria (and the standards and implementation specifications they include) adopted by the Secretary. That is, we focus on the technological development and preparation costs necessary for health IT already certified to the 2014 Edition to upgrade to the proposed 2015 Edition and for, in limited cases, developing and preparing a new Health IT Module to meet the 2015 Edition. The costs for the testing and certification of health IT to the 2015 Edition were captured in the regulatory impact analysis of the Permanent Certification Program final rule as we discuss in more detail below (VIII.B.1.a.iii "Testing and Certification Costs for the 2015 Edition"). In this final rule, we have also included estimated costs for complying with new and revised Principles of Proper Conduct for ONC-ACBs.

Because the costs that EPs, eligible hospitals, and CAHs would incur in adopting and implementing (including training, maintenance, and any other ongoing costs) health IT certified to the 2015 Edition is overwhelmingly attributable to the EHR Incentive Programs Stage 3 and Modifications final rule (published elsewhere in this issue of the **Federal Register**), and would not be incurred in the absence of such rulemaking, such costs are not within the scope of the analysis of this final rule; similarly, any benefits that are contingent upon adoption and implementation would be attributable to CMS's rulemaking.[184] We also note that this final rule does not impose the costs cited as compliance costs, but rather as investments which health IT developers voluntarily take on and may expect to recover with an appropriate rate of return.

i. Development and Preparation Costs for the 2015 Edition

The development and preparation costs we estimate are derived through a health IT developer per criterion cost. In simple terms, we estimate: (1) how many health developers will prepare and develop products against the certification criteria; (2) how many products they will develop; and (3) what it will likely cost them to develop and prepare those products to meet the certification criteria.

Comments. Several commenters expressed concern with the estimated costs and developer hours in the Proposed Rule, stating they were significantly underestimated. However, one commenter stated the average cost estimate for patient health information capture was significantly overestimated. One commenter stated that the developer hour estimates do not

[184] ONC administers a voluntary certification program that provides no incentives for certification. Therefore, to the extent that providers' implementation and adoption costs are attributable to CMS's rulemaking, health IT developers' preparation and development costs would also be attributable to that rulemaking (because all of the costly activities are, directly or indirectly, incentivized by CMS's payment structure). However, a professional organization or other such entity could also require or promote certification, thus generating costs and benefits that are attributable to this final rule. To avoid giving the misleading impression that such effects equal zero, we present in this RIA a subset of the relevant impacts—a quantification of costs that are incurred by health IT developers and a qualitative discussion of benefits. (The missing portion of the subset is providers' implementation and adoption costs.)

appear to be derived from data reported by health IT developers or consulting companies and recommends a total economic impact assessment by a 3rd party is needed.

Response. As noted in the Proposed Rule, we are not aware of an available independent study (e.g., a study capturing the preparation efforts and costs to develop and Health IT Modules to meet the requirements of the 2014 Edition) that we could rely upon as a basis for estimating the efforts and costs required to develop and prepare health IT to meet the 2015 Edition. We based our cost estimates in the Proposed Rule in part on burden hour estimates provided by the Electronic Health Record Association (EHRA) (a health IT developer association) as well as internal estimates. For this final rule, we have once again relied on burden hour estimates provided by the EHRA in response to the Proposed Rule and internal estimates.

We have also once again generally used the EHRA estimates as a basis for our high estimates. We have used the EHRA estimates in this manner because of the uncertain reliability of the information. It is our understanding that these estimates were based on a survey of EHRA's members. It is unclear how many of EHRA's members responded and how each member arrived at their estimates. Further, we cannot rely on these estimates as being generated from an independent, unbiased source because EHRA members must, in some respects, substantiate the costs and fees they charge providers for their certified health IT. We do note, however, that we have also used the EHRA estimates to significantly increase our low estimates.

Based on the estimates provided by the EHRA, by not adopting the 14 proposed certification criteria identified in Table 2 of this final rule and certain other functionality and standards, we have reduced the estimated burden of the 2015 Edition by over 40,000 burden hours per health IT developer. The 14 criteria that were not adopted saved over 25,000 burden hours. An additional 15,000 burden hours were saved through not adopting certain functionality

and standards such as user response "tracking" for clinical decision support and drug-drug, drug-allergy interaction checks, a formulary benefit standard, a standard for recording smoking status, a standard for CPOE laboratory orders, and proposals for certain e-prescribing and C-CDA conformance.

Certification Criteria

We have divided the certification criteria into three categories, each with its own table below. Table 11 is for the new and revised certification criteria associated with the EHR Incentive Programs Stage 3 CEHRT definition and objectives and measures. Table 12 is for the unchanged certification criteria associated with the EHR Incentive Programs Stage 3 CEHRT definition and objectives and measures. These tables also include certification criteria that are mandatory and conditional certification requirements, such as "safety-enhanced design," and "quality management system," "accessibility-centered design," and privacy and security certification criteria as certified Health IT Modules certified to these criteria would be used to meet the CEHRT definition under the EHR Incentive Programs.[185] Table 13 is for all other certification criteria ("Independent Criteria"). We have taken this approach because, based on available data, we can more accurately estimate the number of health IT developers that may develop and prepare Health IT Modules for certification to certification criteria associated with the EHR Incentive Programs.

Health IT Developers and Number of Health IT Modules

New and Revised Stage 3 Criteria

We derive our estimates for the number of health IT developers by beginning with the number of Health IT developers certified to each of the 2014 Edition certification criteria as

[185] Please see section III.A for explanation of the terms "mandatory" and "conditional" as they apply to certification criteria and the certification of a Health IT Module.

identified in CHPL data from November 10, 2014. For the new and revised Stage 3 Criteria that correspond to 2014 Edition certification criteria, we have reduced the number of Health IT developers by 30% from the number that certified against the 2014 Edition. We have done this because we have found a 22% drop in the number of health IT developers that certified technology against the 2014 Edition versus the 2011 Edition. We believe that as both interoperability requirements increase by edition and certain health IT developers gain more market share through competition and acquisition of other health IT developers, there will be an even greater drop in the number of health IT developers that seek certification to the 2015 Edition.

We estimate 2.5 products per health IT developer for each new and revised "Stage 3" criterion. We reached this estimate based both on the number of unique[186] certified products listed on the CHPL as of November 10, 2014 divided by the number of health IT developers certified and stakeholder feedback on our Voluntary Edition proposed rule (79 FR 54474).

We note that these estimates included any new health IT developers.

Unchanged Stage 3 Criteria

For unchanged "Stage 3" criteria, we estimate 5 new health IT developers, each with 1 product. We have attempted to establish a burden estimate for each criterion assuming a health IT developer would be in the same position as a health IT developer that sought certification to the 2011 or 2014 Edition as these 2015 certification criteria are unchanged as compared to those same 2011 and 2014 Edition certification criteria. We do not anticipate more than 5 new health IT developers to certify to these criteria for the market attrition reasons mentioned above. We

[186] We attempted to discern how many Complete EHRs and Health IT Modules were used that would not constitute a newer version of the same technology.

note for health IT developers that have had products previously certified to the 2014 Edition version of these criteria, we estimate no new costs.

Independent Criteria

For the Independent Criteria, we have only estimated the development and preparation of one Health IT Module to meet these criteria. The Independent Criteria are not currently associated with the EHR Incentive Programs or another HHS payment program. Therefore, we continue to have no reliable basis on which to estimate how many developers and products will be certified to these criteria. We do not include these estimated costs in our overall cost estimate for this final rule.

Average Development and Preparation Hours

Our estimated average development hours are based on feedback we received in response to the RIA we completed for the Proposed Rule and internal estimates for criteria where there is no external data to validly rely upon. As noted above, we have generally used estimates from the Electronic Health Record Association as a basis for our high estimates, where applicable. We have accounted for the reduced burden hours related to functionality and standards not adopted (e.g., "CPOE – laboratory," "clinical decision support," and "smoking status," certification criteria).

We have also attempted to capture developmental synergies where development to a vocabulary and/or content exchange standard can significantly reduce a health IT developer's burden when certifying to multiple certification criteria that reference the same vocabulary or content exchange standard. For example, the "transitions of care," "clinical information reconciliation and incorporation," "data export," "view, download, and transmit to 3rd party," "application access – data category request," and "application access – all data request"

certification criteria included the same content exchange standard and many, if not all, the same vocabulary standards. Based on health IT products certified to the 2014 Edition, we expect health IT developers to certify their products to many or all of these criteria. This will create developmental efficiencies and reduced burden. Similarly, a health IT developer preparing a product for certification to the "social, psychological, and behavioral data" criterion would find synergies in meeting all the measures now included in the criterion as they all rely on LOINC®. We note that our estimates also take into account added burden such as with the Direct criteria, which is a result of adoption of a newer version of the standard and other included interoperability requirements.

Estimated Health IT Developers and Development Hours Per Criterion

Table 11. Estimated Health IT Developers and Development and Preparation Hours for the 2015 Edition – New and Revised Criteria Associated with the EHR Incentive Programs Stage 3 ("Stage 3 Criteria")

Item #	CFR Text	Certification Criterion Name	Number of Health IT Developers who Develop Product(s) for Certification to Criterion	Hourly Development Effort by Health IT Developer	
				Low Avg	High Avg
1	§ 170.315(a)(5)	Demographics	268.8	1200	2000
2	§ 170.315(a)(6)	Problem List	256.9	50	100
3	§ 170.315(a)(9)	Clinical Decision Support	235.2	300	400
4	§ 170.315(a)(12)	Family Health History	250	50	100
5	§ 170.315(a)(13)	Patient-specific Education Resources	249.2	300	400
6	§ 170.315(a)(14)	Implantable Device List	90	700	2200
7	§ 170.315(b)(1)	Transitions of Care	242.9	3000	4000
8	§ 170.315(b)(2)	Clinical Information Reconciliation and Incorporation	224	500	600
9	§ 170.315(b)(3)	Electronic Prescribing	224.7	1600	2300
10	§ 170.315(b)(6)	Data Export	228.9	600	1600
11	§ 170.315(c)(1)	CQMs – record and export	246.4	600	800
12	§ 170.315(c)(2)	CQMs – import and calculate	246.4	600	800
13	§ 170.315(c)(3)	CQMs – report	246.4	600	800
14	§ 170.315(d)(2)	Auditable Events and Tamper-resistance	272.3	50	100
15	§ 170.315(d)(8)	Integrity	312.2	50	100
16	§ 170.315(d)(9)	Trusted Connection	242	100	200

17	§ 170.315(d)(10)	Auditing Actions on Health Information	242	100	200
18	§ 170.315(e)(1)	View, Download, and Transmit to 3rd party	256.2	1300	2000
19	§ 170.315(e)(2)	Secure Messaging	246.4	100	200
20	§ 170.315(e)(3)	Patient Health Information Capture	88.9	500	800
21	§ 170.315(f)(1)	Transmission to Immunization Registries	220.5	1000	1600
22	§ 170.315(f)(2)	Transmission to Public Health Agencies—syndromic surveillance	100	600	800
23	§ 170.315(f)(4)	Transmission to Cancer Registries	22.4	800	1000
24	§ 170.315(f)(5)	Transmission to Public Health Agencies – electronic case reporting	21	600	800
25	§ 170.315(f)(6)	Transmission to Public Health Agencies – antimicrobial use and resistance reporting	21	1000	1400
26	§ 170.315(f)(7)	Transmission to Public Health Agencies – health care surveys	21	1000	1400
27	§ 170.315(g)(1)	Automated Numerator Recording	113.4	800	1200
28	§ 170.315(g)(2)	Automated Measure Calculation	264.6	1000	1600
29	§ 170.315(g)(3)	Safety-enhanced Design	266	300	400
30	§ 170.315(g)(4)	Quality Management System	401.8	50	160
31	§ 170.315(g)(5)	Accessibility-Centered Design	401.8	50	100
32	§ 170.315(g)(6)	Consolidated CDA Creation Performance	242	400	900
33	§ 170.315(g)(7)	Application Access – Patient Selection	242	300	400
34	§ 170.315(g)(8)	Application Access – Data Category Request	242	300	400
35	§ 170.315(g)(9)	Application Access – All Data Request	242	300	400
36	§ 170.315(h)(1)	Direct Project	140	800	1100
37	§ 170.315(h)(2)	Direct Project, Edge Protocol, and XDR/XDM	70	800	1100

Table 12. Estimated Health IT Developers and Development and Preparation Hours for Proposed Unchanged Certification Criteria – Criteria Associated with the EHR Incentive Programs Stage 3 ("Stage 3 Criteria")

Item #	CFR Text	Certification Criterion Name	Number of Health IT Developers who Develop Product(s)	Hourly Development Effort by Health IT Developer	
				Low Avg	High Avg

			for Certification to Criterion		
1	§ 170.315(a)(1)	CPOE – medications	5	50	100
2	§ 170.315(a)(2)	CPOE – laboratory	5	50	100
3	§ 170.315(a)(3)	CPOE – diagnostic imaging	5	50	100
4	§ 170.315(a)(4)	DD/DAI Checks for CPOE	5	50	100
5	§ 170.315(a)(8)	Medication List	5	50	100
6	§ 170.315(a)(9)	Medication Allergy List	5	50	100
7	§ 170.315(a)(10)	Drug-formulary and Preferred Drug List Checks	5	50	100
8	§ 170.315(a)(11)	Smoking Status	5	50	100
9	§ 170.315(d)(1)	Authentication, Access Control, Authorization	5	50	100
10	§ 170.315(d)(3)	Audit Report(s)	5	50	100
11	§ 170.315(d)(4)	Amendments	5	50	100
12	§ 170.315(d)(5)	Automatic Access Time-out	5	50	100
13	§ 170.315(d)(6)	Emergency Access	5	50	100
14	§ 170.315(d)(7)	End-User Device Encryption	5	50	100
15	§ 170.315(f)(3)	Transmission to Public Health Agencies – reportable laboratory tests and values/results	5	400	600

Table 13. Estimated Development and Preparation Hours for the 2015 Edition – Criteria Not Associated with the EHR Incentive Programs Stage 3 ("Independent Criteria")

Item #	CFR Text	Certification Criterion Name	Hourly Development Effort by Health IT Developer	
			Low Avg	High Avg
1	§ 170.315(a)(15)	Social, Psychological, and Behavioral Data	800	1000
2	§ 170.315(b)(4)	Common Clinical Data Set Summary Record – Create	1600	2200
3	§ 170.315(b)(5)	Common Clinical Data Set Summary Record – Receive	1600	2200
4	§ 170.315(b)(7)	Data Segmentation for Privacy – send	800	1300
5	§ 170.315(b)(8)	Data Segmentation for Privacy – receive	800	1300
6	§ 170.315(b)(9)	Care Plan	700	1000
7	§ 170.315(c)(4)	CQMs – filter	1000	1500
8	§ 170.315(d)(9)	Accounting of Disclosures	400	600

Health IT Developer Hourly Cost and Cost Range

We have based the effort levels on the hours necessary for a software developer to develop and prepare the health IT for testing and certification. These hours are identified in Tables 11-13 above.

The U.S. Department of Labor, Bureau of Labor Statistics estimates that the median hourly wage for a software developer is $45.92.[187] We have also calculated the costs of an employee's benefits by assuming that an employer expends thirty-six percent (36%) of an employee's hourly wage on benefits for the employee. We have concluded that a 36% expenditure on benefits is an appropriate estimate because it is the routine percentage used by HHS for contract cost estimates. We have rounded up the average software developer's wage with benefits to $63 per hour.

To calculate our cost estimates for each certification criterion in the tables below, we have multiplied both the average low and average high number of development and preparation hours in Tables 11-13 by $63. For tables 14, 15, and 16, dollar amounts are expressed in 2014 dollars.

Estimated Cost Per Criterion for Health IT Developers

Table 14. Total Development and Preparation Costs Per Criterion for Health IT Developers - 2015 Edition New and Revised Criteria Associated with the EHR Incentive Programs Stage 3 ("Stage 3 Criteria")

Item #	CFR Text	Certification Criterion Name	Average Cost Estimates ($)	
			Average Low ($)	Average High ($)
1	§ 170.315(a)(5)	Demographics	20,321,280	33,868,800
2	§ 170.315(a)(6)	Problem List	809,235	1,618,470
3	§ 170.315(a)(9)	Clinical Decision Support	4,445,280	5,927,040
4	§ 170.315(a)(12)	Family Health History	787,500	1,575,000
5	§ 170.315(a)(13)	Patient-specific Education Resources	4,709,880	6,279,840
6	§ 170.315(a)(14)	Implantable Device List	3,969,000	12,474,000
7	§ 170.315(b)(1)	Transitions of Care	45,908,100	61,210,800
8	§ 170.315(b)(2)	Clinical Information Reconciliation and Incorporation	7,056,000	8,467,200
9	§ 170.315(b)(3)	Electronic Prescribing	22,649,760	32,559,030
10	§ 170.315(b)(6)	Data Export	8,652,420	23,073,120
11	§ 170.315(c)(1)	CQMs – record and export	9,313,920	12,418,560
12	§ 170.315(c)(2)	CQMs – import and calculate	9,313,920	12,418,560
13	§ 170.315(c)(3)	CQMs – report	9,313,920	12,418,560

[187] http://www.bls.gov/oes/current/oes151132.htm

14	§ 170.315(d)(2)	Auditable Events and Tamper-resistance	857,745	1,715,490
15	§ 170.315(d)(8)	Integrity	983,430	1,966,860
16	§ 170.315(d)(9)	Trusted Connection	1,524,600	3,049,200
17	§ 170.315(d)(10)	Auditing Actions on Health Information	1,524,600	3,049,200
18	§ 170.315(e)(1)	View, Download, and Transmit to 3rd party	20,982,780	32,281,200
19	§ 170.315(e)(2)	Secure Messaging	1,552,320	3,104,640
20	§ 170.315(e)(3)	Patient Health Information Capture	2,800,350	4,480,560
21	§ 170.315(f)(1)	Transmission to Immunization Registries	13,891,500	22,226,400
22	§ 170.315(f)(2)	Transmission to Public Health Agencies—syndromic surveillance	3,780,000	5,040,000
23	§ 170.315(f)(4)	Transmission to Cancer Registries	1,128,960	1,411,200
24	§ 170.315(f)(5)	Transmission to Public Health Agencies – electronic case reporting	793,800	1,058,400
25	§ 170.315(f)(6)	Transmission to Public Health Agencies – antimicrobial use and resistance reporting	1,323,000	1,852,200
26	§ 170.315(f)(7)	Transmission to Public Health Agencies – health care surveys	1,323,000	1,852,200
27	§ 170.315(g)(1)	Automated Numerator Recording	5,715,360	8,573,040
28	§ 170.315(g)(2)	Automated Measure Calculation	16,669,800	26,671,680
29	§ 170.315(g)(3)	Safety-enhanced Design	5,027,400	6,703,200
30	§ 170.315(g)(4)	Quality Management System	1,265,670	4,050,144
31	§ 170.315(g)(5)	Accessibility-Centered Design	1,265,670	2,531,340
32	§ 170.315(g)(6)	Consolidated CDA Creation Performance	6,098,400	13,721,400
33	§ 170.315(g)(7)	Application Access – Patient Selection	4,573,800	6,098,400
34	§ 170.315(g)(8)	Application Access – Data Category Request	4,573,800	6,098,400
35	§ 170.315(g)(9)	Application Access – All Data Request	4,573,800	6,098,400
36	§ 170.315(h)(1)	Direct Project	7,056,000	9,702,000
37	§ 170.315(h)(2)	Direct Project, Edge Protocol, and XDR/XDM	3,528,000	4,851,000

Table 15. Total Development and Preparation Costs Per Criterion for Health IT Developers - 2015 Edition Unchanged Criteria Associated with the EHR Incentive Programs Stage 3 ("Stage 3 Criteria")

Item #	CFR Text	Certification Criterion Name	Average Cost Estimates ($)	
			Average Low ($)	Average High ($)
1	§ 170.315(a)(1)	CPOE – medications	15,750	31,500

2	§ 170.315(a)(2)	CPOE – laboratory	15,750	31,500
3	§ 170.315(a)(3)	CPOE – diagnostic imaging	15,750	31,500
4	§ 170.315(a)(4)	DD/DAI Checks for CPOE	15,750	31,500
5	§ 170.315(a)(8)	Medication List	15,750	31,500
6	§ 170.315(a)(9)	Medication Allergy List	15,750	31,500
7	§ 170.315(a)(10)	Drug-formulary and Preferred Drug List Checks	15,750	31,500
8	§ 170.315(a)(11)	Smoking Status	15,750	31,500
9	§ 170.315(d)(1)	Authentication, Access Control, Authorization	15,750	31,500
10	§ 170.315(d)(3)	Audit Report(s)	15,750	31,500
11	§ 170.315(d)(4)	Amendments	15,750	31,500
12	§ 170.315(d)(5)	Automatic Access Time-out	15,750	31,500
13	§ 170.315(d)(6)	Emergency Access	15,750	31,500
14	§ 170.315(d)(7)	End-User Device Encryption	15,750	31,500
15	§ 170.315(f)(3)	Transmission to Public Health Agencies – reportable laboratory tests and values/results	126,000	189,000

Table 16. Total Development and Preparation Costs Per Criterion – 2015 Edition Criteria Not Associated with the EHR Incentive Programs Stage 3 ("Independent Criteria")

Item #	CFR Text	Certification Criterion Name	Average Cost Estimates ($)	
			Average Low ($)	Average High ($)
1	§ 170.315(a)(15)	Social, Psychological, and Behavioral Data	50,400	63,000
2	§ 170.315(b)(4)	Common Clinical Data Set Summary Record – Create	100,800	138,600
3	§ 170.315(b)(5)	Common Clinical Data Set Summary Record – Receive	100,800	138,600
4	§ 170.315(b)(7)	Data Segmentation for Privacy – send	50,400	81,900
5	§ 170.315(b)(8)	Data Segmentation for Privacy – receive	50,400	81,900
6	§ 170.315(b)(9)	Care Plan	44,100	63,000
7	§ 170.315(c)(4)	CQMs – filter	63,000	94,500
8	§ 170.315(d)(9)	Accounting of Disclosures	25,200	37,800

ii. Overall Development and Preparation Costs Over a Four-year Period

We estimate the development and preparation costs over a four-year period because a four-year period aligns with our estimated publication date for a subsequent final rule (2015) and the year in which CMS proposes that participants in the EHR Incentive Programs must use health IT certified to the 2015 Edition (2018) (see the EHR Incentive Programs Stage 3 and Modifications final rule published elsewhere in this issue of the **Federal Register**).

In total, we estimate the overall costs to develop and prepare health IT for certification over a four-year period to be $260.44 million to $403.19 million, with a cost mid-point of approximately $331.82 million. Evenly distributed over calendar years 2015 through 2018, the cost range would be $65.11 million to $100.79 million per year with an annual cost mid-point of approximately $82.95 million. However, we project these costs to be unevenly distributed. We estimate the distribution as follows: 2015 (15%); 2016 (35%); 2017 (35%); and 2018 (15%). We reached this distribution based on these assumptions and information:

- We expect for health IT developers to spend the rest of the year preparing and developing their health IT to meet the 2015 Edition. We note that we lowered the percentage to 15% for 2015 from 25% in the Proposed Rule due to the later-than-anticipated publication date of this final rule. We redistributed the 10% over 2016 and 2017.
- We expect health IT developers to aggressively work in 2016 and 2017 to prepare and develop their health IT to meet the 2015 Edition as the compliance date for the EHR Incentive Programs CEHRT definition draws near (i.e., 2018) and because health IT certified to the 2015 Edition could be used in 2017 under the EHR Incentive Programs CEHRT definition finalized in the EHR Incentive Programs Stage 3 and Modifications final rule (published elsewhere in this issue of the **Federal Register**).
- We expect health IT developers to continue to prepare and develop health IT to the 2015 Edition in 2018 based on their approach to the 2014 Edition.

Table 17 below represents the costs attributable to this proposed rule distributed as discussed above. The dollar amounts expressed in Table 17 are expressed in 2014 dollars.

Table 17. Distributed Total 2015 Edition Development and Preparation Costs for Health IT Developers (4-year period) – Totals Rounded

Year	Ratio	Total Low Cost Estimate ($M)	Total High Cost Estimate ($M)	Total Average Cost Estimate ($M)
2015	15%	39.07	60.48	49.77
2016	35%	91.15	141.12	116.14
2017	35%	91.15	141.12	116.14
2018	15%	39.07	60.48	49.77
4-Year Totals		260.44	403.19	331.82

iii. Testing and Certification Costs for the 2015 Edition

In the RIA of the Permanent Certification Program final rule, we estimated the costs for testing and certification of technologies that would be used for providers to attempt to achieve EHR Incentive Programs Stages 1-3.[188] These costs were based on the requirements of the certification program and a two-year rulemaking cycle for the CEHRT definition and each EHR Incentive Programs stage. We believe the costs we attributed to testing and certification of technologies in support of EHR Incentive Programs Stage 2 in the Permanent Certification Program final rule would encompass the actual testing and certification of technologies to both the 2014 and 2015 Editions. This assessment is based on the number of technologies currently certified to the 2014 Edition and our projections in this proposed rule for the number of technologies that would likely be tested and certified to the 2015 Edition. Further, we note that the estimated costs in the Permanent Certification Program final rule included costs for surveillance of technologies and also estimated the costs for testing and certification above what we understand are the cost ranges charged by ONC-ACBs today.

iv. New and Revised Principles of Proper Conduct Estimated Costs

Costs to ONC-ACBs

[188] 76 FR 1318

We have estimated the costs associated with new and revised PoPC finalized in this final rule. For reporting requirements under 45 CFR 170.523(f), (m), and (n), we have used burden hour estimates provided in the Proposed Rule (80 FR 16893). For 45 CFR 170.523(i), we have increased the burden hours based on the quarterly reporting requirements and the nature of what must be reported. For 45 CFR 170.523(g) and (k), we have established burden hour estimates based on the number of certifications performed per year by ONC-ACBs.

We believe that an employee equivalent to the Federal Classification of GS-12 Step 1 could report the required information for 45 CFR 170.523(f), retain the records under 45 CFR 170.523(g), compile and submit surveillance results quarterly per 45 CFR 170.523(i), collect adaptations/updates quarterly per 45 CFR 170.523(m), and compile and submit complaints per 45 CFR 170.523(n). We believe that an employee equivalent to the Federal Classification of GS-14 Step 1 could verify health IT developers' compliance with 45 CFR 170.523(k). We have utilized the corresponding employee hourly rates for the locality pay area of Washington, D.C., as published by OPM, to calculate our cost estimates. We have also calculated the costs of the employee's benefits while completing the specified tasks. We have calculated these costs by assuming that an ONC-ACB expends thirty-six percent (36%) of an employee's hourly wage on benefits for the employee. We have concluded that a 36% expenditure on benefits is an appropriate estimate because it is the routine percentage used by HHS for contract cost estimates. Our cost estimates are expressed in Table 18 below and are expressed in 2015 dollars (rounded).

Table 18. Annual Costs for an ONC-ACB to Comply with New and Revised PoPC

Program Requirement	Employee Equivalent	Annual Burden Hours Per ONC-ACB	Employee Hourly Wage Rate ($)	Employee Benefits Hourly Cost ($)	Total Cost Per ONC-ACB ($)
45 CFR 170.523(f)	GS-12, Step 1	230	36.60	13.18	11,449.40

45 CFR 170.523(g)	GS-12, Step 1	1000	36.60	13.18	49,780
45 CFR 170.523(i)	GS-12, Step 1	80	36.60	13.18	3,982.40
45 CFR 170.523(k)	GS-14, Step 1	1000	51.43	18.51	69,940
45 CFR 170.523(m)	GS-12, Step 1	4	36.60	13.18	199.12
45 CFR 170.523(n)	GS-12, Step 1	4	36.60	13.18	199.12
Total					135,550.04

We estimate the total annual costs to be $406,650.12 based on three ONC-ACBs.

Costs to Health IT Developers

Certain new and revised PoPC create indirect costs on health IT developers, which we have attempted to estimate in this final rule below. We have estimated the burden hours to the extent possible. We have used the same cost factors as discussed above. We have estimated 402 health IT developers based on the highest estimated number of health IT developers we expect to be certified to a 2015 Edition certification criterion (see Table 11 above). Our cost estimates are expressed in Table 19 below and are expressed in 2015 dollars (rounded).

Table 19. Annual Costs for Health IT Developers to Comply with Transparency and Reporting Requirements

Program Requirement	**Employee Equivalent**	**Annual Burden Hours Per Health IT Developer**	**Employee Hourly Wage Rate**	**Employee Benefits Hourly Cost**	**Total Number of Health IT Developers**	**Total Cost ($M)**
45 CFR 170.523(k)	GS-14, Step 1	100	$51.43	$18.51	402	2.81
45 CFR 170.523(m)	GS-12, Step 1	8	$36.60	$13.18	402	.16
Total Costs						2.97

b. Benefits

As noted above, we expect that health IT developers will recover an appropriate rate of return for their investments in developing and preparing their health IT for certification to the 2015 Edition certification criteria adopted in this final rule. However, we do not have data available to quantify these benefits or other benefits that will likely arise from health IT developers certifying their health IT to the 2015 Edition.

We believe that there will be several significant benefits that may arise from this final rule for patients, health care providers, and health IT developers. The 2015 Edition continues to improve health IT interoperability through the adoption of new and updated standards and implementation specifications. For example, many adopted certification criteria include standards and implementation specifications for interoperability that directly support the EHR Incentive Programs, which include objectives and measures for the interoperable exchange of health information and for providing patients electronic access to their health information in structured formats. In addition, 2015 Edition certification criteria that support the collection of patient data that could be used to address health disparities would not only benefit patients, but the entire health care delivery system through improved quality of care. The 2015 Edition also supports usability and patient safety through new and enhanced certification requirements for health IT.

This final rule also makes the ONC Health IT Certification Program open and accessible to more types of health IT and for health IT that supports a variety of care and practice settings. This should benefit health IT developers, providers practicing in other care/practice settings, and consumers through the availability and use of certified health IT that includes capabilities that promote interoperability and enhanced functionality.

We note that, in general, these benefits will be realized only if health care providers actually adopt new technology. As discussed elsewhere in this RIA, we believe that such adoption—and thus the benefits noted in this section—would be overwhelmingly attributable to CMS's final rule.

2. Regulatory Flexibility Act (RFA)

The RFA requires agencies to analyze options for regulatory relief of small businesses if a rule has a significant impact on a substantial number of small entities.

The Small Business Administration (SBA) establishes the size of small businesses for federal government programs based on average annual receipts or the average employment of a firm. While health IT developers that pursue certification under the ONC Health IT Certification Program represent a small segment of the overall information technology industry, we believe that the entities impacted by this proposed rule most likely fall under the North American Industry Classification System (NAICS) code 541511 "Custom Computer Programming Services" specified in 13 CFR 121.201 where the SBA publishes "Small Business Size Standards by NAICS Industry." The SBA size standard associated with this NAICS code is set at $27.5 million in annual receipts[189] which "indicates the maximum allowed for a concern and its affiliates to be considered small entities."

Based on our analysis, we believe that there is enough data generally available to establish that between 75% and 90% of entities that are categorized under the NAICS code 541511 are under the SBA size standard, but note that the available data does not show how many of these entities will develop a health IT product that will be certified to the 2015 Edition

[189] The SBA references that annual receipts means "total income" (or in the case of a sole proprietorship, "gross income") plus "cost of goods sold" as these terms are defined and reported on Internal Revenue Service tax return forms. http://www.sba.gov/sites/default/files/files/Size_Standards_Table.pdf

under the ONC Health IT Certification Program. We also note that with the exception of aggregate business information available through the U.S. Census Bureau and the SBA related to NAICS code 541511, it appears that many health IT developers that pursue certification under the ONC Health IT Certification Program are privately held or owned and do not regularly, if at all, make their specific annual receipts publicly available. As a result, it is difficult to locate empirical data related to many of these health IT developers to correlate to the SBA size standard. However, although not correlated to the size standard for NAICS code 541511, we do have information indicating that over 60% of health IT developers that have had Complete EHRs and/or EHR Modules certified to the 2011 Edition have less than 51 employees.

We estimate that this final rule would have effects on health IT developers that are likely to pursue certification under the ONC Health IT Certification Program, some of which may be small entities. However, we believe that we have adopted the minimum amount of requirements necessary to accomplish our policy goals, including a reduction in regulatory burden and additional flexibility for the regulated community, and that no additional appropriate regulatory alternatives could be developed to lessen the compliance burden associated with this final rule. We note that this final rule does not impose the costs cited in the RIA as compliance costs, but rather as investments which these health IT developers voluntarily take on and may expect to recover with an appropriate rate of return. Accordingly, we do not believe that the final rule will create a significant impact on a substantial number of small entities. Additionally, the Secretary certifies that this final rule will not have a significant impact on a substantial number of small entities.

3. Executive Order 13132 - Federalism

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct requirement costs on state and local governments, preempts state law, or otherwise has federalism implications. Nothing in this final rule imposes substantial direct compliance costs on state and local governments, preempts state law or otherwise has federalism implications. We are not aware of any State laws or regulations that are contradicted or impeded by any of the standards, implementation specifications, or certification criteria that we have adopted.

4. Unfunded Mandates Reform Act of 1995

Section 202 of the Unfunded Mandates Reform Act of 1995 requires that agencies assess anticipated costs and benefits before issuing any rule whose mandates require spending in any one year of $100 million in 1995 dollars, updated annually for inflation. The current inflation-adjusted statutory threshold is approximately $144 million. This final rule will not impose an unfunded mandate on State, local, and tribal governments or on the private sector that will reach the threshold level.

OMB reviewed this final rule.

List of Subjects in 45 CFR Part 170

Computer technology, Electronic health record, Electronic information system, Electronic transactions, Health, Health care, Health information technology, Health insurance, Health records, Hospitals, Incorporation by reference, Laboratories, Medicaid, Medicare, Privacy, Reporting and recordkeeping requirements, Public health, Security.

For the reasons set forth in the preamble, 45 CFR subtitle A, subchapter D, part 170, is amended as follows:

PART 170 – HEALTH INFORMATION TECHNOLOGY STANDARDS, IMPLEMENTATION SPECIFICATIONS, AND CERTIFICATION CRITERIA AND CERTIFICATION PROGRAMS FOR HEALTH INFORMATION TECHNOLOGY

1. The authority citation for part 170 continues to read as follows:

Authority: 42 U.S.C. 300jj–11; 42 U.S.C. 300jj–14; 5 U.S.C. 552.

2. Amend § 170.102 by:

a. Removing the definitions for "Base EHR", "Certified EHR Technology", "Common MU Data Set", and "EHR Module"; and

b. Adding in alphanumeric order the definitions for "2014 Edition Base EHR", "2015 Edition Base EHR", "2015 Edition health IT certification criteria", "Common Clinical Data Set", "Device identifier", "Global Unique Device Identification Database (GUDID)", "Health IT Module", "Implantable device", "Production identifier", and "Unique device identifier".

The revisions read as follows:

§ 170.102 Definitions.

<u>2014 Edition Base EHR</u> means an electronic record of health-related information on an individual that:

(1) Includes patient demographic and clinical health information, such as medical history and problem lists;

(2) Has the capacity:

(i) To provide clinical decision support;

(ii) To support physician order entry;

(iii) To capture and query information relevant to health care quality;

(iv) To exchange electronic health information with, and integrate such information from other sources;

(v) To protect the confidentiality, integrity, and availability of health information stored and exchanged; and

(3) Has been certified to the certification criteria adopted by the Secretary:

(i) For at least one of the four criteria adopted at § 170.314(a)(1), (18), (19), or (20);

(ii) At § 170.314(a)(3);

(iii) At § 170.314(a)(5) through (8);

(iv) Both § 170.314(b)(1) and (2); or, both § 170.314(b)(8) and (h)(1); or § 170.314(b)(1) and (2) combined with either § 170.314(b)(8) or (h)(1), or both § 170.314(b)(8) and (h)(1);

(v) At § 170.314(b)(7);

(vi) At §170.314(c)(1) through (3);

(vii) At §170.314(d)(1) through (8);

(4) Has been certified to the certification criteria at § 170.314(c)(1) and (2):

(i) For no fewer than 9 clinical quality measures covering at least 3 domains from the set selected by CMS for eligible professionals, including at least 6 clinical quality measures from the recommended core set identified by CMS; or

(ii) For no fewer than 16 clinical quality measures covering at least 3 domains from the set selected by CMS for eligible hospitals and critical access hospitals.

* * * * *

2015 Edition Base EHR means an electronic record of health-related information on an individual that:

(1) Includes patient demographic and clinical health information, such as medical history and problem lists;

(2) Has the capacity:

(i) To provide clinical decision support;

(ii) To support physician order entry;

(iii) To capture and query information relevant to health care quality;

(iv) To exchange electronic health information with, and integrate such information from other sources; and

(3) Has been certified to the certification criteria adopted by the Secretary in § 170.315(a)(1), (2), or (3); (a)(5) through (9); (a)(11); (a)(15); (b)(1) and (6); (c)(1); (g)(7) through (9); and (h)(1) or (2);

2015 Edition health IT certification criteria means the certification criteria in § 170.315.

* * * * *

Common Clinical Data Set means the following data expressed, where indicated, according to the specified standard(s):

(1) Patient name. For certification to both the 2014 Edition EHR certification criteria and the 2015 Edition health IT certification criteria.

(2) Sex. (i) No required standard for certification to the 2014 Edition EHR certification criteria.

(ii) The standard specified in § 170.207(n)(1) for certification to the 2015 Edition health IT certification criteria.

(3) Date of birth. For certification to both the 2014 Edition EHR certification criteria and the 2015 Edition health IT certification criteria.

(4) Race. (i) The standard specified in § 170.207(f)(1) for certification to the 2014 Edition EHR certification criteria.

(ii) For certification to the 2015 Edition health IT certification criteria:

(A) The standard specified in § 170.207(f)(2);

(B) The standard specified in § 170.207(f)(1) for each race identified in accordance § 170.207(f)(2).

(5) Ethnicity. (i) The standard specified in § 170.207(f)(1) for certification to the 2014 Edition EHR certification criteria.

(ii) For certification to the 2015 Edition health IT certification criteria:

(A) The standard specified in § 170.207(f)(2);

(B) The standard specified in § 170.207(f)(1) for each ethnicity identified in accordance § 170.207(f)(2).

(6) Preferred language. (i) The standard specified in § 170.207(g)(1) for certification to the 2014 Edition EHR certification criteria.

(ii) The standard specified in § 170.207(g)(2) for certification to the 2015 Edition Health IT certification criteria.

(7) Smoking status. For certification to both the 2014 Edition EHR certification criteria and the 2015 Edition health IT certification criteria: The standard specified in § 170.207(h).

(8) Problems. (i) At a minimum, the standard specified in § 170.207(a)(3) for certification to the 2014 Edition EHR certification criteria.

(ii) At a minimum, the standard specified in § 170.207(a)(4) for certification to the 2015 Edition Health IT certification criteria.

(9) Medications. (i) At a minimum, the standard specified in § 170.207(d)(2) for certification to the 2014 Edition EHR certification criteria.

(ii) At a minimum, the standard specified in § 170.207(d)(3) for certification to the 2015 Edition Health IT certification criteria.

(10) Medication allergies. (i) At a minimum, the standard specified in § 170.207(d)(2) for certification to the 2014 Edition EHR certification criteria.

(ii) At a minimum, the standard specified in § 170.207(d)(3) for certification to the 2015 Edition Health IT certification criteria.

(11) Laboratory test(s). (i) At a minimum, the standard specified in § 170.207(c)(2) for certification to the 2014 Edition EHR certification criteria.

(ii) At a minimum, the standard specified in § 170.207(c)(3) for certification to the 2015 Edition Health IT certification criteria.

(12) Laboratory value(s)/result(s). For certification to both the 2014 Edition EHR certification criteria and the 2015 Edition health IT certification criteria.

(13) Vital signs. (i) Height/length, weight, blood pressure, and BMI for certification to the 2014 Edition EHR certification criteria.

(ii) For certification to the 2015 Edition Health IT certification criteria:

(A) The patient's diastolic blood pressure, systolic blood pressure, body height, body weight, heart rate, respiratory rate, body temperature, pulse oximetry, and inhaled oxygen concentration must be exchanged in numerical values only; and

(B) In accordance with the standard specified in § 170.207(c)(3) and with the associated applicable unit of measure for the vital sign measurement in the standard specified in § 170.207(m)(1).

(C) Optional. The patient's BMI percentile per age and sex for youth 2-20 years of age, weight for age per length and sex for children less than 3 years of age, and head occipital-frontal circumference for children less than 3 years of age must be recorded in numerical values only in accordance with the standard specified in § 170.207(c)(3) and with the associated applicable unit of measure for the vital sign measurement in the standard specified in § 170.207(m)(1). For BMI percentile per age and sex for youth 2-20 years of age and weight for age per length and sex for children less than 3 years of age, the reference range/scale or growth curve should be included as appropriate.

(14) Care plan field(s), including goals and instructions. For certification to the 2014 Edition EHR certification criteria.

(15) Procedures— (i)(A) At a minimum, the version of the standard specified in § 170.207(a)(3) for certification to the 2014 Edition EHR certification criteria and § 170.207(a)(4) for certification to the 2015 Edition health IT certification criteria, or § 170.207(b)(2); or

(B) For technology primarily developed to record dental procedures, the standard specified in § 170.207(b)(3) for certification to both the 2014 Edition EHR certification criteria and the 2015 Edition health IT certification criteria.

(ii) Optional. The standard specified in § 170.207(b)(4) for certification to both the 2014 Edition EHR certification criteria and the 2015 Edition health IT certification criteria.

(16) Care team member(s). For certification to both the 2014 Edition EHR certification criteria and the 2015 Edition health IT certification criteria.

(17) Immunizations. In accordance with, at a minimum, the standards specified in § 170.207(e)(3) and (4) for certification to the 2015 Edition health IT certification criteria.

(18) Unique device identifier(s) for a patient's implantable device(s). In accordance with the "Product Instance" in the "Procedure Activity Procedure Section" of the standard specified in § 170.205(a)(4) for certification to the 2015 Edition health IT certification criteria.

(19) Assessment and plan of treatment. For certification to the 2015 Edition health IT certification criteria:

(i) In accordance with the "Assessment and Plan Section (V2)" of the standard specified in § 170.205(a)(4); or

(ii) In accordance with the "Assessment Section (V2)" and "Plan of Treatment Section (V2)" of the standard specified in § 170.205(a)(4).

(20) Goals. In accordance with the "Goals Section" of the standard specified in § 170.205(a)(4) for certification to the 2015 Edition health IT certification criteria.

(21) Health concerns. In accordance with the "Health Concerns Section" of the standard specified in § 170.205(a)(4) for certification to the 2015 Edition health IT certification criteria.

* * * * *

Device identifier is defined as it is in 21 CFR 801.3.

* * * * *

Global Unique Device Identification Database (GUDID) is defined as it is in 21 CFR 801.3.

Health IT Module means any service, component, or combination thereof that can meet the requirements of at least one certification criterion adopted by the Secretary.

* * * * *

Implantable device is defined as it is in 21 CFR 801.3.

* * * * *

Production identifier is defined as it is in 21 CFR 801.3.

* * * * *

Unique device identifier is defined as it is in 21 CFR 801.3.

§ 170.200 [Amended]

3. In § 170.200, remove the term "EHR Modules" and add in its place "Health IT Modules."

4. Amend § 170.202 by—

a. Revising the section heading;

b. Revising paragraph (a); and

c. Adding paragraph (e).

The additions and revisions read as follows:

§ 170.202 Transport standards and other protocols.

* * * * *

(a) Direct Project--(1) Standard. ONC Applicability Statement for Secure Health Transport, Version 1.0 (incorporated by reference in § 170.299).

(2) Standard. ONC Applicability Statement for Secure Health Transport, Version 1.2 (incorporated by reference in § 170.299).

* * * * *

(e) Delivery notification--(1) Standard. ONC Implementation Guide for Delivery Notification in Direct (incorporated by reference in § 170.299).

(2) [Reserved]

5. Amend § 170.204 by—

a. Revising paragraphs (a) and (b)(2); and

b. Adding paragraphs (b)(3) and (4).

The additions and revisions read as follows:

§ 170.204 Functional standards.

* * * * *

(a) Accessibility--(1) Standard. Web Content Accessibility Guidelines (WCAG) 2.0, Level A Conformance (incorporated by reference in § 170.299).

(2) Standard. Web Content Accessibility Guidelines (WCAG) 2.0, Level AA Conformance (incorporated by reference in § 170.299).

(b) * * *

(2) Implementation specifications. HL7 Implementation Guide: Service-Oriented Architecture Implementations of the Context-aware Knowledge Retrieval (Infobutton) Domain, Draft Standard for Trial Use, Release 1 (incorporated by reference in § 170.299).

(3) Standard. HL7 Version 3 Standard: Context Aware Knowledge Retrieval Application. ("Infobutton"), Knowledge Request, Release 2 (incorporated by reference in § 170.299).

Implementation specifications. HL7 Implementation Guide: Service-Oriented Architecture Implementations of the Context-aware Knowledge Retrieval (Infobutton) Domain, Release 1 (incorporated by reference in § 170.299).

(4) Standard. HL7 Version 3 Standard: Context Aware Knowledge Retrieval Application ("Infobutton"), Knowledge Request, Release 2 (incorporated by reference in § 170.299). Implementation specifications. HL7 Version 3 Implementation Guide: Context-Aware Knowledge Retrieval (Infobutton), Release 4 (incorporated by reference in § 170.299).

6. Amend § 170.205 by—

a. Adding paragraphs (a)(4), (d)(4), and (e)(4);

b. Revising paragraphs (h), (i), and (k);

c. Reserving paragraphs (1), (m), (n), and (q); and

d. Adding paragraphs (o), (p), (r), and (s).

The additions and revisions read as follows:

§ 170.205 Content exchange standards and implementation specifications for exchanging electronic health information.

* * * * *

(a) * * *

(4) Standard. HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use, Volume 1 – Introductory Material, Release 2.1 and HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use, Volume 2 – Templates and Supporting Material, Release 2.1 (incorporated by reference in § 170.299).

* * * * *

(d) * * *

(4) Standard. HL7 2.5.1 (incorporated by reference in §170.299). Implementation specifications. PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent Care,

Inpatient and Ambulatory Care Settings, Release 2.0, April 21, 2015 (incorporated by reference in § 170.299) and Erratum to the CDC PHIN 2.0 Implementation Guide, August 2015; Erratum to the CDC PHIN 2.0 Messaging Guide, April 2015 Release for Syndromic Surveillance: Emergency Department, Urgent Care, Inpatient and Ambulatory Care Settings (incorporated by reference in § 170.299).

(e) * * *

(4) Standard. HL7 2.5.1 (incorporated by reference in § 170.299). Implementation specifications. HL7 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5 (incorporated by reference in § 170.299) and HL7 Version 2.5.1 Implementation Guide for Immunization Messaging (Release 1.5)—Addendum, July 2015 (incorporated by reference in § 170.299).

* * * * *

(h) Clinical quality measure data import, export and reporting. (1) Standard. HL7 Implementation Guide for CDA® Release 2: Quality Reporting Document Architecture (incorporated by reference in § 170.299).

(2) Standard. HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture – Category I (QRDA I); Release 1, DSTU Release 3 (US Realm), Volume 1 – Introductory Material and HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture – Category I (QRDA I); Release 1, DSTU Release 3 (US Realm), Volume 2 – Templates and Supporting Material (incorporated by reference in § 170.299).

(i) Cancer information--(1) Standard. HL7 Clinical Document Architecture (CDA), Release 2.0, Normative Edition (incorporated by reference in § 170.299). Implementation specifications. Implementation Guide for Ambulatory Healthcare Provider Reporting to Central

Cancer Registries, HL7 Clinical Document Architecture (CDA), Release 1.0 (incorporated by reference in § 170.299).

(2) Standard. HL7 Clinical Document Architecture (CDA), Release 2.0, Normative Edition (incorporated by reference in § 170.299). Implementation specifications. HL7 CDA© Release 2 Implementation Guide: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1; DSTU Release 1.1, Volume 1 – Introductory Material and HL7 CDA© Release 2 Implementation Guide: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1; DSTU Release 1.1 (US Realm), Volume 2 – Templates and Supporting Material (incorporated by reference in § 170.299).

* * * * *

(k) Clinical quality measure aggregate reporting. (1) Standard. Quality Reporting Document Architecture Category III, Implementation Guide for CDA Release 2 (incorporated by reference in § 170.299).

(2) Standard. Errata to the HL7 Implementation Guide for CDA® Release 2: Quality Reporting Document Architecture – Category III, DSTU Release 1 (US Realm), September 2014 (incorporated by reference in § 170.299).

(l) [Reserved]

(m) [Reserved]

(n) [Reserved]

(o) Data segmentation for privacy--(1) Standard. HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1 (incorporated by reference in § 170.299).

(2) [Reserved]

(p) XDM package processing--(1) Standard. IHE IT Infrastructure Technical Framework Volume 2b (ITI TF-2b) (incorporated by reference in § 170.299).

(2) [Reserved]

(q) [Reserved]

(r) Public health – antimicrobial use and resistance information--(1) Standard. The following sections of HL7 Implementation Guide for CDA® Release 2 – Level 3: Healthcare Associated Infection Reports, Release 1, U.S. Realm (incorporated by reference in § 170.299). Technology is only required to conform to the following sections of the implementation guide:

(i) HAI Antimicrobial Use and Resistance (AUR) Antimicrobial Resistance Option (ARO) Report (Numerator) specific document template in Section 2.1.2.1 (pages 69-72);

(ii) Antimicrobial Resistance Option (ARO) Summary Report (Denominator) specific document template in Section 2.1.1.1 (pages 54-56); and

(iii) Antimicrobial Use (AUP) Summary Report (Numerator and Denominator) specific document template in Section 2.1.1.2 (pages 56-58).

(2) [Reserved]

(s) Public health – health care survey information--(1) Standard. HL7 Implementation Guide for CDA® Release 2: National Health Care Surveys (NHCS), Release 1 – US Realm, HL7 Draft Standard for Trial Use, Volume 1 – Introductory Material and HL7 Implementation Guide for CDA® Release 2: National Health Care Surveys (NHCS), Release 1 – US Realm, HL7 Draft Standard for Trial Use, Volume 2 – Templates and Supporting Material (incorporated by reference in § 170.299).

(2) [Reserved]

7. Amend § 170.207 by—

a. Adding paragraphs (a)(4), (c)(3), (d)(3), (e)(3) and (4);

b. Revising paragraphs (f) and (g); and

c. Reserving paragraphs (k) and (l); and

d. Adding paragraphs (m), (n), (o), (p), (q), (r), and (s).

The additions and revisions read as follows:

§ 170.207 Vocabulary standards for representing electronic health information.

*** * * * ***

(a) * * *

(4) Standard. IHTSDO SNOMED CT®, U.S. Edition, September 2015 Release (incorporated by reference in § 170.299).

* * * * *

(c) * * *

(3) Standard. Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.52, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc. (incorporated by reference in § 170.299).

(d) * * *

(3) Standard. RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine, September 8, 2015 Release (incorporated by reference in § 170.299).

(e) * * *

(3) Standard. HL7 Standard Code Set CVX—Vaccines Administered, updates through August 17, 2015 (incorporated by reference in § 170.299).

(4) Standard. National Drug Code Directory (NDC)– Vaccine NDC Linker, updates through August 17, 2015 (incorporated by reference in § 170.299).

(f) Race and Ethnicity--(1) Standard. The Office of Management and Budget Standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity, Statistical Policy Directive No. 15, as revised, October 30, 1997 (incorporated by reference in § 170.299).

(2) Standard. CDC Race and Ethnicity Code Set Version 1.0 (March 2000) (incorporated by reference in § 170.299).

(g) Preferred language--(1) Standard. As specified by the Library of Congress, ISO 639-2 alpha-3 codes limited to those that also have a corresponding alpha-2 code in ISO 639-1 (incorporated by reference in § 170.299).

(2) Standard. Request for Comments (RFC) 5646 (incorporated by reference in § 170.299).

* * * * *

(k) [Reserved]

(l) [Reserved]

(m) Numerical references--(1) Standard. The Unified Code of Units of Measure, Revision 1.9 (incorporated by reference in § 170.299).

(2) [Reserved]

(n) Sex--(1) Standard. Birth sex must be coded in accordance with HL7 Version 3 Standard, Value Sets for AdministrativeGender and NullFlavor (incorporated by reference in § 170.299), attributed as follows:

(i) Male. M

(ii) Female. F

(iii) Unknown. nullFlavor UNK

(2) [Reserved]

(o) Sexual orientation and gender identity--(1) Standard. Sexual orientation must be coded in accordance with, at a minimum, the version of SNOMED CT® codes specified in paragraph (a)(4) of this section for paragraphs (o)(1)(i) through (iii) of this section and HL7 Version 3 Standard, Value Sets for AdministrativeGender and NullFlavor (incorporated by reference in § 170.299), for paragraphs (o)(1)(iv) through (vi) of this section, attributed as follows:

(i) Lesbian, gay or homosexual. 38628009

(ii) Straight or heterosexual. 20730005

(iii) Bisexual. 42035005

(iv) Something else, please describe. nullFlavor OTH

(v) Don't know. nullFlavor UNK

(vi) Choose not to disclose. nullFlavor ASKU

(2) Standard. Gender identity must be coded in accordance with, at a minimum, the version of SNOMED CT® codes specified in paragraph (a)(4) of this section for paragraphs (o)(2)(i) through (v) of this section and HL7 Version 3 Standard, Value Sets for AdministrativeGender and NullFlavor (incorporated by reference in § 170.299), for paragraphs (o)(2)(vi) and (vii) of this section, attributed as follows:

(i) Male. 446151000124109

(ii) Female. 446141000124107

(iii) Female-to-Male (FTM)/Transgender Male/Trans Man. 407377005

(iv) Male-to-Female (MTF)/Transgender Female/Trans Woman. 407376001

(v) Genderqueer, neither exclusively male nor female. 446131000124102

(vi) Additional gender category or other, please specify. nullFlavor OTH

(vii) Choose not to disclose. nullFlavor ASKU

(p) Social, psychological, and behavioral data--(1) Financial resource strain. Financial resource strain must be coded in accordance with, at a minimum, the version of LOINC® codes specified in paragraph (c)(3) of this section and attributed with the LOINC® code 76513-1 and LOINC® answer list ID LL3266-5.

(2) Education. Education must be coded in accordance with, at a minimum, the version of LOINC® codes specified in paragraph (c)(3) of this section and attributed with LOINC® code 63504-5 and LOINC® answer list ID LL1069-5.

(3) Stress. Stress must be coded in accordance with, at a minimum, the version of LOINC® codes specified in paragraph (c)(3) of this section and attributed with the LOINC® code 76542-0 and LOINC® answer list LL3267-3.

(4) Depression. Depression must be coded in accordance with, at a minimum, the version of LOINC® codes specified in paragraph (c)(3) of this section and attributed with LOINC® codes 55757-9, 44250-9 (with LOINC® answer list ID LL358-3), 44255-8 (with LOINC® answer list ID LL358-3), and 55758-7 (with the answer coded with the associated applicable unit of measure in the standard specified in § 170.207(m)(1)).

(5) Physical activity. Physical activity must be coded in accordance with, at a minimum, the version of LOINC® codes specified in paragraph (c)(3) of this section and attributed with LOINC® codes 68515-6 and 68516-4. The answers must be coded with the associated applicable unit of measure in the standard specified in § 170.207(m)(1).

(6) Alcohol use. Alcohol use must be coded in accordance with, at a minimum, the version of LOINC® codes specified in paragraph (c)(3) of this section and attributed with LOINC® codes

72109-2, 68518-0 (with LOINC® answer list ID LL2179-1), 68519-8 (with LOINC® answer list ID LL2180-9), 68520-6 (with LOINC® answer list ID LL2181-7), and 75626-2.

(7) Social connection and isolation. Social connection and isolation must be coded in accordance with, at a minimum, the version of LOINC® codes specified in paragraph (c)(3) of this section and attributed with the LOINC® codes 76506-5, 63503-7 (with LOINC answer list ID LL1068-7), 76508-1 (with the associated applicable unit of measure in the standard specified in § 170.207(m)(1)), 76509-9 (with the associated applicable unit of measure in the standard specified in § 170.207(m)(1)), 76510-7 (with the associated applicable unit of measure in the standard specified in § 170.207(m)(1)), 76511-5 (with LOINC answer list ID LL963-0), and 76512-3 (with the associated applicable unit of measure in the standard specified in § 170.207(m)(1)).

(8) Exposure to violence (intimate partner violence). Exposure to violence: intimate partner violence must be coded in accordance with, at a minimum, the version of LOINC® codes specified in paragraph (c)(3) of this section and attributed with the LOINC® code 76499-3, 76500-8 (with LOINC® answer list ID LL963-0), 76501-6 (with LOINC® answer list ID LL963-0), 76502-4 (with LOINC® answer list ID LL963-0), 76503-2 (with LOINC® answer list ID LL963-0), and 76504-0 (with the associated applicable unit of measure in the standard specified in § 170.207(m)(1)).

(q) Patient matching. (1) Phone number standard. ITU-T E.123, Series E: Overall Network Operation, Telephone Service, Service Operation and Human Factors, International operation – General provisions concerning users: Notation for national and international telephone numbers, e-mail addresses and web addresses (incorporated by reference in § 170.299); and ITU-T E.164, Series E: Overall Network Operation, Telephone Service, Service Operation and Human Factors,

International operation – Numbering plan of the international telephone service: The international public telecommunication numbering plan (incorporated by reference in § 170.299).

(2) [Reserved]

(r) Provider type. (1) Standard. Crosswalk: Medicare Provider/Supplier to Healthcare Provider Taxonomy, April 2, 2015 (incorporated by reference in § 170.299).

(2) [Reserved]

(s) Patient insurance. (1) Standard. Public Health Data Standards Consortium Source of Payment Typology Code Set Version 5.0 (October 2011) (incorporated by reference in § 170.299).

(2) [Reserved]

8. In § 170.210:

a. Add paragraph (a)(2)

b. Revise paragraphs (c) and (e)(1)(i);

c. Amend paragraphs (e)(3) by removing the term "EHR technology" and adding in its place "health IT"; and

d. Revise paragraph (h).

The addition and revisions read as follows:

§ 170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged.

* * * * *

(a) * * *

(2) General. Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information

Processing Standards (FIPS) Publication 140-2, October 8, 2014 (incorporated by reference in § 170.299).

* * * * *

(c) Hashing of electronic health information. (1) Standard. A hashing algorithm with a security strength equal to or greater than SHA–1 (Secure Hash Algorithm (SHA-1)) as s specified by the National Institute of Standards and Technology (NIST) in FIPS PUB 180-4 (March 2012)).

(2) Standard. A hashing algorithm with a security strength equal to or greater than SHA-2 as specified by NIST in FIPS Publication 180-4 (August 2015) (incorporated by reference in § 170.299).

* * * * *

(e) * * *

(1)(i) The audit log must record the information specified in sections 7.2 through 7.4, 7.6, and 7.7 of the standard specified in § 170.210(h) and changes to user privileges when health IT is in use.

* * * * *

(h) Audit log content. ASTM E2147-01(Reapproved 2013), (incorporated by reference in § 170.299).

9. In § 170.299:

a. Revise paragraph (c)(1).

b. Add paragraphs (d)(10) through (16), (e)(3) and (f)(15) through (29).

c. Redesignate paragraphs (g), (h), (i), (j), (k), (l), (m), and (n) as paragraphs (h), (j), (k), (l), (m), (o), (q), and (r), respectively.

d. Add new paragraphs (g), (i), (n), and (p).

e. Amend newly redesignated paragraph (h) by revising paragraph (h) introductory text and adding paragraph (h)(3).

f. Amend newly redesignated paragraph (l) by adding paragraphs (l)(3) and (4).

g. Amend newly redesignated paragraph (m) by revising paragraph (m) introductory text.

h. Amend newly redesignated paragraph (o) by revising paragraph (o) introductory text and adding paragraphs (o)(3) and (4).

i. Amend newly redesignated paragraph (q) by adding paragraphs (q)(6) and (7).

The additions and revisions read as follows:

§ 170.299 Incorporation by reference.

* * * * *

(c) * * *

(1) ASTM E2147-01 (Reapproved 2013) Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems, approved March 1, 2013, IBR approved for § 170.210(h).

* * * * *

(d) * * *

(10) PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent Care, Inpatient and Ambulatory Care Settings, Release 2.0, April 21, 2015, IBR approved for § 170.205(d).

(11) Erratum to the CDC PHIN 2.0 Implementation Guide, August 2015; Erratum to the CDC PHIN 2.0 Messaging Guide, April 2015 Release for Syndromic Surveillance: Emergency Department, Urgent Care, Inpatient and Ambulatory Care Settings, IBR approved for § 170.205(d).

(12) HL7 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5, October 1, 2014, IBR approved for § 170.205(e).

(13) HL7 Version 2.5.1 Implementation Guide for Immunization Messaging (Release 1.5)—Addendum, July 2015, IBR approved for § 170.205(e).

(14) HL7 Standard Code Set CVX—Vaccines Administered, updates through August 17, 2015, IBR approved for § 170.207(e).

(15) National Drug Code Directory (NDC) – Vaccine NDC Linker, updates through August 17, 2015, IBR approved for § 170.207(e).

(16) CDC Race and Ethnicity Code Set Version 1.0 (March 2000), IBR approved for § 170.207(f).

(e) * * *

(3) Crosswalk: Medicare Provider/Supplier to Healthcare Provider Taxonomy, April 2, 2015, IBR approved for § 170.207(r).

(f) * * *

(15) HL7 Version 3 Standard: Context Aware Retrieval Application (“Infobutton”), Knowledge Request, Release 2, 2014 Release, IBR approved for § 170.204(b).

(16) HL7 Implementation Guide: Service-Oriented Architecture Implementations of the Context-aware Knowledge Retrieval (Infobutton) Domain, Release 1, August 9, 2013, IBR approved for § 170.204(b).

(17) HL7 Version 3 Implementation Guide: Context-Aware Knowledge Retrieval (Infobutton), Release 4, June 13, 2014, IBR approved for § 170.204(b).

(18) HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use, Volume 1 – Introductory Material, Release 2.1, August 2015, IBR approved for § 170.205(a).

(19) HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use, Volume 2 – Templates and Supporting Material, Release 2.1, August 2015, IBR approved for § 170.205(a).

(20) HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture – Category I (QRDA I); Release 1, DSTU Release 3 (US Realm), Volume 1 – Introductory Material, June 2015, IBR approved for § 170.205(h).

(21) HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture – Category I (QRDA I); Release 1, DSTU Release 3 (US Realm), Volume 2 – Templates and Supporting Material, June 2015, IBR approved for § 170.205(h).

(22) HL7 CDA© Release 2 Implementation Guide: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1; DSTU Release 1.1 (US Realm), Volume 1 – Introductory Material, April 2015, IBR approved for § 170.205(i).

(23) HL7 CDA© Release 2 Implementation Guide: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1; DSTU Release 1.1 (US Realm), Volume 2 – Templates and Supporting Material, April 2015, IBR approved for § 170.205(i).

(24) Errata to the HL7 Implementation Guide for CDA® Release 2: Quality Reporting Document Architecture – Category III, DSTU Release 1 (US Realm), September 2014, IBR approved for § 170.205(k).

(25) HL7 Version 3 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1, Part 1: CDA R2 and Privacy Metadata Reusable Content Profile, May 16, 2014, IBR approved for § 170.205(o).

(26) HL7 Implementation Guide for CDA® Release 2 – Level 3: Healthcare Associated Infection Reports, Release 1 (U.S. Realm), August 9, 2013, IBR approved for § 170.205(r).

(27) HL7 Implementation Guide for CDA® Release 2: National Health Care Surveys (NHCS), Release 1 – US Realm, HL7 Draft Standard for Trial Use, Volume 1 – Introductory Material, December 2014, IBR approved for § 170.205(s).

(28) HL7 Implementation Guide for CDA® Release 2: National Health Care Surveys (NHCS), Release 1 – US Realm, HL7 Draft Standard for Trial Use, Volume 2 – Templates and Supporting Material, December 2014, IBR approved for § 170.205(s).

(29) HL7 Version 3 (V3) Standard, Value Sets for AdministrativeGender and NullFlavor, published August 1, 2013, IBR approved for § 170.207(n) and (o).

(g) Integrating the Healthcare Enterprise (IHE), 820 Jorie Boulevard, Oak Brook, IL, Telephone (630) 481-1004, http://http://www.ihe.net/.

(1) IHE IT Infrastructure Technical Framework Volume 2b (ITI TF-2b), Transactions Part B – Sections 3.29 – 2.43, Revision 7.0, August 10, 2010, IBR approved for § 170.205(p).

(2) [Reserved]

(h) Internet Engineering Task Force (IETF) Secretariat, c/o Association Management Solutions, LLC (AMS), 48377 Fremont Blvd., Suite 117, Fremont, CA, 94538, Telephone (510) 492-4080, http://www.ietf.org/rfc.html.

* * * * *

(3) Request for Comment (RFC) 5646, "Tags for Identifying Languages, September 2009," copyright 2009, IBR approved for § 170.207(g).

(i) International Telecommunication Union (ITU), Place des Nations, 1211 Geneva 20 Switzerland, Telephone (41) 22 730 511, http://www.itu.int/en/pages/default.aspx.

(1) ITU-T E.123, Series E: Overall Network Operation, Telephone Service, Service Operation and Human Factors, International operation – General provisions concerning users: Notation for national and international telephone numbers, e-mail addresses and web addresses, February 2001, IBR approved for § 170.207(q).

(2) ITU-T E.164, Series E: Overall Network Operation, Telephone Service, Service Operation and Human Factors, International operation – Numbering plan of the international telephone service, The international public telecommunication numbering plan, November 2010, IBR approved for § 170.207(q).

* * * * *

(l) * * *

(3) Annex A: Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, October 8, 2014, IBR approved for § 170.210(a).

(4) FIPS PUB 180-4, Secure Hash Standard (August 2015), IBR approved for § 170.210(c).

(m) Office of the National Coordinator for Health Information Technology (ONC), 330 C Street, SW, Washington, D.C. 20201, http://healthit.hhs.gov.

* * * * *

(n) Public Health Data Standards Consortium, 111 South Calvert Street, Suite 2700, Baltimore, MD 21202, http://www.phdsc.org/.

(1) Public Health Data Standards Consortium Source of Payment Typology Code Set Version 5.0 (October 2011), IBR approved for § 170.207(s).

(2) [Reserved]

(o) Regenstrief Institute, Inc., LOINC® c/o Regenstrief Center for Biomedical Informatics, Inc., 410 West 10th Street, Suite 2000, Indianapolis, IN 46202-3012, http://loinc.org/.

* * * * *

(3) Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.52, Released June 2015, IBR approved for § 170.207(c).

(4) The Unified Code of Units for Measure, Revision 1.9, October 23, 2013, IBR approved for § 170.207.

(p) The Direct Project, c/o the Office of the National Coordinator for Health Information Technology (ONC), 330 C Street, SW, Washington, D.C. 20201, http://healthit.hhs.gov.

(1) Applicability Statement for Secure Health Transport, Version 1.2, August 2015, IBR approved for § 170.202(a).

(2) Implementation Guide for Delivery Notification in Direct, Version 1.0, June 29, 2012, IBR approved for § 170.202(e).

(q) * * *

(6) International Health Terminology Standards Development Organization (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®) U.S. Edition, September 2015 Release, IBR approved for § 170.207(a).

(7) RxNorm, September 8, 2015 Full Release Update, IBR approved for § 170.207(d).

10. In § 170.300, revise paragraph (d) to read as follows:

§ 170.300 Applicability.

* * * * *

(d) In §§ 170.314 and 170.315, all certification criteria and all capabilities specified within a certification criterion have general applicability (i.e., apply to any health care setting) unless designated as "inpatient setting only" or "ambulatory setting only."

(1) Inpatient setting only means that the criterion or capability within the criterion is only required for certification of health IT designed for use in an inpatient setting.

(2) Ambulatory setting only means that the criterion or capability within the criterion is only required for certification of health IT designed for use in an ambulatory setting.

§ 170.314 [Amended]

11. In § 170.314:

a. In paragraph (a)(3)(i)(A), remove "§ 170.207(f)" and add in its place "§ 170.207(f)(1)";

b. In paragraph (a)(3)(i)(B), remove "§ 170.207(g)" and add in its place "§ 170.207(g)(1)";

c. In paragraph (a)(8)(iii)(B)(2), remove "paragraph (b)(1)(iii)" and add in its place "paragraph (b)(1)(iii)(B) or (b)(9)(ii)(D)";

d. In paragraphs (b)(2)(i) introductory text, (b)(7) introductory text, (b)(8)(iii) introductory text, (e)(1)(i)(A)(1), and (e)(2)(iii)(A), remove the term "Common MU Data Set" and add in its place "Common Clinical Data Set";

e. In paragraph (c)(1)(ii), remove "§ 170.205(h)" and add in its place "§ 170.205(h)(1)";

f. In paragraph (c)(2)(i), remove "§ 170.205(h)" and add in its place "§ 170.205(h)(1)";

g. In paragraph (c)(3)(i), remove "§ 170.205(h)" and add in its place "§ 170.205(h)(1)";

h. In paragraph (c)(3)(i), remove "(k)" and add in its place "§ (k)(1)";

i. In paragraphs (d)(8)(i) and (ii), remove "§ 170.210(c)" and add in its place "170.210(c)(1)";

j. In paragraph (e)(1)(i)(A) introductory text, remove "§ 170.204(a)" and add in its place "§ 170.204(a)(1)";

k. In paragraph (f)(6)(i), remove "§ 170.205(i)" and add in its place " § 170.205(i)(1)";

l. In paragraphs (b)(1)(i)(A) and (B), (b)(2)(ii)(A) and (B), (b)(8)(i)(A) and (B), (e)(1)(i)(C)(1)(i) and (ii), (e)(1)(i)(C)(2)(i) and (ii), and (h)(1) and (2), remove "§ 170.202(a)" and add in its place "§ 170.202(a)(1)".

12. Add § 170.315 to subpart C to read as follows:

§ 170.315 2015 Edition health IT certification criteria.

The Secretary adopts the following certification criteria for health IT. Health IT must be able to electronically perform the following capabilities in accordance with all applicable standards and implementation specifications adopted in this part:

(a) Clinical--(1) Computerized provider order entry – medications. (i) Enable a user to record, change, and access medication orders.

(ii) Optional. Include a "reason for order" field.

(2) Computerized provider order entry – laboratory. (i) Enable a user to record, change, and access laboratory orders.

(ii) Optional. Include a "reason for order" field.

(3) Computerized provider order entry – diagnostic imaging. (i) Enable a user to record, change, and access diagnostic imaging orders.

(ii) Optional. Include a "reason for order" field.

(4) Drug-drug, drug-allergy interaction checks for CPOE--(i) Interventions. Before a medication order is completed and acted upon during computerized provider order entry (CPOE), interventions must automatically indicate to a user drug-drug and drug-allergy contraindications based on a patient's medication list and medication allergy list.

(ii) Adjustments. (A) Enable the severity level of interventions provided for drug-drug interaction checks to be adjusted.

(B) Limit the ability to adjust severity levels in at least one of these two ways:

(1) To a specific set of identified users.

(2) As a system administrative function.

(5) Demographics. (i) Enable a user to record, change, and access patient demographic data including race, ethnicity, preferred language, sex, sexual orientation, gender identity, and date of birth.

(A) Race and ethnicity. (1) Enable each one of a patient's races to be recorded in accordance with, at a minimum, the standard specified in § 170.207(f)(2) and whether a patient declines to specify race.

(2) Enable each one of a patient's ethnicities to be recorded in accordance with, at a minimum, the standard specified in § 170.207(f)(2) and whether a patient declines to specify ethnicity.

(3) Aggregate each one of the patient's races and ethnicities recorded in accordance with paragraphs (a)(5)(i)(A)(1) and (2) of this section to the categories in the standard specified in § 170.207(f)(1).

(B) Preferred language. Enable preferred language to be recorded in accordance with the standard specified in § 170.207(g)(2) and whether a patient declines to specify a preferred language.

(C) Sex. Enable sex to be recorded in accordance with the standard specified in § 170.207(n)(1).

(D) Sexual orientation. Enable sexual orientation to be recorded in accordance with the standard specified in § 170.207(o)(1) and whether a patient declines to specify sexual orientation.

(E) Gender identity. Enable gender identity to be recorded in accordance with the standard specified in § 170.207(o)(2) and whether a patient declines to specify gender identity.

(ii) Inpatient setting only. Enable a user to record, change, and access the preliminary cause of death and date of death in the event of mortality.

(6) Problem list. Enable a user to record, change, and access a patient's active problem list:

(i) Ambulatory setting only. Over multiple encounters in accordance with, at a minimum, the version of the standard specified in § 170.207(a)(4).

(ii) Inpatient setting only. For the duration of an entire hospitalization in accordance with, at a minimum, the version of the standard specified in § 170.207(a)(4).

(7) Medication list. Enable a user to record, change, and access a patient's active medication list as well as medication history:

(i) Ambulatory setting only. Over multiple encounters.

(ii) Inpatient setting only. For the duration of an entire hospitalization.

(8) Medication allergy list. Enable a user to record, change, and access a patient's active medication allergy list as well as medication allergy history:

(i) Ambulatory setting only. Over multiple encounters.

(ii) Inpatient setting only. For the duration of an entire hospitalization.

(9) Clinical decision support (CDS)-- (i) CDS intervention interaction. Interventions provided to a user must occur when a user is interacting with technology.

(ii) CDS configuration. (A) Enable interventions and reference resources specified in paragraphs (a)(9)(iii) and (iv) of this section to be configured by a limited set of identified users (e.g., system administrator) based on a user's role.

(B) Enable interventions:

(1) Based on the following data:

(i) Problem list;

(ii) Medication list;

(iii) Medication allergy list;

(iv) At least one demographic specified in paragraph (a)(5)(i) of this section;

(v) Laboratory tests; and

(vi) Vital signs.

(2) When a patient's medications, medication allergies, and problems are incorporated from a transition of care/referral summary received and pursuant to paragraph (b)(2)(iii)(D) of this section.

(iii) Evidence-based decision support interventions. Enable a limited set of identified users to select (i.e., activate) electronic CDS interventions (in addition to drug-drug and drug-allergy contraindication checking) based on each one and at least one combination of the data referenced in paragraphs (a)(9)(ii)(B)(1)(i) through (vi) of this section.

(iv) Linked referential CDS. (A) Identify for a user diagnostic and therapeutic reference information in accordance at least one of the following standards and implementation specifications:

(1) The standard and implementation specifications specified in § 170.204(b)(3).

(2) The standard and implementation specifications specified in § 170.204(b)(4).

(B) For paragraph (a)(9)(iv)(A) of this section, technology must be able to identify for a user diagnostic or therapeutic reference information based on each one and at least one combination of the data referenced in paragraphs (a)(9)(ii)(B)(1)(i), (ii), and (iv) of this section.

(v) Source attributes. Enable a user to review the attributes as indicated for all CDS resources:

(A) For evidence-based decision support interventions under paragraph (a)(9)(iii) of this section:

(1) Bibliographic citation of the intervention (clinical research/guideline);

(2) Developer of the intervention (translation from clinical research/guideline);

(3) Funding source of the intervention development technical implementation; and

(4) Release and, if applicable, revision date(s) of the intervention or reference source.

(B) For linked referential CDS in paragraph (a)(9)(iv) of this section and drug-drug, drug-allergy interaction checks in paragraph (a)(4) of this section, the developer of the intervention, and where clinically indicated, the bibliographic citation of the intervention (clinical research/guideline).

(10) Drug-formulary and preferred drug list checks. The requirements specified in one of the following paragraphs (that is, paragraphs (a)(10)(i) and (a)(10)(ii) of this section) must be met to satisfy this certification criterion:

(i) Drug formulary checks. Automatically check whether a drug formulary exists for a given patient and medication.

(ii) Preferred drug list checks. Automatically check whether a preferred drug list exists for a given patient and medication.

(11) Smoking status. Enable a user to record, change, and access the smoking status of a patient.

(12) Family health history. Enable a user to record, change, and access a patient's family health history in accordance with the familial concepts or expressions included in, at a minimum, the version of the standard in § 170.207(a)(4).

(13) Patient-specific education resources. (i) Identify patient-specific education resources based on data included in the patient's problem list and medication list in accordance with at least one of the following standards and implementation specifications:

(A) The standard and implementation specifications specified in § 170.204(b)(3).

(B) The standard and implementation specifications specified in § 170.204(b)(4).

(ii) Optional. Request that patient-specific education resources be identified in accordance with the standard in § 170.207(g)(2).

(14) Implantable device list. (i) Record Unique Device Identifiers associated with a patient's Implantable Devices.

(ii) Parse the following identifiers from a Unique Device Identifier:

(A) Device Identifier;

(B) The following identifiers that compose the Production Identifier:

(1) The lot or batch within which a device was manufactured;

(2) The serial number of a specific device;

(3) The expiration date of a specific device;

(4) The date a specific device was manufactured; and

(5) For an HCT/P regulated as a device, the distinct identification code required by 21 CFR 1271.290(c).

(iii) Obtain and associate with each Unique Device Identifier:

(A) A description of the implantable device referenced by at least one of the following:

(1) The "GMDN PT Name" attribute associated with the Device Identifier in the Global Unique Device Identification Database.

(2) The "SNOMED CT® Description" mapped to the attribute referenced in in paragraph (a)(14)(iii)(A)(1) of this section.

(B) The following Global Unique Device Identification Database attributes:

(1) "Brand Name";

(2) "Version or Model";

(3) "Company Name";

(4) "What MRI safety information does the labeling contain?"; and

(5) "Device required to be labeled as containing natural rubber latex or dry natural rubber (21 CFR 801.437)."

(iv) Display to a user an implantable device list consisting of:

(A) The active Unique Device Identifiers recorded for a patient; and

(B) For each active Unique Device Identifier recorded for a patient, the description of the implantable device specified by paragraph (a)(14)(iii)(A) of this section.

(C) A method to access all Unique Device Identifiers recorded for a patient.

(v) For each Unique Device Identifier recorded for a patient, enable a user to access:

(A) The Unique Device Identifier;

(B) The description of the implantable device specified by paragraph (a)(14)(iii)(A) of this section;

(C) The identifiers associated with the Unique Device Identifier, as specified by paragraph (a)(14)(ii) of this section;

(D) The attributes associated with the Unique Device Identifier, as specified by paragraph (a)(14)(iii)(B) of this section.

(vi) Enable a user to change the status of a Unique Device Identifier recorded for a patient.

(15) Social, psychological, and behavioral data. Enable a user to record, change, and access the following patient social, psychological, and behavioral data:

(i) Financial resource strain. Enable financial resource strain to be recorded in accordance with the standard specified in § 170.207(p)(1) and whether a patient declines to specify financial resource strain.

(ii) Education. Enable education to be recorded in accordance with the standard specified in § 170.207(p)(2) and whether a patient declines to specify education.

(iii) Stress. Enable stress to be recorded in accordance with the standard specified in § 170.207(p)(3) and whether a patient declines to specify stress.

(iv) Depression. Enable depression to be recorded in accordance with the standard specified in § 170.207(p)(4) and whether a patient declines to specify depression.

(v) Physical activity. Enable physical activity to be recorded in accordance with the standard specified in § 170.207(p)(5) and whether a patient declines to specify physical activity.

(vi) Alcohol use. Enable alcohol use to be recorded in accordance with the standard specified in § 170.207(p)(6) and whether a patient declines to specify alcohol use.

(vii) Social connection and isolation. Enable social connection and isolation to be recorded in accordance the standard specified in § 170.207(p)(7) and whether a patient declines to specify social connection and isolation.

(viii) Exposure to violence (intimate partner violence). Enable exposure to violence (intimate partner violence) to be recorded in accordance with the standard specified in § 170.207(p)(8) and whether a patient declines to specify exposure to violence (intimate partner violence).

(b) Care coordination--(1) Transitions of care--(i) Send and receive via edge protocol--(A) Send transition of care/referral summaries through a method that conforms to the standard specified in § 170.202(d) and that leads to such summaries being processed by a service that has implemented the standard specified in §170.202(a)(2); and

(B) Receive transition of care/referral summaries through a method that conforms to the standard specified in § 170.202(d) from a service that has implemented the standard specified in § 170.202(a)(2).

(C) XDM processing. Receive and make available the contents of a XDM package formatted in accordance with the standard adopted in § 170.205(p)(1) when the technology is also being certified using an SMTP-based edge protocol.

(ii) Validate and display--(A) Validate C-CDA conformance – system performance. Demonstrate the ability to detect valid and invalid transition of care/referral summaries received and formatted in accordance with the standards specified in § 170.205(a)(3) and § 170.205(a)(4) for the Continuity of Care Document, Referral Note, and (inpatient setting only) Discharge Summary document templates. This includes the ability to:

(1) Parse each of the document types.

(2) Detect errors in corresponding “document-templates,” “section-templates,” and “entry-templates,” including invalid vocabulary standards and codes not specified in the standards adopted in § 170.205(a)(3) and § 170.205(a)(4).

(3) Identify valid document-templates and process the data elements required in the corresponding section-templates and entry-templates from the standards adopted in § 170.205(a)(3) and § 170.205(a)(4).

(4) Correctly interpret empty sections and null combinations.

(5) Record errors encountered and allow a user through at least one of the following ways to:

(i) Be notified of the errors produced.

(ii) Review the errors produced.

(B) Display. Display in human readable format the data included in transition of care/referral summaries received and formatted according to the standards specified in § 170.205(a)(3) and § 170.205(a)(4).

(C) Display section views. Allow for the individual display of each section (and the accompanying document header information) that is included in a transition of care/referral summary received and formatted in accordance with the standards adopted in § 170.205(a)(3) and § 170.205(a)(4) in a manner that enables the user to:

(1) Directly display only the data within a particular section;

(2) Set a preference for the display order of specific sections; and

(3) Set the initial quantity of sections to be displayed.

(iii) Create. Enable a user to create a transition of care/referral summary formatted in accordance with the standard specified in § 170.205(a)(4) using the Continuity of Care Document, Referral Note, and (inpatient setting only) Discharge Summary document templates that includes, at a minimum:

(A) The Common Clinical Data Set.

(B) Encounter diagnoses. Formatted according to at least one of the following standards:

(1) The standard specified in § 170.207(i).

(2) At a minimum, the version of the standard specified in § 170.207(a)(4).

(C) Cognitive status.

(D) Functional status.

(E) Ambulatory setting only. The reason for referral; and referring or transitioning provider's name and office contact information.

(F) Inpatient setting only. Discharge instructions.

(G) Patient matching data. First name, last name, previous name, middle name (including middle initial), suffix, date of birth, address, phone number, and sex. The following constraints apply:

(1) Date of birth constraint--(i) The year, month and day of birth must be present for a date of birth. The technology must include a null value when the date of birth is unknown.

(ii) Optional. When the hour, minute, and second are associated with a date of birth the technology must demonstrate that the correct time zone offset is included.

(2) Phone number constraint. Represent phone number (home, business, cell) in accordance with the standards adopted in § 170.207(q)(1). All phone numbers must be included when multiple phone numbers are present.

(3) Sex constraint. Represent sex in accordance with the standard adopted in § 170.207(n)(1).

(2) Clinical information reconciliation and incorporation--(i) General requirements. Paragraphs (b)(2)(ii) and (iii) of this section must be completed based on the receipt of a transition of care/referral summary formatted in accordance with the standards adopted in § 170.205(a)(3) and § 170.205(a)(4) using the Continuity of Care Document, Referral Note, and (inpatient setting only) Discharge Summary document templates.

(ii) Correct patient. Upon receipt of a transition of care/referral summary formatted according to the standards adopted § 170.205(a)(3) and § 170.205(a)(4), technology must be able to demonstrate that the transition of care/referral summary received can be properly matched to the correct patient.

(iii) Reconciliation. Enable a user to reconcile the data that represent a patient's active medication list, medication allergy list, and problem list as follows. For each list type:

(A) Simultaneously display (i.e., in a single view) the data from at least two sources in a manner that allows a user to view the data and their attributes, which must include, at a minimum, the source and last modification date.

(B) Enable a user to create a single reconciled list of each of the following: medications; medication allergies; and problems.

(C) Enable a user to review and validate the accuracy of a final set of data.

(D) Upon a user's confirmation, automatically update the list, and incorporate the following data expressed according to the specified standard(s):

(1) Medications. At a minimum, the version of the standard specified in § 170.207(d)(3);

(2) Medication allergies. At a minimum, the version of the standard specified in § 170.207(d)(3); and

(3) Problems. At a minimum, the version of the standard specified in § 170.207(a)(4).

(iv) System verification. Based on the data reconciled and incorporated, the technology must be able to create a file formatted according to the standard specified in § 170.205(a)(4) using the Continuity of Care Document document template.

(3) Electronic prescribing. (i) Enable a user to perform all of the following prescription-related electronic transactions in accordance with the standard specified in § 170.205(b)(2) and, at a minimum, the version of the standard specified in § 170.207(d)(3) as follows:

(A) Create new prescriptions (NEWRX).

(B) Change prescriptions (RXCHG, CHGRES).

(C) Cancel prescriptions (CANRX, CANRES).

(D) Refill prescriptions (REFREQ, REFRES).

(E) Receive fill status notifications (RXFILL).

(F) Request and receive medication history information (RXHREQ, RXHRES).

(ii) For each transaction listed in paragraph (b)(3)(i) of this section, the technology must be able to receive and transmit the reason for the prescription using the diagnosis elements in DRU Segment.

(iii) Optional. For each transaction listed in paragraph (b)(3)(i) of this section, the technology must be able to receive and transmit the reason for the prescription using the indication elements in the SIG Segment.

(iv) Limit a user's ability to prescribe all oral liquid medications in only metric standard units of mL (i.e., not cc).

(v) Always insert leading zeroes before the decimal point for amounts less than one and must not allow trailing zeroes after a decimal point when a user prescribes medications.

(4) Common Clinical Data Set summary record – create. Enable a user to create a transition of care/referral summary formatted in accordance with the standard specified in § 170.205(a)(4) using the Continuity of Care Document, Referral Note, and (inpatient setting only) Discharge Summary document templates that includes, at a minimum:

(i) The Common Clinical Data Set.

(ii) Encounter diagnoses. Formatted according to at least one of the following standards:

(A) The standard specified in § 170.207(i).

(B) At a minimum, the version of the standard specified in § 170.207(a)(4).

(iii) Cognitive status.

(iv) Functional status.

(v) Ambulatory setting only. The reason for referral; and referring or transitioning provider's name and office contact information.

(vi) Inpatient setting only. Discharge instructions.

(vii) Patient matching data. First name, last name, previous name, middle name (including middle initial), suffix, date of birth, address, phone number, and sex. The following constraints apply:

(A) Date of birth constraint--(1) The year, month and day of birth must be present for a date of birth. The technology must include a null value when the date of birth is unknown.

(2) Optional. When the hour, minute, and second are associated with a date of birth the technology must demonstrate that the correct time zone offset is included.

(B) Phone number constraint. Represent phone number (home, business, cell) in accordance with the standards adopted in § 170.207(q)(1). All phone numbers must be included when multiple phone numbers are present.

(C) Sex constraint. Represent sex in accordance with the standard adopted in § 170.207(n)(1).

(5) Common Clinical Data Set summary record – receive--(i) Enable a user to receive a transition of care/referral summary formatted in accordance with the standards adopted in §

170.205(a)(3) and § 170.205(a)(4) using the Continuity of Care Document, Referral Note, and (inpatient setting only) Discharge Summary document templates that includes, at a minimum:

(A) The Common Clinical Data Set.

(B) Encounter diagnoses. Formatted according to at least one of the following standards:

(1) The standard specified in § 170.207(i).

(2) At a minimum, the standard specified in § 170.207(a)(4).

(C) Cognitive status.

(D) Functional status.

(E) Ambulatory setting only. The reason for referral; and referring or transitioning provider's name and office contact information.

(F) Inpatient setting only. Discharge instructions.

(ii) Validate and display. Demonstrate the following functionalities for the document received in accordance with paragraph (b)(5)(i) of this section:

(A) Validate C-CDA conformance – system performance. Detect valid and invalid transition of care/referral summaries including the ability to:

(1) Parse each of the document types formatted according to the following document templates: Continuity of Care Document, Referral Note, and (inpatient setting only) Discharge Summary.

(2) Detect errors in corresponding "document-templates," "section-templates," and "entry-templates," including invalid vocabulary standards and codes not specified in the standards adopted in § 170.205(a)(3) and § 170.205(a)(4).

(3) Identify valid document-templates and process the data elements required in the corresponding section-templates and entry-templates from the standards adopted in § 170.205(a)(3) and § 170.205(a)(4).

(4) Correctly interpret empty sections and null combinations.

(5) Record errors encountered and allow a user through at least one of the following ways to:

(i) Be notified of the errors produced.

(ii) Review the errors produced.

(B) Display. Display in human readable format the data included in transition of care/referral summaries received and formatted according to the standards specified in § 170.205(a)(3) and § 170.205(a)(4).

(C) Display section views. Allow for the individual display of each section (and the accompanying document header information) that is included in a transition of care/referral summary received and formatted in accordance with the standards adopted in § 170.205(a)(3) and § 170.205(a)(4) in a manner that enables the user to:

(1) Directly display only the data within a particular section;

(2) Set a preference for the display order of specific sections; and

(3) Set the initial quantity of sections to be displayed.

(6) Data export--(i) General requirements for export summary configuration. (A) Enable a user to set the configuration options specified in paragraph (b)(6)(ii) through (v) of this section when creating an export summary as well as a set of export summaries for patients whose information is stored in the technology. A user must be able to execute these capabilities at any time the user chooses and without subsequent developer assistance to operate.

(B) Limit the ability of users who can create export summaries in at least one of these two ways:

(1) To a specific set of identified users.

(2) As a system administrative function.

(ii) Creation configuration. Enable a user to configure the technology to create export summaries formatted in accordance with the standard specified in § 170.205(a)(4) using the Continuity of Care Document document template that includes, at a minimum:

(A) The Common Clinical Data Set.

(B) Encounter diagnoses. Formatted according to at least one of the following standards:

(1) The standard specified in § 170.207(i).

(2) At a minimum, the version of the standard specified in § 170.207(a)(4).

(C) Cognitive status.

(D) Functional status.

(E) Ambulatory setting only. The reason for referral; and referring or transitioning provider's name and office contact information.

(F) Inpatient setting only. Discharge instructions.

(iii) Timeframe configuration. (A) Enable a user to set the date and time period within which data would be used to create the export summaries. This must include the ability to enter in a start and end date and time range.

(B) Consistent with the date and time period specified in paragraph (b)(6)(iii)(A) of this section, enable a user to do each of the following:

(1) Create export summaries in real-time;

(2) Create export summaries based on a relative date and time (e.g., the first of every month at 1:00am); and

(3) Create export summaries based on a specific date and time (e.g., on 10/24/2015 at 1:00am).

(iv) Location configuration. Enable a user to set the storage location to which the export summary or export summaries are intended to be saved.

(7) Data segmentation for privacy – send. Enable a user to create a summary record formatted in accordance with the standard adopted in § 170.205(a)(4) that is document-level tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1).

(8) Data segmentation for privacy – receive. Enable a user to:

(i) Receive a summary record that is formatted in accordance with the standard adopted in § 170.205(a)(4) that is document-level tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1);

(ii) Sequester the document-level tagged document from other documents received; and

(iii) View the restricted document without incorporating any of the data from the document.

(9) Care plan. Enable a user to record, change, access, create, and receive care plan information in accordance with the Care Plan document template, including the Health Status Evaluations and Outcomes Section and Interventions Section (V2), in the standard specified in § 170.205(a)(4).

(c) Clinical quality measures--(1) Clinical quality measures – record and export--(i) Record. For each and every CQM for which the technology is presented for certification, the technology must be able to record all of the data that would be necessary to calculate each CQM. Data required for CQM exclusions or exceptions must be codified entries, which may include specific terms as defined by each CQM, or may include codified expressions of "patient reason," "system reason," or "medical reason."

(ii) Export. A user must be able to export a data file at any time the user chooses and without subsequent developer assistance to operate:

(A) Formatted in accordance with the standard specified in § 170.205(h)(2);

(B) Ranging from one to multiple patients; and

(C) That includes all of the data captured for each and every CQM to which technology was certified under paragraph (c)(1)(i) of this section.

(2) Clinical quality measures – import and calculate--(i) Import. Enable a user to import a data file in accordance with the standard specified in § 170.205(h)(2) for one or multiple patients and use such data to perform the capability specified in paragraph (c)(2)(ii) of this section. A user must be able to execute this capability at any time the user chooses and without subsequent developer assistance to operate.

(ii) Calculate each and every clinical quality measure for which it is presented for certification.

(3) Clinical quality measures--report. Enable a user to electronically create a data file for transmission of clinical quality measurement data:

(i) At a minimum, in accordance with the standards specified in § 170.205(h)(2) and § 170.205(k)(1) and (2).

(ii) Optional. That can be electronically accepted by CMS.

(4) Clinical quality measures – filter. (i) Record the data listed in paragraph (c)(4)(iii) of this section in accordance with the identified standards, where specified.

(ii) Filter CQM results at the patient and aggregate levels by each one and any combination of the data listed in paragraph (c)(4)(iii) of this section and be able to:

(A) Create a data file of the filtered data in accordance with the standards adopted in § 170.205(h)(2) and § 170.205(k)(1) and (2); and

(B) Display the filtered data results in human readable format.

(iii) Data.

(A) Taxpayer Identification Number.

(B) National Provider Identifier.

(C) Provider type in accordance with, at a minimum, the standard specified in § 170.207(r)(1).

(D) Practice site address.

(E) Patient insurance in accordance with, at a minimum, the standard specified in § 170.207(s)(1).

(F) Patient age.

(G) Patient sex in accordance with, at a minimum, the version of the standard specified in § 170.207(n)(1).

(H) Patient race and ethnicity in accordance with, at a minimum, the version of the standard specified in § 170.207(f)(2).

(I) Patient problem list data in accordance with, at a minimum, the version of the standard specified in § 170.207(a)(4).

(d) Privacy and security--(1) Authentication, access control, and authorization. (i) Verify against a unique identifier(s) (e.g., username or number) that a user seeking access to electronic health information is the one claimed; and

(ii) Establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided in paragraph (d)(1)(i) of this section, and the actions the user is permitted to perform with the technology.

(2) Auditable events and tamper-resistance--(i) Record actions. Technology must be able to:

(A) Record actions related to electronic health information in accordance with the standard specified in § 170.210(e)(1);

(B) Record the audit log status (enabled or disabled) in accordance with the standard specified in § 170.210(e)(2) unless it cannot be disabled by any user; and

(C) Record the encryption status (enabled or disabled) of electronic health information locally stored on end-user devices by technology in accordance with the standard specified in § 170.210(e)(3) unless the technology prevents electronic health information from being locally stored on end-user devices (see paragraph (d)(7) of this section).

(ii) Default setting. Technology must be set by default to perform the capabilities specified in paragraph (d)(2)(i)(A) of this section and, where applicable, paragraphs (d)(2)(i)(B) and (d)(2)(i)(C) of this section.

(iii) When disabling the audit log is permitted. For each capability specified in paragraphs (d)(2)(i)(A) through (C) of this section that technology permits to be disabled, the ability to do so must be restricted to a limited set of users.

(iv) Audit log protection. Actions and statuses recorded in accordance with paragraph (d)(2)(i) of this section must not be capable of being changed, overwritten, or deleted by the technology.

(v) Detection. Technology must be able to detect whether the audit log has been altered.

(3) Audit report(s). Enable a user to create an audit report for a specific time period and to sort entries in the audit log according to each of the data specified in the standards in § 170.210(e).

(4) Amendments. Enable a user to select the record affected by a patient's request for amendment and perform the capabilities specified in paragraph (d)(4)(i) or (ii) of this section.

(i) Accepted amendment. For an accepted amendment, append the amendment to the affected record or include a link that indicates the amendment's location.

(ii) Denied amendment. For a denied amendment, at a minimum, append the request and denial of the request in at least one of the following ways:

(A) To the affected record.

(B) Include a link that indicates this information's location.

(5) Automatic access time-out. (i) Automatically stop user access to health information after a predetermined period of inactivity.

(ii) Require user authentication in order to resume or regain the access that was stopped.

(6) Emergency access. Permit an identified set of users to access electronic health information during an emergency.

(7) End-user device encryption. The requirements specified in one of the following paragraphs (that is, paragraphs (d)(7)(i) and (d)(7)(ii) of this section) must be met to satisfy this certification criterion.

(i) Technology that is designed to locally store electronic health information on end-user devices must encrypt the electronic health information stored on such devices after use of the technology on those devices stops.

(A) Electronic health information that is stored must be encrypted in accordance with the standard specified in § 170.210(a)(2).

(B) Default setting. Technology must be set by default to perform this capability and, unless this configuration cannot be disabled by any user, the ability to change the configuration must be restricted to a limited set of identified users.

(ii) Technology is designed to prevent electronic health information from being locally stored on end-user devices after use of the technology on those devices stops.

(8) Integrity. (i) Create a message digest in accordance with the standard specified in § 170.210(c)(2).

(ii) Verify in accordance with the standard specified in § 170.210(c)(2) upon receipt of electronically exchanged health information that such information has not been altered.

(9) Trusted connection. Establish a trusted connection using one of the following methods:

(i) Message-level. Encrypt and integrity protect message contents in accordance with the standards specified in § 170.210(a)(2) and (c)(2).

(ii) Transport-level. Use a trusted connection in accordance with the standards specified in § 170.210(a)(2) and (c)(2).

(10) Auditing actions on health information. (i) By default, be set to record actions related to electronic health information in accordance with the standard specified in § 170.210(e)(1).

(ii) If technology permits auditing to be disabled, the ability to do so must be restricted to a limited set of users.

(iii) Actions recorded related to electronic health information must not be capable of being changed, overwritten, or deleted by the technology.

(iv) Technology must be able to detect whether the audit log has been altered.

(11) Accounting of disclosures. Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in § 170.210(d).

(e) Patient engagement—(1) View, download, and transmit to 3rd party. (i) Patients (and their authorized representatives) must be able to use internet-based technology to view, download, and transmit their health information to a 3rd party in the manner specified below. Such access must be consistent and in accordance with the standard adopted in § 170.204(a)(1) and may alternatively be demonstrated in accordance with the standard specified in § 170.204(a)(2).

(A) View. Patients (and their authorized representatives) must be able to use health IT to view, at a minimum, the following data:

(1) The Common Clinical Data Set (which should be in their English (i.e., non-coded) representation if they associate with a vocabulary/code set).

(2) Ambulatory setting only. Provider's name and office contact information.

(3) Inpatient setting only. Admission and discharge dates and locations; discharge instructions; and reason(s) for hospitalization.

(4) Laboratory test report(s). Laboratory test report(s), including:

(i) The information for a test report as specified all the data specified in 42 CFR 493.1291(c)(1) through (7);

(ii) The information related to reference intervals or normal values as specified in 42 CFR 493.1291(d); and

(iii) The information for corrected reports as specified in 42 CFR 493.1291(k)(2).

(5) Diagnostic image report(s).

(B) Download. (1) Patients (and their authorized representatives) must be able to use technology to download an ambulatory summary or inpatient summary (as applicable to the health IT setting for which certification is requested) in the following formats:

(i) Human readable format; and

(ii) The format specified in accordance to the standard specified in § 170.205(a)(4) following the CCD document template.

(2) When downloaded according to the standard specified in § 170.205(a)(4) following the CCD document template, the ambulatory summary or inpatient summary must include, at a minimum, the following data (which, for the human readable version, should be in their English representation if they associate with a vocabulary/code set):

(i) Ambulatory setting only. All of the data specified in paragraph (e)(1)(i)(A)(1), (2), (4), and (5) of this section.

(ii) Inpatient setting only. All of the data specified in paragraphs (e)(1)(i)(A)(1), and (3) through (5) of this section.

(3) Inpatient setting only. Patients (and their authorized representatives) must be able to download transition of care/referral summaries that were created as a result of a transition of care (pursuant to the capability expressed in the certification criterion specified in paragraph (b)(1) of this section).

(C) Transmit to third party. Patients (and their authorized representatives) must be able to:

(1) Transmit the ambulatory summary or inpatient summary (as applicable to the health IT setting for which certification is requested) created in paragraph (e)(1)(i)(B)(2) of this section in accordance with both of the following ways:

(i) Email transmission to any email address; and

(ii) An encrypted method of electronic transmission.

(2) Inpatient setting only. Transmit transition of care/referral summaries (as a result of a transition of care/referral as referenced by (e)(1)(i)(B)(3)) of this section selected by the patient (or their authorized representative) in both of the ways referenced (e)(1)(i)(C)(1)(i) and (ii) of this section).

(D) Timeframe selection. With respect to the data available to view, download, and transmit as referenced paragraphs (e)(1)(i)(A), (B), and (C) of this section, patients (and their authorized representatives) must be able to:

(1) Select data associated with a specific date (to be viewed, downloaded, or transmitted); and

(2) Select data within an identified date range (to be viewed, downloaded, or transmitted).

(ii) Activity history log. (A) When any of the capabilities included in paragraphs (e)(1)(i)(A) through (C) of this section are used, the following information must be recorded and made accessible to the patient:

(1) The action(s) (i.e., view, download, transmission) that occurred;

(2) The date and time each action occurred in accordance with the standard specified in § 170.210(g);

(3) The user who took the action; and

(4) Where applicable, the addressee to whom an ambulatory summary or inpatient summary was transmitted.

(B) Technology presented for certification may demonstrate compliance with paragraph (e)(1)(ii)(A) of this section if it is also certified to the certification criterion specified in § 170.315(d)(2) and the information required to be recorded in paragraph (e)(1)(ii)(A) of this section is accessible by the patient.

(2) Secure messaging. Enable a user to send messages to, and receive messages from, a patient in a secure manner.

(3) Patient health information capture. Enable a user to:

(i) Identify, record, and access information directly and electronically shared by a patient (or authorized representative).

(ii) Reference and link to patient health information documents.

(f) Public health--(1) Transmission to immunization registries. (i) Create immunization information for electronic transmission in accordance with:

(A) The standard and applicable implementation specifications specified in § 170.205(e)(4).

(B) At a minimum, the version of the standard specified in § 170.207(e)(3) for historical vaccines.

(C) At a minimum, the version of the standard specified in § 170.207(e)(4) for administered vaccines.

(ii) Enable a user to request, access, and display a patient's evaluated immunization history and the immunization forecast from an immunization registry in accordance with the standard at § 170.205(e)(4).

(2) Transmission to public health agencies—syndromic surveillance. Create syndrome-based public health surveillance information for electronic transmission in accordance with the standard (and applicable implementation specifications) specified in § 170.205(d)(4).

(3) Transmission to public health agencies – reportable laboratory tests and values/results. Create reportable laboratory tests and values/results for electronic transmission in accordance with:

(i) The standard (and applicable implementation specifications) specified in § 170.205(g).

(ii) At a minimum, the versions of the standards specified in § 170.207(a)(3) and (c)(2).

(4) Transmission to cancer registries. Create cancer case information for electronic transmission in accordance with:

(i) The standard (and applicable implementation specifications) specified in § 170.205(i)(2).

(ii) At a minimum, the versions of the standards specified in § 170.207(a)(4) and (c)(3).

(5) Transmission to public health agencies – electronic case reporting. (i) Consume and maintain a table of trigger codes to determine which encounters may be reportable.

(ii) Match a patient visit or encounter to the trigger code based on the parameters of the trigger code table.

(iii) Case report creation. Create a case report for electronic transmission:

(A) Based on a matched trigger from paragraph (f)(5)(ii).

(B) That includes, at a minimum:

(1) The Common Clinical Data Set.

(2) Encounter diagnoses. Formatted according to at least one of the following standards:

(i) The standard specified in § 170.207(i).

(ii) At a minimum, the version of the standard specified in § 170.207(a)(4).

(3) The provider's name, office contact information, and reason for visit.

(4) An identifier representing the row and version of the trigger table that triggered the case report.

(6) Transmission to public health agencies – antimicrobial use and resistance reporting. Create antimicrobial use and resistance reporting information for electronic transmission in accordance with the standard specified in § 170.205(r)(1).

(7) Transmission to public health agencies – health care surveys. Create health care survey information for electronic transmission in accordance with the standard specified in § 170.205(s)(1).

(g) Design and performance--(1) Automated numerator recording. For each EHR Incentive Programs percentage-based measure, technology must be able to create a report or file that enables a user to review the patients or actions that would make the patient or action eligible to be included in the measure's numerator. The information in the report or file created must be of sufficient detail such that it enables a user to match those patients or actions to meet the measure's denominator limitations when necessary to generate an accurate percentage.

(2) Automated measure calculation. For each EHR Incentive Programs percentage-based measure that is supported by a capability included in a technology, record the numerator and denominator and create a report including the numerator, denominator, and resulting percentage associated with each applicable measure.

(3) Safety-enhanced design. (i) User-centered design processes must be applied to each capability technology includes that is specified in the following certification criteria: paragraphs (a)(1) through (9) and (14), (b)(2) and (3) of this section.

(ii) Number of test participants. A minimum of 10 test participants must be used for the testing of each capability identified in paragraph (g)(3)(i) of this section.

(iii) One of the following must be submitted on the user-centered design processed used:

(A) Name, description and citation (URL and/or publication citation) for an industry or federal government standard.

(B) Name the process(es), provide an outline of the process(es), a short description of the process(es), and an explanation of the reason(s) why use of any of the existing user-centered design standards was impractical.

(iv) The following information/sections from NISTIR 7742 must be submitted for each capability to which user-centered design processes were applied:

(A) Name and product version; date and location of the test; test environment; description of the intended users; and total number of participants;

(B) Description of participants, including: sex; age; education; occupation/role; professional experience; computer experience; and product experience;

(C) Description of the user tasks that were tested and association of each task to corresponding certification criteria;

(D) The specific metrics captured during the testing of each user task performed in (g)(3)(iv)(C) of this section, which must include: task success (%); task failures (%); task standard deviations (%); task performance time; and user satisfaction rating (based on a scale with 1 as very difficult and 5 as very easy) or an alternative acceptable user satisfaction measure;

(E) Test results for each task using the metrics identified above in paragraph (g)(3)(iv)(D) of this section; and

(F) Results and data analysis narrative, including: major test finding; effectiveness; efficiency; satisfaction; and areas for improvement.

(v) Submit test scenarios used in summative usability testing.

(4) Quality management system. (i) For each capability that a technology includes and for which that capability's certification is sought, the use of a Quality Management System (QMS) in the development, testing, implementation, and maintenance of that capability must be identified that satisfies one of the following ways:

(A) The QMS used is established by the Federal government or a standards developing organization.

(B) The QMS used is mapped to one or more QMS established by the Federal government or standards developing organization(s).

(ii) When a single QMS was used for applicable capabilities, it would only need to be identified once.

(iii) When different QMS were applied to specific capabilities, each QMS applied would need to be identified.

(5) Accessibility-centered design. For each capability that a Health IT Module includes and for which that capability's certification is sought, the use of a health IT accessibility-centered design standard or law in the development, testing, implementation and maintenance of that capability must be identified.

(i) When a single accessibility-centered design standard or law was used for applicable capabilities, it would only need to be identified once.

(ii) When different accessibility-centered design standards and laws were applied to specific capabilities, each accessibility-centered design standard or law applied would need to be identified. This would include the application of an accessibility-centered design standard or law to some capabilities and none to others.

(iii) When no accessibility-centered design standard or law was applied to all applicable capabilities such a response is acceptable to satisfy this certification criterion.

(6) Consolidated CDA creation performance. The following technical and performance outcomes must be demonstrated related to Consolidated CDA creation. The capabilities required under paragraphs (g)(6)(i) through (iv) of this section can be demonstrated in tandem and do not need to be individually addressed in isolation or sequentially. This certification criterion's scope includes only data expressed within the Common Clinical Data Set definition.

(i) Reference C-CDA match. Create a data file formatted in accordance with the standard adopted in § 170.205(a)(4) that matches a gold-standard, reference data file.

(ii) Document-template conformance. Create a data file formatted in accordance with the standard adopted in § 170.205(a)(4) that demonstrates a valid implementation of each document template applicable to the certification criterion or criteria within the scope of the certificate sought. The scope of this certification criterion will not exceed the evaluation of the CCD, Referral Note, and Discharge Summary document templates.

(iii) Vocabulary conformance. Create a data file formatted in accordance with the standard adopted in § 170.205(a)(4) that demonstrates the required vocabulary standards (and value sets) are properly implemented.

(iv) Completeness verification. Create a data file for each of the applicable document templates referenced in paragraph (g)(6)(ii) of this section without the omission of any of the data included in the Common Clinical Data Set definition.

(7) Application access – patient selection. The following technical outcome and conditions must be met through the demonstration of an application programming interface (API).

(i) Functional requirement. The technology must be able to receive a request with sufficient information to uniquely identify a patient and return an ID or other token that can be used by an application to subsequently execute requests for that patient's data.

(ii) Documentation--(A) The API must include accompanying documentation that contains, at a minimum:

(1) API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(2) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(3) Terms of use. The terms of use for the API must be provided, including, at a minimum, any associated developer policies and required developer agreements.

(B) The documentation used to meet paragraph (g)(7)(ii)(A) of this section must be available via a publicly accessible hyperlink.

(8) Application access – data category request. The following technical outcome and conditions must be met through the demonstration of an application programming interface.

(i) Functional requirements. (A) Respond to requests for patient data (based on an ID or other token) for each of the individual data categories specified in the Common Clinical Data Set and

return the full set of data for that data category (according to the specified standards, where applicable) in a computable format.

(B) Respond to requests for patient data associated with a specific date as well as requests for patient data within a specified date range.

(ii) Documentation--(A) The API must include accompanying documentation that contains, at a minimum:

(1) API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(2) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(3) Terms of use. The terms of use for the API must be provided, including, at a minimum, any associated developer policies and required developer agreements.

(B) The documentation used to meet paragraph (g)(8)(ii)(A) of this section must be available via a publicly accessible hyperlink.

(9) Application access – all data request. The following technical outcome and conditions must be met through the demonstration of an application programming interface.

(i) Functional requirements. (A) Respond to requests for patient data (based on an ID or other token) for all of the data categories specified in the Common Clinical Data Set at one time and return such data (according to the specified standards, where applicable) in a summary record formatted according to the standard specified in § 170.205(a)(4) following the CCD document template.

(B) Respond to requests for patient data associated with a specific date as well as requests for patient data within a specified date range.

(ii) Documentation--(A) The API must include accompanying documentation that contains, at a minimum:

(1) API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(2) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(3) Terms of use. The terms of use for the API must be provided, including, at a minimum, any associated developer policies and required developer agreements.

(B) The documentation used to meet paragraph (g)(9)(ii)(A) of this section must be available via a publicly accessible hyperlink.

(h) Transport methods and other protocols--(1) Direct Project--(i) Applicability Statement for Secure Health Transport. Able to send and receive health information in accordance with the standard specified in § 170.202(a)(2), including formatted only as a "wrapped" message.

(ii) Applicability Statement for Secure Health Transport and Delivery Notification in Direct. Able to send and receive health information in accordance with the standard specified in § 170.202(e)(1).

(2) Direct Project, Edge Protocol, and XDR/XDM--(i) Able to send and receive health information in accordance with:

(A) The standard specified in § 170.202(a)(2), including formatted only as a "wrapped" message;

(B) The standard specified in § 170.202(b), including support for both limited and full XDS metadata profiles; and

(C) Both edge protocol methods specified by the standard in § 170.202(d).

(ii) Applicability Statement for Secure Health Transport and Delivery Notification in Direct. Able to send and receive health information in accordance with the standard specified in § 170.202(e)(1).

§§ 170.500, 170.501, 170.502, 170.503, 170.504, 170.505, 170.510, 170.520, 170.523, 170.525, 170.530, 170.535, 170.540, 170.545, 170.550, 170.553, 170.555, 170.557, 170.560, 170.565, 170.570, 170.575, and 170.599 [Amended]

13. In subpart E, consisting of §§ 170.500 through 170.599:

a. Remove the term ‘‘ONC HIT Certification Program” and add in its place “ONC Health IT Certification Program” wherever it may appear;

b. Remove the acronym ‘‘HIT” and add in its place ‘‘health IT” wherever it may appear;

c. Remove the term “EHR Module” and add in its place “Health IT Module” wherever it may appear;

d. Remove the term “EHR Modules” and add in its place “Health IT Modules” wherever it may appear; and

e. Remove the term “EHR Module(s)” and add in its place “Health IT Module(s)” wherever it may appear.

14. In § 170.503, revise paragraph (e)(4) to read as follows:

§ 170.503 Requests for ONC-AA status and ONC-AA ongoing responsibilities.

* * * * *

(e) * * *

(4) Verify that ONC-ACBs are performing surveillance as required by and in accordance with § 170.556, § 170.523(k), and their respective annual plans; and

* * * * *

15. Amend § 170.523 by—

a. Revising paragraphs (f), (g), (i), and (k); and

b. Adding paragraphs (m) and (n).

The additions and revisions read as follows:

§ 170.523 Principles of proper conduct for ONC-ACBs.

* * * * *

(f) Provide ONC, no less frequently than weekly, a current list of Health IT Modules, Complete EHRs, and/or EHR Modules that have been certified that includes, at a minimum:

(1) For the 2015 Edition health IT certification criteria and subsequent editions of health IT certification criteria:

(i) The Health IT Module developer name; product name; product version; developer website, physical address, email, phone number, and contact name;

(ii) The ONC-ACB website, physical address, email, phone number, and contact name, contact function/title;

(iii) The ATL website, physical address, email, phone number, and contact name, contact function/title;

(iv) Location and means by which the testing was conducted (e.g., remotely with health IT developer at its headquarters location);

(v) The date(s) the Health IT Module was tested;

(vi) The date the Health IT Module was certified;

(vii) The unique certification number or other specific product identification;

(viii) The certification criterion or criteria to which the Health IT Module has been certified, including the test procedure and test data versions used, test tool version used, and whether any test data was altered (i.e., a yes/no) and for what purpose;

(ix) The way in which each privacy and security criterion was addressed for the purposes of certification;

(x) The standard or mapping used to meet the quality management system certification criterion;

(xi) The standard(s) or lack thereof used to meet the accessibility-centered design certification criterion;

(xii) Where applicable, the hyperlink to access an application programming interface (API)'s documentation and terms of use;

(xiii) Where applicable, which certification criteria were gap certified;

(xiv) Where applicable, if a certification issued was a result of an inherited certified status request;

(xv) Where applicable, the clinical quality measures to which the Health IT Module has been certified;

(xvi) Where applicable, any additional software a Health IT Module relied upon to demonstrate its compliance with a certification criterion or criteria adopted by the Secretary;

(xvii) Where applicable, the standard(s) used to meet a certification criterion where more than one is permitted;

(xviii) Where applicable, any optional capabilities within a certification criterion to which the Health IT Module was tested and certified;

(xix) Where applicable, and for each applicable certification criterion, all of the information required to be submitted by Health IT Module developers to meet the safety-enhanced design

certification criterion. Each user-centered design element required to be reported must be at a granular level (e.g., task success/failure));

(xx) A hyperlink to the disclosures required by § 170.523(k)(1) for the Health IT Module;

(xxi) The attestation required by § 170.523(k)(2);

(xxii) When applicable, for each instance in which a Health IT Module failed to conform to its certification and for which corrective action was instituted under § 170.556 (provided no provider or practice site is identified):

(A) The specific certification requirements to which the technology failed to conform, as determined by the ONC-ACB;

(B) A summary of the deficiency or deficiencies identified by the ONC-ACB as the basis for its determination of non-conformity;

(C) When available, the health IT developer's explanation of the deficiency or deficiencies;

(D) The dates surveillance was initiated and completed;

(E) The results of randomized surveillance, including pass rate for each criterion in instances where the Health IT Module is evaluated at more than one location;

(F) The number of sites that were used in randomized surveillance;

(G) The date of the ONC-ACB's determination of non-conformity;

(H) The date on which the ONC-ACB approved a corrective action plan;

(I) The date corrective action began (effective date of approved corrective action plan);

(J) The date by which corrective action must be completed (as specified by the approved corrective action plan);

(K) The date corrective action was completed; and

(L) A description of the resolution of the non-conformity or non-conformities.

(2) For the 2014 Edition EHR certification criteria:

(i) The Complete EHR or EHR Module developer name (if applicable);

(ii) The date certified;

(iii) The product version;

(iv) The unique certification number or other specific product identification;

(v) The clinical quality measures to which a Complete EHR or EHR Module has been certified;

(vi) Where applicable, any additional software a Complete EHR or EHR Module relied upon to demonstrate its compliance with a certification criterion or criteria adopted by the Secretary;

(vii) Where applicable, the certification criterion or criteria to which each EHR Module has been certified; and

(viii) A hyperlink to the test results used to certify the Complete EHRs and/or EHR Modules that can be accessed by the public.

(ix) A hyperlink to the disclosures required by § 170.523(k)(1) for the Complete EHRs and/or EHR Modules; and

(x) The attestation required by § 170.523(k)(2); and

(xi) <u>When applicable</u>, for each instance in which a Complete EHR or EHR Module failed to conform to its certification and for which corrective action was instituted under § 170.556 (provided no provider or practice site is identified):

(A) The specific certification requirements to which the technology failed to conform, as determined by the ONC-ACB;

(B) A summary of the deficiency or deficiencies identified by the ONC-ACB as the basis for its determination of non-conformity;

(C) When available, the health IT developer's explanation of the deficiency or deficiencies;

(D) The dates surveillance was initiated and completed;

(E) The results of randomized surveillance, including pass rate for each criterion in instances where the Complete EHR or EHR Module is evaluated at more than one location;

(F) The number of sites that were used in randomized surveillance;

(G) The date of the ONC-ACB's determination of non-conformity;

(H) The date on which the ONC-ACB approved a corrective action plan;

(I) The date corrective action began (effective date of approved corrective action plan);

(J) The date by which corrective action must be completed (as specified by the approved corrective action plan);

(K) The date corrective action was completed; and

(L) A description of the resolution of the non-conformity or non-conformities.

(g) Records retention. (1) Retain all records related to the certification of Complete EHRs and Health IT Modules to an edition of certification criteria for a minimum of 3 years from the effective date that removes the applicable edition from the Code of Federal Regulations; and

(2) Make the records available to HHS upon request during the retention period described in paragraph (g)(1) of this section;

* * * * *

(i) Surveillance plan. Submit an annual surveillance plan to the National Coordinator and, in accordance with its surveillance plan, its accreditation, and § 170.556:

(1) Conduct surveillance of certified Complete EHRs and Health IT Modules; and

(2) Report, at a minimum, on a quarterly basis to the National Coordinator the results of its surveillance.

* * * * *

(k) Ensure adherence to the following requirements when issuing any certification and during surveillance of Complete EHRs and Health IT Modules the ONC-ACB has certified.

(1) Mandatory disclosures. A Health IT developer must conspicuously include the following on its website and in all marketing materials, communications statements, and other assertions related to the Complete EHR or Health IT Module's certification:

(i) The disclaimer "This [Complete EHR or Health IT Module] is [specify Edition of EHR certification criteria] compliant and has been certified by an ONC-ACB in accordance with the applicable certification criteria adopted by the Secretary of Health and Human Services. This certification does not represent an endorsement by the U.S. Department of Health and Human Services."

(ii) The following information an ONC-ACB is required to report to the National Coordinator:

(A) For a Health IT Module certified to 2015 Edition health IT certification criteria, the information specified by paragraphs (f)(1)(i), (vi), (vii), (viii), (xvi), and (xvii) of this section as applicable for the specific Health IT Module.

(B) For a Complete EHR or EHR Module certified to 2014 Edition health IT certification criteria, the information specified by paragraphs (f)(2)(i), (ii), (iv)-(v), and (vii) of this section as applicable for the specific Complete EHR or EHR Module.

(iii) In plain language, a detailed description of all known material information concerning:

(A) Additional types of costs that a user may be required to pay to implement or use the Complete EHR or Health IT Module's capabilities, whether to meet meaningful use objectives and measures or to achieve any other use within the scope of the health IT's certification.

(B) Limitations that a user may encounter in the course of implementing and using the Complete EHR or Health IT Module's capabilities, whether to meet meaningful use objectives and measures or to achieve any other use within the scope of the health IT's certification.

(iv) The types of information required to be disclosed under paragraph (k)(iii) of this section include but are not limited to:

(A) Additional types of costs or fees (whether fixed, recurring, transaction-based, or otherwise) imposed by a health IT developer (or any third-party from whom the developer purchases, licenses, or obtains any technology, products, or services in connection with its certified health IT) to purchase, license, implement, maintain, upgrade, use, or otherwise enable and support the use of capabilities to which health IT is certified; or in connection with any data generated in the course of using any capability to which health IT is certified.

(B) Limitations, whether by contract or otherwise, on the use of any capability to which technology is certified for any purpose within the scope of the technology's certification; or in connection with any data generated in the course of using any capability to which health IT is certified.

(C) Limitations, including but not limited to technical or practical limitations of technology or its capabilities, that could prevent or impair the successful implementation, configuration, customization, maintenance, support, or use of any capabilities to which technology is certified; or that could prevent or limit the use, exchange, or portability of any data generated in the course of using any capability to which technology is certified.

(v) Health IT self-developers are excluded from the requirements of paragraph (k)(1)(iii) of this section.

(2) Transparency attestation. As a condition of a Complete EHR or Health IT Module's certification to any certification criterion, a health IT developer must make one of the following attestations:

(i) An attestation that it will voluntarily and timely provide, in plain writing and in a manner calculated to inform, any part (including all of) the information required to be disclosed under paragraph (k)(1) of this section,

(A) to all customers, prior to providing or entering into any agreement to provide any certified health IT or related product or service (including subsequent updates, add-ons, or additional products or services during the course of an on-going agreement);

(B) to any person who requests or receives a quotation, estimate, description of services, or other assertion or information from the developer in connection with any certified health IT or any capabilities thereof; and

(C) to any person, upon request.

(ii) An attestation by the developer that it has been asked to make the voluntary transparency attestation described by paragraph (k)(2)(i) of this section and has elected not to make such attestation.

(3) A certification issued to a pre-coordinated, integrated bundle of Health IT Modules shall be treated the same as a certification issued to a Complete EHR for the purposes of paragraph (k)(1) of this section, except that the certification must also indicate each Health IT Module that is included in the bundle; and

(4) A certification issued to a Complete EHR or Health IT Module based solely on the applicable certification criteria adopted by the Secretary at subpart C of this part must be separate and distinct from any other certification(s) based on other criteria or requirements.

* * * * *

(m) Adaptations and updates. On a quarterly basis each calendar year, obtain a record of:

(1) All adaptations of certified Complete EHRs and certified Health IT Modules; and

(2) All updates made to certified Complete EHRs and certified Health IT Modules affecting the capabilities in certification criteria to which the "safety-enhanced design" criteria apply.

(n) Complaints reporting. Submit a list of complaints received to the National Coordinator on a quarterly basis each calendar year that includes the number of complaints received, the nature/substance of each complaint, and the type of complainant for each complaint.

16. Amend § 170.550 by—

a. Redesignating paragraph (g) as paragraph (k);

b. Adding paragraphs (g), (h) and (j); and

c. Adding reserved paragraph (i).

The additions read as follows:

§ 170.550 Health IT Module certification.

* * * * *

(g) When certifying a Health IT Module to the 2015 Edition health IT certification criteria, an ONC-ACB must certify the Health IT Module in accordance with the certification criteria at:

(1) Section 170.315(g)(3) if the Health IT Module is presented for certification to one or more listed certification criteria in § 170.315(g)(3);

(2) Section 170.315(g)(4);

(3) Section 170.315(g)(5); and

(4) Section 170.315(g)(6) if the Health IT Module is presented for certification with C-CDA creation capabilities within its scope. If the scope of certification sought includes multiple

certification criteria that require C-CDA creation, § 170.315(g)(6) need only be tested in association with one of those certification criteria and would not be expected or required to be tested for each. If the scope of certification sought includes multiple certification criteria that require C-CDA creation, § 170.315(g)(6) need only be tested in association with one of those certification criteria and would not be expected or required to be tested for each so long as all applicable C-CDA document templates have been evaluated as part of § 170.315(g)(6) for the scope of the certification sought.

(h) Privacy and security certification framework--(1) General rule. When certifying a Health IT Module to the 2015 Edition health IT certification criteria, an ONC-ACB can only issue a certification to a Health IT Module if the privacy and security certification criteria in paragraphs (h)(3)(i) through (viii) of this section have also been met (and are included within the scope of the certification).

(2) In order to be issued a certification, a Health IT Module would only need to be tested once to each applicable privacy and security criterion in paragraphs (h)(3)(i) through (viii) of this section so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification, except for the following:

(i) A Health IT Module presented for certification to § 170.315(e)(1) must be separately tested to § 170.315(d)(9); and

(ii) A Health IT Module presented for certification to § 170.315(e)(2) must be separately tested to § 170.315(d)(9).

(3) Applicability. (i) Section 170.315(a) is also certified to the certification criteria specified in § 170.315(d)(1) through (7);

(ii) Section 170.315(b) is also certified to the certification criteria specified in § 170.315(d)(1) through (3) and (d)(5) through (8);

(iii) Section 170.315(c) is also certified to the certification criteria specified in § 170.315(d)(1) through (3), and (5);

(iv) Section 170.315(e)(1) is also certified to the certification criteria specified in § 170.315(d)(1) through (3), (5), (7), and (9);

(v) Section 170.315(e)(2) and (3) is also certified to the certification criteria specified in § 170.315(d)(1) through (3), (5), and (9);

(vi) Section 170.315(f) is also certified to the certification criteria specified in § 170.315(d)(1) through (3) and (7);

(vii) Section 170.315(g)(7), (8) and (9) is also certified to the certification criteria specified in § 170.315(d)(1) and (9); and (d)(2) or (10);

(viii) Section 170.315(h) is also certified to the certification criteria specified in § 170.315(d)(1) through (3); and

(4) Methods to demonstrate compliance with each privacy and security criterion. One of the following methods must be used to meet each applicable privacy and security criterion listed in paragraph (h)(3) of this section:

(i) Directly, by demonstrating a technical capability to satisfy the applicable certification criterion or certification criteria; or

(ii) Demonstrate, through system documentation sufficiently detailed to enable integration, that the Health IT Module has implemented service interfaces for each applicable privacy and security certification criterion that enable the Health IT Module to access external services necessary to meet the privacy and security certification criterion.

(i) [Reserved]

(j) Direct Project transport method. An ONC-ACB can only issue a certification to a Health IT Module for § 170.315(h)(1) if the Health IT Module's certification also includes § 170.315(b)(1).

* * * * *

§ 170.553 [Removed and Reserved]

17. Remove and reserve § 170.553.

18. Add § 170.556 to read as follows:

§ 170.556 In-the-field surveillance and maintenance of certification for Health IT.

(a) In-the-field surveillance. Consistent with its accreditation to ISO/IEC 17065 and the requirements of this subpart, an ONC-ACB must initiate surveillance "in the field" as necessary to assess whether a certified Complete EHR or certified Health IT Module continues to conform to the requirements of its certification once the certified Complete EHR or certified Health IT Module has been implemented and is in use in a production environment.

(1) Production environment. An ONC-ACB's assessment of a certified capability in the field must be based on the use of the capability in a production environment, which means a live environment in which the capability has been implemented and is in use.

(2) Production data. An ONC-ACB's assessment of a certified capability in the field must be based on the use of the capability with production data unless the use of test data is specifically approved by the National Coordinator.

(b) Reactive surveillance. An ONC-ACB must initiate surveillance (including, as necessary, in-the-field surveillance required by paragraph (a) of this section) whenever it becomes aware of facts or circumstances that would cause a reasonable person to question a certified Complete

EHR or certified Health IT Module's continued conformity to the requirements of its certification.

(1) Review of required disclosures. When an ONC-ACB performs reactive surveillance under this paragraph, it must verify that the requirements of § 170.523(k)(1) have been followed as applicable to the issued certification.

(2) [Reserved]

(c) Randomized surveillance. During each calendar year surveillance period, an ONC-ACB must conduct in-the-field surveillance for certain randomly selected Complete EHRs and Health IT Modules to which it has issued a certification.

(1) Scope. When an ONC-ACB selects a certified Complete EHR or certified Health IT Module for randomized surveillance under this paragraph, its evaluation of the certified Complete EHR or certified Health IT Module must include all certification criteria prioritized by the National Coordinator that are part of the scope of the certification issued to the Complete EHR or Health IT Module.

(2) Minimum number of products selected per year. 2% of the Complete EHRs and Health IT Modules to which an ONC-ACB has issued a certification must be subject to randomized surveillance.

(3) Selection method. An ONC-ACB must randomly select (subject to appropriate weighting and sampling considerations) certified Complete EHRs and certified Health IT Modules for surveillance under this paragraph.

(4) Number and types of locations for in-the-field surveillance. For each certified Compete EHR or certified Health IT Module selected for randomized surveillance under this paragraph, an ONC-ACB must:

(i) Evaluate the certified Complete EHR or certified Health IT Module's capabilities at one or more locations where the certified Complete EHR or certified Health IT Module is implemented and in use in the field.

(ii) Ensure that the locations are selected at random (subject to appropriate weighting and sampling considerations) from among all locations where the certified Complete EHR or certified Health IT Module is implemented and in use in the field.

(5) Exclusion and exhaustion. An ONC-ACB must make a good faith effort to complete in-the-field surveillance of a certified Complete EHR or certified Health IT Module at each location selected under paragraph (c)(3) of this section. If the ONC-ACB is unable to complete surveillance at a location due to circumstances beyond its control, the ONC-ACB may substitute a different location that meets the requirements of paragraph (c)(3) of this section. If no such location exists, the ONC-ACB may exclude the certified Complete EHR or certified Health IT Module and substitute a different randomly selected Complete EHR or Health IT Module to which it has issued a certification.

(6) Prohibition on consecutive selection for randomized surveillance. An ONC-ACB is prohibited from selecting a certified Complete EHR or certified Health IT Module for randomized surveillance under this paragraph more than once during any consecutive 12 month period. This limitation does not apply to reactive and other forms of surveillance required under this subpart and the ONC-ACB's accreditation.

(d) Corrective action plan and procedures. (1) When an ONC-ACB determines, through surveillance under this section or otherwise, that a Complete EHR or Health IT Module does not conform to the requirements of its certification, the ONC-ACB must notify the developer of its

findings and require the developer to submit a proposed corrective action plan for the applicable certification criterion, certification criteria, or certification requirement.

(2) The ONC-ACB shall provide direction to the developer as to the required elements of the corrective action plan.

(3) The ONC-ACB shall verify the required elements of the corrective action plan, consistent with its accreditation and any elements specified by the National Coordinator. At a minimum, any corrective action plan submitted by a developer to an ONC-ACB must include:

(i) A description of the identified non-conformities or deficiencies;

(ii) An assessment of how widespread or isolated the identified non-conformities or deficiencies may be across all of the developer's customers and users of the certified Complete EHR or certified Health IT Module;

(iii) How the developer will address the identified non-conformities or deficiencies, both at the locations under which surveillance occurred and for all other potentially affected customers and users;

(iv) How the developer will ensure that all affected and potentially affected customers and users are alerted to the identified non-conformities or deficiencies, including a detailed description of how the developer will assess the scope and impact of the problem, including identifying all potentially affected customers; how the developer will promptly ensure that all potentially affected customers are notified of the problem and plan for resolution; how and when the developer will resolve issues for individual affected customers; and how the developer will ensure that all issues are in fact resolved.

(v) The timeframe under which corrective action will be completed.

(vi) An attestation by the developer that it has completed all elements of the approved corrective action plan.

(4) When the ONC-ACB receives a proposed corrective action plan (or a revised proposed corrective action plan), the ONC-ACB shall either approve the corrective action plan or, if the plan does not adequately address the elements described by paragraph (d)(3) of this section and other elements required by the ONC-ACB, instruct the developer to submit a revised proposed corrective action plan.

(5) Suspension. Consistent with its accreditation to ISO/IEC 17065 and procedures for suspending a certification, an ONC-ACB shall initiate suspension procedures for a Complete EHR or Health IT Module:

(i) 30 days after notifying the developer of a non-conformity pursuant to paragraph (d)(1) of this section, if the developer has not submitted a proposed corrective action plan;

(ii) 90 days after notifying the developer of a non-conformity pursuant to paragraph (d)(1) of this section, if the ONC-ACB cannot approve a corrective action plan because the developer has not submitted a revised proposed corrective action plan in accordance with paragraph (d)(4) of this section; and

(iii) Immediately, if the developer has not completed the corrective actions specified by an approved corrective action plan within the time specified therein.

(6) Termination. If a certified Complete EHR or certified Health IT Module's certification has been suspended in the context of randomized surveillance under this paragraph, an ONC-ACB is permitted to initiate certification termination procedures for the Complete EHR or Health IT Module (consistent with its accreditation to ISO/IEC 17065 and procedures for terminating a

certification) when the developer has not completed the actions necessary to reinstate the suspended certification.

(e) Reporting of surveillance results requirements— (1) Rolling submission of in-the-field surveillance results. The results of in-the-field surveillance under this section must be submitted to the National Coordinator on an ongoing basis throughout the calendar year.

(2) Confidentiality of locations evaluated. The contents of an ONC-ACB's surveillance results submitted to the National Coordinator must not include any information that would identify any user or location that participated in or was subject to surveillance.

(3) Reporting of corrective action plans. When a corrective action plan is initiated for a Complete EHR or Health IT Module, an ONC-ACB must report the Complete EHR or Health IT Module and associated product and corrective action information to the National Coordinator in accordance with § 170.523(f)(1)(xxii) or (f)(2)(xi), as applicable.

(f) Relationship to other surveillance requirements. Nothing in this section shall be construed to limit or constrain an ONC-ACB's duty or ability to perform surveillance, including in-the-field surveillance, or to suspend or terminate the certification, of any certified Complete EHR or certified Health IT Module as required or permitted by this subpart and the ONC-ACB's accreditation to ISO/IEC 17065.

RIN 0991-AB93

Dated: September 25, 2015.

_____

Sylvia M. Burwell,
Secretary.

BILLING CODE: 4150-45-P

[FR Doc. 2015-25597 Filed: 10/6/2015 04:15 pm; Publication Date: 10/16/2015]