ENTERED
SEP 30 2020
FRANKLIN CIRCUIT COURT
AMY FELDMAN, CLERK

**COMMONWEALTH OF KENTUCKY**
**FRANKLIN CIRCUIT COURT**
**DIV. I**
**CIVIL ACTION NO. 20-CI-00771**

**IN THE MATTER OF:**

**ANTHEM, INC.**

## ASSURANCE OF VOLUNTARY COMPLIANCE

Pursuant to KRS 367.230, the Assurance of Voluntary Compliance attached hereto is provided to the Commonwealth of Kentucky, ex. rel. Daniel Cameron, Attorney General, by Anthem, Inc.

WHEREFORE, the parties being in agreement and having agreed to the approval and filing of this Assurance of Voluntary Compliance, the requirements of KRS 367.230 having been met, and the Court being well and sufficiently advised and having jurisdiction and venue pursuant to KRS 367.230, the Assurance of Voluntary Compliance attached hereto is hereby approved. The amount payable to the Commonwealth of Kentucky pursuant to the Assurance of Voluntary Compliance is $1,929,942.02, which includes $1,017,451.83 for the recovery of the Attorney General's reasonable costs of investigation and litigation.

DATE: 9-30-20

Phillip J. Shepherd
JUDGE, FRANKLIN CIRCUIT COURT

## KENTUCKY SPECIFIC PROVISIONS REGARDING THE COURT FILING OF THE ASSURANCE

In relation to the filing of the Assurance in the applicable court in the Commonwealth of Kentucky as required by statute, Anthem, Inc. waives notice and service of process regarding the filing of the Assurance, and does not object to the court's approval and entry of this Assurance. Anthem, Inc. also does not object to the ex parte submission and presentation of this Assurance by the Kentucky Attorney General's Office to the court.

## ASSURANCE OF VOLUNTARY COMPLIANCE

This Assurance of Voluntary Compliance ("Assurance")[1] is entered into by the Attorneys General of Alaska, Arizona, Arkansas, Colorado, Connecticut, the District of Columbia, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Nebraska, New Hampshire, New Jersey, New York, Nevada, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Virginia, Washington, West Virginia, and Wisconsin (collectively, "Attorneys General") and Anthem, Inc. ("Anthem") to resolve the Attorneys General's investigation into the criminal cyberattack on Anthem's systems, which Anthem publicly announced on February 4, 2015 (collectively, the "Parties").[2]

In consideration of their mutual agreements to the terms of this Assurance, and such other consideration as described herein, the sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

## I. INTRODUCTION

This Assurance constitutes a good faith settlement and release between Anthem and the Attorneys General of claims under state law and the federal Health Insurance and Portability & Accountability Act of 1996, Public Law 104-191, and its implementing regulations, 45 C.F.R. §§ 160, 162, and 164 ("HIPAA") related to a data breach, publicly announced by Anthem on February 4, 2015, in which a criminal cyber-attacker gained unauthorized access to its network and infiltrated an internally hosted enterprise data warehouse, which contained the personal information ("PI") and/or protected health information ("PHI") of Anthem plan members and other

[1] This Assurance of Voluntary Compliance shall, for all necessary purposes, also be considered an Assurance of Discontinuance.

[2] The State of California has simultaneously entered into a settlement with Anthem in a form consistent with California law.

individuals (the "Data Breach"). Anthem discovered the unauthorized access that caused the Data Breach on or about January 29, 2015. The Data Breach affected approximately 78,800,000 individuals nationwide. The information accessed in unencrypted form by the cyber-attacker included names, dates of birth, Social Security numbers, healthcare identification numbers, home addresses, email addresses, phone numbers, and employment information, including income data.

## II. DEFINITIONS

1. For purposes of this Assurance, the following definitions shall apply:

   A. "Anthem" shall mean Anthem, Inc., its wholly owned, integrated, and operated affiliates, subsidiaries, and divisions, successors, and assigns, directors and officers, and employees doing business in the United States.

   B. "Anthem Network" shall mean the networking equipment, databases or data stores, applications, servers, and endpoints that are capable of using and sharing software, data, and hardware resources and that are owned and/or operated by Anthem.

   C. "Business Associate" shall be defined in accordance with 45 C.F.R. § 160.103 and is a person or entity that provides certain services to or performs functions on behalf of covered entities, or other business associates of covered entities, that require access to PHI.

   D. "Consumer Protection Acts" shall mean the State citations listed in Appendix A.

   E. "Covered Entity" shall be defined in accordance with 45 C.F.R. § 160.103 as a health plan, health care clearinghouse, or health care provider that transmits protected health information in electronic form in connection with

a transaction for which the U.S. Department of Health and Human Services has adopted standards.

F. "Covered Systems" shall mean components, such as servers, workstations, and devices, within the Anthem Network that are routinely used to collect, process, communicate, and/or store PI and/or PHI.

G. "Data Breach" shall mean the security incident discovered by Anthem on or about January 29, 2015, and publicly announced on February 4, 2015, in which a malicious cyber-attacker gained unauthorized access to portions of the Anthem Network that stored PI and/or PHI, and which impacted approximately 78,800,000 individuals nationwide.

H. "Data Breach Notification Law" shall mean the State citations listed in Appendix B.

I. "Effective Date" shall be October 30, 2020.

J. "Encrypt," "Encrypted," or "Encryption" shall refer to the transformation of data at rest or in transit into a form in which meaning cannot be assigned without the use of a confidential process or key. The manner of Encryption shall conform to existing industry standard.[3]

K. "Minimum Necessary Standard" shall refer to the requirements of the Privacy Rule that, when using or disclosing Protected Health Information or when requesting Protected Health Information from another Covered Entity or Business Associate, a Covered Entity or Business Associate must

[3] For the purposes of this Assurance, the term "existing industry standard" applies to what the standard may become as the industry changes over time. As of the Effective Date, the existing industry standard shall be defined pursuant to Federal Information Processing Standards Publication 140-2.

make reasonable efforts to limit Protected Health Information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request as defined in 45 C.F.R. § 164.502(b) and § 164.514(d).

L. "Multi-factor Authentication" means authentication through verification of at least two of the following authentication factors: (i) knowledge factors, such as a password; or (ii) possession factors, such as a token, connection through a known authenticated source, or a text message on a mobile phone; or (iii) inherent factors, such as biometric characteristics.

M. "Personal Information" or "PI" shall mean the data elements in the definition of personal information set forth in the Data Breach Notification Law and/or Personal Information Protection Act listed in Appendix B.

N. "Personal Information Protection Act" shall mean the State citations listed in Appendix B.

O. "Privacy Rule" shall refer to the HIPAA Regulations that establish national standards for safeguarding individuals' medical records and other Protected Health Information, including electronic PHI, that is created, received, used, or maintained by a Covered Entity or a Business Associate, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E.

P. "Protected Health Information" or "PHI" shall be defined in accordance with 45 C.F.R. § 160.103, including electronic protected health information.

Q. "Security Event" shall mean any compromise that (i) results in the unauthorized access, acquisition, or exfiltration of electronic PI or PHI

collected, processed, transmitted, stored, or disposed of by Anthem, or (ii) causes lack of enterprise availability of electronic PI or PHI of at least 500 U.S. consumers held, processed, or stored by Anthem.

R. "Security Rule" shall refer to the HIPAA Regulations that establish national standards to safeguard individuals' electronic Protected Health Information that is created, received, used, or maintained by a Covered Entity or Business Associate that performs certain services on behalf of the Covered Entity, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C.

## III. ASSURANCES

### A. Compliance with State and Federal Law

2. Anthem shall not misrepresent the extent to which Anthem maintains and protects the privacy, security, or confidentiality of any PI or PHI collected from or about consumers.

3. If a Security Event does not trigger the Data Breach Notification Law, Anthem shall create a report that includes a description of the Security Event and Anthem's response to that Security Event ("Security Event Report"). The Security Event Report shall be made available for inspection by the Third-Party Security Assessor as described in Paragraph 27.

### B. Information Security Program

4. Anthem shall develop, implement, and maintain a written information security program ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of PI and PHI that Anthem collects, stores, transmits, maintains, and/or destroys. The Information Security Program shall, at a minimum, include the specific information security requirements set forth in Paragraphs 5 through 25 of this Assurance.

a. The Information Security Program shall comply with any applicable requirements under state or federal law, and shall contain administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of Anthem's operations; (ii) the nature and scope of Anthem's activities; and (iii) the sensitivity of the PI and PHI that Anthem collects, stores, transmits and/or maintains.

b. The Information Security Program shall be written and modified to allow access to PHI consistent with the Minimum Necessary Standard. Anthem shall consider and adopt where reasonably feasible the principles of zero trust architecture throughout the Anthem Network. As used herein, zero trust architecture means Anthem will:

i. Regularly monitor, log, and inspect network traffic, including log-in attempts, through the implementation of hardware, software, or procedural mechanisms that record and evaluate such activity;

ii. Authorize and authenticate relevant device, user, and network activity within the Anthem Network; and

iii. Require appropriate authorization and authentication prior to any user's access to the Anthem Network.

c. Anthem may satisfy the requirements of this Assurance, including the implementation of the Information Security Program through the review, maintenance, and, if necessary, updating of an existing information security program or existing safeguards, provided that such existing program or safeguards meet the requirements set forth in this Assurance.

d. Anthem shall review not less than annually the Information Security Program.

e. Anthem shall employ an executive or officer who shall be responsible for implementing, maintaining, and monitoring the Information Security Program ("Chief Information Security Officer" or "CISO"). The CISO shall have the background and expertise in information security appropriate to the level, size, and complexity of her/his role in implementing, maintaining, and monitoring the Information Security Program.

f. The role of the CISO will include regular and direct reporting to the Chief Executive Officer ("CEO"), Executive Staff, and Board of Directors concerning Anthem's security posture, the security risks faced by Anthem, and the security implications of Anthem's business decisions. The CISO shall meet with and provide a report to: (1) the Board of Directors on at least a semi-annual basis and (2) the CEO on at least a quarterly basis. The CISO shall report to the CEO within twenty-four (24) hours of a confirmed Security Event impacting 500 or more consumers residing in the United States. The CISO shall include such Security Events in its annual report to the Board of Directors.

g. Anthem shall provide notice of the requirements of this Assurance to the employees of Anthem's Information Security organization and shall implement training on the requirements of this Assurance to those employees. Anthem shall provide the training required under this paragraph to such employees within ninety (90) days of the Effective Date of this Assurance or prior to their starting their responsibilities for implementing, maintaining, or monitoring the Information Security Program.

h. As part of its Information Security Program, Anthem shall develop, implement, and maintain a written incident response plan to prepare for and respond to Security Events. Anthem shall revise and update this response plan, as necessary, to adapt to any material changes that affect the security of PI and PHI. Such a plan shall, at a minimum, identify and

describe the following phases: (i) Preparation; (ii) Detection and Analysis; (iii) Containment; (iv) Notification and Coordination with Law Enforcement; (v) Eradication; (vi) Recovery; (vii) Consumer and Regulator Notification and Remediation; and (viii) Post-Incident Analysis.

i. Anthem shall budget such that its Information Security Program receives the resources and support reasonably necessary to function as intended.

j. Anthem shall take reasonable efforts, using a reasonable and documented risk-based approach, to evaluate whether vendors that routinely handle PI or PHI have safeguards in place to protect such information and that such vendors will notify Anthem promptly of any potential compromise to the confidentiality, integrity, or availability of PI or PHI held, stored, or processed by the vendors on behalf of Anthem.

**C. Specific Information Security Requirements**

5. **Data Collection & Retention**: Anthem shall develop, implement, and maintain reasonable policies and procedures governing its collection, use, and retention of PI and PHI. Anthem shall limit its use, disclosure of, and requests for PHI in accordance with the Minimum Necessary Standard, and to fulfill all applicable regulatory, legal, and contractual obligations.

6. **Segmentation**: Anthem shall develop, implement, and maintain reasonable policies and procedures designed to reasonably segment the Anthem Network. At a minimum, within ninety (90) days, Anthem shall develop a timetable to implement:

a. segmentation of its VOIP servers; and

b. segmentation of its development and production environments.

On a semiannual basis, Anthem will report to the Board of Directors regarding the implementation timetable progress, as well as document any significant delays or revisions to the timetable.

7. **Cyber Security Operations Center ("C-SOC")**: Anthem shall maintain the existence and operation of its C-SOC or a reasonably equivalent technology. The C-SOC shall be staffed continuously to provide comprehensive monitoring of servers and other technologies to identify improper use of data, including PI and/or PHI. The C-SOC's analytic capabilities shall be deployed to detect, analyze, and respond to potential and confirmed Security Events.

8. **Logging & Monitoring**: Anthem shall develop, implement, and maintain reasonable policies and procedures designed to properly log and monitor the Anthem Network. At a minimum:

a. Anthem shall employ tools, such as a Security Information and Event Monitoring solution ("SIEM") (or a reasonably equivalent technology), among others, to log and monitor network traffic to detect and respond to Security Events.

b. Anthem shall take reasonable steps to properly configure, and regularly update or maintain the SIEM (or a reasonably equivalent technology) used pursuant to subsection (a) and shall take reasonable steps to adequately log system activity and identify potential Security Events for review. Using the SIEM (or a reasonably equivalent technology), Anthem shall actively review and analyze in real-time the logs of system activity and take appropriate follow-up with respect to Security Events.

c. Anthem shall maintain logs in conformance with industry standards and all applicable laws.

d. In addition to the requirements set forth in subparagraphs (a) through (c) of this Paragraph, Anthem shall develop, implement, and maintain defined and specific policies and procedures with respect to logging and monitoring of the internal data warehouse involved in the Data Breach and any database (or set of databases) that collects, processes, transmits, and/or stores

PI and/or PHI of similar volume as the internal data warehouse involved in the Data Breach. At a minimum:

i. Anthem shall deploy an appropriate database activity monitoring tool or a reasonably equivalent technology in the internal data warehouse involved in the Data Breach and any similar database (or set of databases) that Anthem uses to collect, process, transmit, and/or store PI and/or PHI of similar volume as the internal data warehouse involved in the Data Breach, to the extent it is commercially feasible.

ii. The monitoring of such database(s) shall include commercially reasonable query categories available in a database activity monitoring tool or reasonable equivalent issued to the relevant database(s).

iii. The monitoring of such database(s) shall be performed by appropriately trained or experienced personnel.

e. Anthem shall create a formalized procedure to track Security Events and alerts on privileged user queries on a regular basis and document identified issues and necessary action items.

9. **Antivirus Maintenance**: Anthem shall implement and maintain current, up-to-date antivirus protection programs or a reasonably equivalent technology on the Anthem Network components that require antivirus software, which shall be at the highest technical level available within Anthem-approved antivirus products that can be supported on such components, subject to any reasonable and documented security exceptions.

10. **Access Controls**: Anthem shall implement and maintain appropriate controls to manage access to and use of all accounts with access to PI or PHI, including individual accounts, administrator accounts, service accounts, and vendor accounts. Such controls shall include a means

to regularly review access and access levels of users and remove network and remote access within twenty-four (24) hours of notification of termination for any employee whose employment has ended or any non-associate whose term has ended.

11. **Authentication**: Anthem shall implement and maintain reasonable policies and procedures requiring the use of authentication in accordance with industry standards, where commercially feasible, including as appropriate under industry standards, the use of strong passwords, password rotation, and ensuring that stored passwords are protected from unauthorized access.

12. **Privileged Account Management**: Anthem shall implement and maintain reasonable controls to secure use of privileged credentials, such as through a Privileged Access Management tool or reasonably equivalent technology that vaults and rotates elevated credentials in places where privileged access credentials are required. Administrators shall be required to use Multi-factor Authentication or reasonably equivalent technology to gain access to their safe within the vault to retrieve their credentials.

13. **Remote Access/ Multi-factor Authentication**: Anthem shall require the use of Multi-factor Authentication or reasonably equivalent technology for end-user remote access to the Anthem Network that are servers. Additionally, Anthem will require during vendor security assessments business record documentation that demonstrates the vendor deploys Multi-factor Authentication or reasonably equivalent technology for end-user remote access to the Anthem Network via any business-to-business connection.

14. **Encryption**: Anthem shall develop, implement, maintain, regularly review, and revise policies and procedures to Encrypt PI and PHI at rest and in transit as reasonable and appropriate, and in accordance with applicable law.

15. **Asset Inventory**: Anthem shall develop, maintain, and regularly update a reasonable inventory of the assets that primarily comprise the Anthem Network and assign criticality ratings to such assets, as feasible.

16. **Risk Assessments**: Anthem shall develop, implement, and maintain a risk assessment program to identify, address, and, as appropriate, remediate risks affecting its Covered Systems. At a minimum, Anthem shall have an annual risk assessment performed by an independent third party. The assessment shall include assessment of all reasonably anticipated, internal and external risks to the security, confidentiality, or availability of PI and PHI collected, processed, transmitted, stored, or disposed of by Anthem, excluding legal documents and analyses that Anthem reasonably asserts are exempt from disclosure under legally-recognized privilege. Such reports shall be maintained by the CISO and be made available for inspection by the Third-Party Assessor described in Paragraph 27 of this Assurance.

17. **Vulnerability Management**: Anthem shall commit to continuing its current practices related to vulnerability scanning or a reasonably equivalent technology and remediation.

18. **Penetration Testing**: Anthem shall develop, implement, and maintain a penetration testing program designed to identify, assess, and remediate security vulnerabilities within the Anthem Network, which shall include annual external penetration tests or a reasonably equivalent technology and appropriate remediation of vulnerabilities revealed by such testing. Anthem shall develop, implement, and maintain an internal penetration testing program through the use of its Adversary Simulation Team or a reasonably equivalent group, who shall perform biannual internal penetration tests. The reports of such external and internal penetration tests shall be maintained by the CISO for a period of not less than six (6) years and be made available for inspection by the Third-Party Assessor described in Paragraph 27 of this Assurance.

19. **Email Filtering and Phishing Solutions**: Anthem shall maintain email protection and filtering solutions for all Anthem email accounts, including email SPAM, phishing attacks, and anti-malware or a reasonably equivalent technology.

20. **Employee Training**: In addition to the requirements set forth in Paragraph 4(g) above, Anthem shall conduct an initial training for all new employees and, on at least an annual basis, train existing employees concerning its information privacy and security policies, the proper handling and protection of PI and PHI, and disciplinary measures for violation, up to and including termination. At a minimum:

a. Anthem's new employee and annual training shall cover social engineering schemes, such as phishing;

b. Anthem shall conduct annual mock phishing exercises and all employees who fail must successfully complete additional training; and

c. Anthem shall document such trainings and the results of the mock phishing exercises.

21. **Network Sensors**: Anthem shall deploy network sensors or a reasonably equivalent technology to detect attempts to communicate from the Anthem Network to known malicious IP addresses.

22. **Endpoint Detection and Response**: Anthem will implement, maintain, and monitor controls designed to provide real-time notification of malicious systems modifications and anomalous systems activity in the Covered Systems.

23. **Intrusion Detection and Prevention Solution(s)**: Anthem shall develop, implement, and maintain an intrusion detection and prevention solution to assist in detecting and preventing unauthorized access to the Anthem Network.

24. **Data Loss Prevention**: Anthem shall develop, implement, and maintain a data loss prevention technology or a reasonably equivalent technology to detect and prevent unauthorized data exfiltration from the Anthem Network.

25. **Whitelisting**: Anthem shall implement and maintain controls designed to identify applications permitted to be on the Covered Systems while blocking and/or preventing the execution of unauthorized applications (i.e., applications not on the whitelist) on critical servers.

**D. Information Security Program Assessment**

26. Anthem shall obtain an initial and annual information security assessment of its policies and practices pertaining to the collection, storage, maintenance, transmission, and disposal of PI and PHI, from an independent third-party professional ("Third-Party Assessor") within one year of the Effective Date of this Assurance and then once a year thereafter for a total period of three (3) years.

27. The Third-Party Assessor must be an organization that employs at least one individual to perform the assessment that is: (a) qualified as a Certified Information System Security Professional ("CISSP") or as a Certified Information Systems Auditor ("CISA"), or a similar qualification; and (b) has at least five (5) years of experience evaluating the effectiveness of computer systems or information system security.

28. Anthem may satisfy the initial assessment by providing a copy of the Assessment Report performed for calendar year 2019 pursuant to the settlement of *In re Anthem Inc. Data Breach Litig.*, MDL 2617. For the remaining two assessments, the Third-Party Assessor shall review this Assurance and the Security Event Report, risk assessments, and penetration test reports provided by Anthem as set forth in Paragraphs 3, 16, and 18, respectively. The Third-Party Assessor shall prepare a formal report ("Security Report") that shall confirm Anthem's

development, implementation, and maintenance of a written Information Security Program with security controls and processes that meet the requirements of this Assurance related to: segmentation, antivirus maintenance, access controls including privileged access management and multi-factor authentication, vulnerability scanning and remediation, logging and monitoring, encryption, application whitelisting, e-mail filtering, and information system activity review and detection. The Security Report shall also confirm that Anthem has complied with the provisions of this Assurance related to the employment of a CISO or equivalent officer, maintenance of a C-SOC facility, and performance of internal and external penetration tests and information security training. In preparing each Security Report, the Third-Party Assessor may rely on the Assessment Report performed for calendar years 2020 and 2021 for *In re Anthem Inc. Data Breach Litig.*, MDL 2617, for security controls and processes addressed by both that Assessment Report and this Assurance.

29. The Security Report shall be provided to the Connecticut Attorney General no later than ten (10) days after its completion. Anthem will also provide the Risk Assessment, as set forth in Paragraph 16, and a SOC 2 Type 2 Assessment, as referenced in Paragraph 31 to the Connecticut Attorney General on an annual basis during the three-year term.

a. Confidentiality: The Connecticut Attorney General's Office shall, to the extent permitted by state law, treat each Security Report as exempt from disclosure as applicable under the relevant public records laws.

b. State Access: The Connecticut Attorney General's Office may provide a copy of each Security Report to any other of the Attorneys General upon request, and each requesting Attorney General shall, to the extent permitted by state law, treat such report as exempt from disclosure as applicable under the relevant public records laws.

30. Upon receipt of each Security Report, Anthem will review and evaluate whether to revise its current policies and procedures based on the findings of the Security Report. Within sixty (60) days of Anthem's receipt of each Security Report, Anthem shall forward to the Connecticut Attorney General a description of any action they plan to take, or if no action is taken, a detailed description why no action is necessary, in response to each Security Report.

**E. Information Security Program Audit**

31. Anthem shall provide to the Connecticut Attorney General an annual SOC 2 Type 2 Assessment for calendar year 2019 and then once a year thereafter for a total period of three (3) years. At a minimum, this Assessment shall include the trust service principles of Security and Confidentiality.

## IV. PAYMENT TO THE STATES

32. Anthem shall pay a total amount of Thirty-Nine Million and Five Hundred Thousand Dollars ($39,500,000.00). Said payment shall be divided and paid by Anthem directly to each of the Attorneys General in an amount to be designated by the Attorneys General and communicated to Anthem by the Connecticut Attorney General, along with instructions for such payments.[4] Payment shall be made in full within thirty (30) business days of the Effective Date and receipt of payment instructions by Anthem from the Connecticut Attorney General, except that where state law requires judicial or other approval of the Assurance, payment shall be made no later than thirty (30) days after notice from the relevant Attorney General that such final approval for the Assurance has been secured.

33. Of the total amount, Anthem shall pay $1,929,942.02 to the Kentucky Attorney General. The amount payable to the Commonwealth of Kentucky pursuant to the Assurance of

[4] Payment to the State of California pursuant to its settlement with Anthem will be a portion of the total amount paid as set forth in this Paragraph.

Voluntary Compliance is $1,929,942.02 which includes $1,017,451.83 for the recovery of the Attorney General's reasonable costs of investigation and litigation.

34. Also out of the total amount, as set forth above, Anthem will make payment to the NAGTRI Endowment Fund maintained in trust by the National Association of Attorneys General within thirty (30) days of the Effective Date, in an amount designated and communicated to Anthem by the Connecticut Attorney General.

## V. RELEASE AND EXPIRATION

35. Release: Following full payment of the amounts due by Anthem under this Assurance, the Attorneys General shall release and discharge Anthem from all civil claims that the Attorneys General could have brought under the Consumer Protection Acts, Personal Information Protection Acts, Security Breach Notification Acts, HIPAA, and any common law claims concerning unfair, deceptive, or fraudulent trade practices based on Anthem's conduct related to the Data Breach. Nothing contained in this paragraph shall be construed to limit the ability of the Attorneys General to enforce the obligations that Anthem, its officers, subsidiaries, affiliates, agents, representatives, employees, successors, and assigns, have under this Assurance. Further, nothing in the Assurance shall be construed to create, waive, or limit any private right of action.

36. Notwithstanding any term of this Assurance, any and all of the following forms of liability are specifically reserved and excluded from the release in Paragraph 35 as to any entity or person, including Anthem:

a. Any criminal liability that any person or entity, including Anthem, has or may have to the States.

b. Any civil or administrative liability that any person or entity, including Anthem, has or may have to the States under any statute, regulation, or rule giving rise to any and all of the following claims:

i. State or federal antitrust violations;

ii. State or federal securities violations; or

iii. State or federal tax claims.

37. Expiration: The obligations and other provisions of this Assurance set forth in Paragraphs 4(b), 6-13, 15, 17-19, and 21-25 shall expire at the conclusion of the five (5) year period after the Effective Date of this Assurance. The obligations and other provisions of this Assurance set forth in Paragraphs 14, 16, 20(a)-(c), 47, and 48 shall expire at the conclusion of the seven (7) year period after the Effective Date of the Assurance, unless they have expired at an earlier date pursuant to their specific terms. Provided, however, that nothing in this Paragraph shall be construed as excusing or exempting Anthem from complying with any state or federal law, rule, or regulation, nor shall any of the provisions of this Assurance be deemed to authorize or require Anthem to engage in any acts or practices prohibited by any law, rule, or regulation.

## VI. GENERAL PROVISIONS

38. Meet and Confer: If any Attorney General determines that Anthem has failed to comply with any of the terms of this Assurance, and if in the Attorney General's sole discretion the failure to comply does not threaten the health or safety of the Attorney General's State and/or does not create an emergency requiring immediate action, the Attorney General will notify Anthem in writing of such failure to comply and Anthem shall have thirty (30) days from receipt of such written notice to provide a good faith response to the Attorney General's determination. The response shall include: (A) a statement explaining why Anthem believes it is in full compliance

with this Assurance; or (B) a detailed explanation of how the alleged violation(s) occurred, and either (i) a statement regarding whether the alleged violation(s) has been addressed and how, or (ii) a statement regarding whether the alleged violation cannot be reasonably addressed within thirty (30) days receipt of the notice, but, if (B)(ii) then also a statement (a) indicating whether Anthem has begun to take corrective action(s) to address the alleged violation(s), (b) stating what corrective action(s) Anthem is pursuing, and (c) providing the Attorneys General with a reasonable timetable for addressing the alleged violation(s). Nothing herein shall prevent an Attorney General from agreeing in writing to provide Anthem with additional time beyond the thirty (30) day period to respond to the notice referenced in this Paragraph. Nothing herein shall be construed to exonerate any failure to comply with any provision of this Assurance after the Effective Date or compromise the authority of the Attorney General to initiate a proceeding for any failure to comply with this Assurance.

39. Any failure by the Attorneys General to insist upon Anthem's compliance with any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the Attorneys General, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Assurance to be performed by Anthem.

40. If any clause, provision, or section of this Assurance shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity, or unenforceability shall not affect any other clause, provision, or section of this Assurance and this Assurance shall be construed and enforced as if such illegal, invalid, or unenforceable clause, section, or provision had not been contained herein.

41. Nothing contained in this Assurance shall be construed to waive or limit any right of action by any consumer, person or entity, or by any local, state, federal or other governmental entity, except as provided by the Release herein.

42. Nothing in this Assurance shall prevent or restrict the use of this Assurance by the State in any action against Anthem for failure to comply with any of its provisions, or in the event that Anthem is in default of any of its terms and conditions. A default on the part of Anthem shall include any material breach of any of the terms or requirements of this Assurance. Nothing in this Assurance shall be construed to (i) exonerate any failure to comply with any of its provisions after the Effective Date of this Assurance, (ii) compromise or limit the authority of the State to initiate a proceeding for any failure to comply, or (iii) compromise the authority of the Court or any other court of competent jurisdiction to impose any applicable remedies for any violation of this Assurance.

43. Nothing in this Assurance is intended to be and shall not be construed or deemed to be an admission or concession or evidence of any liability or wrongdoing whatsoever on the part of Anthem or of any fact or violation of any law, rule, or regulation. This Assurance is made without trial or adjudication of any alleged issue of fact or law and without any finding of liability of any kind.

44. Anthem hereby acknowledges that its undersigned representative or representatives are authorized to enter into and execute this Assurance. Anthem has been represented by legal counsel and has been advised by their legal counsel of the meaning and legal effect of this Assurance.

45. This Assurance shall bind Anthem and its subsidiaries, affiliates, successors, future purchasers, acquiring parties, and assigns.

46. Within thirty (30) days of the Effective Date, Anthem will deliver a copy of this Assurance to (a) its Chief Executive Officer, Chief Information Officer, Chief Information Security Officer, and its General Counsel, and (b) its Board of Directors. In the event that any person assumes the role of Chief Executive Officer, Chief Information Officer, Chief Information Security Officer, and its General Counsel, or becomes a member of the Board of Directors and such person has not been previously delivered a copy of this Assurance, Anthem shall deliver a copy of this Assurance to such person within thirty (30) days from which such person assumes such role or becomes a member of the Board of Directors and maintain a record of such.

47. With respect to existing subsidiaries and affiliates, which do not yet fall under the definition of Anthem as set forth in Paragraph 1(A), but which are wholly owned and Anthem intends to integrate and operate, Anthem shall within one hundred and eighty (180) days following the Effective Date of this Assurance develop a reasonable and appropriate implementation timetable for those subsidiaries and affiliates to achieve compliance with the provisions of this Assurance. For purposes of this provision, implementation shall mean (i) that Anthem or its subsidiaries and affiliates have taken the relevant measure(s) where technologically feasible and otherwise reasonable, or have taken alternative measure(s) that alone or in the aggregate provide for substantially equivalent security, or (ii) that Anthem or its wholly owned, integrated, and operated subsidiaries and affiliates have developed a reasonable and appropriate plan to evaluate the technological and operational feasibility of the provisions of this Assurance. On a semiannual basis, Anthem will report to the Board of Directors regarding the implementation timetable progress, as well as document any significant delays or revisions to the timetable.

48. In the event that (1) Anthem acquires or merges with a subsidiary or affiliate after the Effective Date, (2) the subsidiary is wholly owned by Anthem, and (3) Anthem determines that

it intends to wholly integrate and operate that subsidiary following the completion of an integration assessment, Anthem shall have one-hundred twenty (120) days from the date Anthem completes the integration assessment to develop and then implement an integration timetable regarding compliance with the terms of this Assurance. For purposes of this provision, implementation shall mean (i) that Anthem or its wholly owned, integrated, and operated subsidiaries and affiliates have taken the relevant measure(s) where technologically feasible and otherwise reasonable, or have taken alternative measure(s) that alone or in the aggregate provide for substantially equivalent security, or (ii) that Anthem or its wholly owned, integrated, and operated subsidiaries and affiliates have developed a reasonable and appropriate plan to evaluate the technological and operational feasibility of the provisions of this Assurance. On a semiannual basis, Anthem will report to the Board of Directors regarding the implementation timetable progress, as well as document any significant delays or revisions to the timetable.

49. The settlement negotiations resulting in this Assurance have been undertaken by the Parties in good faith and for settlement purposes only, and no evidence of negotiations or communications underlying this Assurance shall be offered or received in evidence in any action or proceeding for any purpose.

50. In states where statute requires that this Assurance be filed with and/or approved by a court, Anthem consents to the filing of this Assurance and its approval by the court, and authorizes the Attorneys General in such states to represent that Anthem does not object to court approval of the Assurance. Anthem further consents to the jurisdiction of each such court for the purpose of approving or enforcing this Assurance. To the extent there are any court costs associated with the filing of this Assurance (if legally required), Anthem agrees to pay such costs.

51. This Assurance does not constitute an approval by the Attorneys General of any of Anthem's past or future practices, and Anthem shall not make any representation to the contrary.

52. Anthem shall not participate directly in any activity to form or proceed as a separate entity or corporation for the purpose of engaging in acts prohibited in this Assurance. Anthem shall not knowingly cause, permit, or encourage any other persons or entities acting on its behalf, to engage in practices prohibited by this Assurance.

## VII. NOTICES UNDER ASSURANCE

53. Any notices or other documents required to be sent to the Parties pursuant to the Assurance shall be sent to the following address via first class and electronic mail, unless a different address is specified in writing by the party changing such address:

For the Attorney General:

Approved 9-30-20
Phillip Shepherd

Chris Lewis
Executive Director
Office of Consumer Protection
Kentucky Office of the Attorney General
1024 Capital Center Drive, Suite 200
Frankfort, KY 40601
(502) 696-5300
Christian.Lewis@ky.gov

For Anthem:

Office of the General Counsel
Anthem, Inc.
220 Virginia Avenue
Indianapolis, IN 46204
Tel.: (800) 331-1476

with a copy to:

Craig Hoover
Michelle Kisloff
Allison Holt Ryan
Hogan Lovells US LLP
555 Thirteenth Street, NW
Washington, DC 20004
Tel.: (202) 637-5600
craig.hoover@hoganlovells.com
michelle.kisloff@hoganlovells.com
allison.holt-ryan@hoganlovells.com

APPROVED:

ATTORNEY GENERAL, THE COMMONWEALTH OF KENTUCKY

By: _____ Date: 9/29/2020

Chris Lewis
Executive Director
Office of Consumer Protection
Kentucky Office of the Attorney General
1024 Capital Center Drive, Suite 200
Frankfort, KY 40601
(502) 696-5300
Christian.Lewis@ky.gov

[Additional approvals on subsequent pages]

APPROVED:

DEFENDANT
ANTHEM, INC.

By: _____ Date: 9/25/2020

Pamela C. Williams
Senior Vice President & Counsel
Anthem, Inc.
220 Virginia Avenue
Indianapolis, IN 46204

COUNSEL FOR DEFENDANT, ANTHEM, INC.

By: _____ Date: 9/25/2020

Michelle A. Kisloff
Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, D.C. 20004

# Appendix A

| STATE | CONSUMER PROTECTION ACTS |
|---|---|
| Alaska | Unfair Trade Practices Act, AS 45.50.471 *et seq.* |
| Arizona | Arizona Consumer Fraud Act, A.R.S. §§ 44-1521 *et seq.* |
| Arkansas | Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-101 *et seq.* |
| Colorado | Colorado Consumer Protection Act, C.R.S. §§ 6-1-101 *et seq.* |
| Connecticut | Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. §§ 42-110b *et seq.* |
| Delaware | Consumer Fraud Act, 6 Del. C. §§ 2511 *et seq.* |
| District of Columbia | Consumer Protection Procedures Act, D.C. Code §§ 28-3901 *et seq.* |
| Florida | Florida Deceptive and Unfair Trade Practices Act, Chapter 501, Part II, Florida Statutes |
| Georgia | Georgia Fair Business Practices Act, O.C.G.A. §§ 10-1-390 through 408 |
| Hawaii | Uniform Deceptive Trade Practice Act, Haw. Rev. Stat. Chpt. 481A and Haw. Rev. Stat. Sect. 480-2 |
| Idaho | Idaho Consumer Protection Act, Idaho Code §§ 48-601 *et seq.* |
| Illinois | Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.* |
| Indiana | Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5-1 *et seq.* |
| Iowa | Iowa Consumer Fraud Act, Iowa Code § 714.16 |
| Kansas | Kansas Consumer Protection Act, K.S.A §§ 50-623 *et seq.* |
| Kentucky | Kentucky Consumer Protection Act, KRS §§ 367.110-.300, 367.990 |
| Louisiana | Unfair Trade Practices and Consumer Protection Law, La. R.S. §§ 51:1401 *et seq.* |
| Maine | Maine Unfair Trade Practices Act, 5 M.R.S.A. §§ 205-A *et seq.* |
| Maryland | Maryland Consumer Protection Act, Md. Code Ann., Com. Law §§ 13-101 *et seq.* (2013 Repl. Vol and 2019 Supp.) |

## Appendix A

| | |
|---|---|
| Massachusetts | Mass. Gen. Laws ch. 93A |
| Michigan | Michigan Consumer Protection Act, MCL §§ 445.901 *et seq.* |
| Minnesota | The Uniform Deceptive Trade Practices Act, Minn. Stat. §§ 325D.43–.48; Consumer Fraud Act, Minn Stat. §§ 325F.68-.694 |
| Mississippi | Miss. Code Ann. § 75-24-1 *et seq.* |
| Missouri | Missouri Merchandising Practices Act, Mo. Rev. Stat. §§ 407.010 *et seq.* |
| Nebraska | Nebraska Consumer Protection Act, Neb. Rev. Stat. §§ 59-1601 *et seq.*; Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-301 *et seq.* |
| Nevada | Nevada Deceptive Trade Practices Act; Nev. Rev. Stat. §§ 598.0903 *et seq.* |
| New Hampshire | NH RSA 358-A |
| New Jersey | New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 *et seq.* |
| New York | Executive Law 63(12), General Business Law 349/350 |
| North Carolina | North Carolina Unfair and Deceptive Trade Practices Act, N.C.G.S. §§ 75-1.1 *et seq.* |
| North Dakota | Unlawful Sales or Advertising Practices, N.D.C.C. §§ 51-15-01 *et seq.* |
| Ohio | Ohio Consumer Sales Practices Act, R.C. §§ 1345.01 *et seq.* |
| Oklahoma | Oklahoma Consumer Protection Act, 15 O.S. §§ 751 *et seq.* |
| Oregon | Oregon Unlawful Trade Practices Act, ORS 646.605 *et seq.* |
| Pennsylvania | Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1 *et seq.* |
| Rhode Island | Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws §§ 6-13.1-1 *et seq.* |
| South Carolina | South Carolina Unfair Trade Practices Act, S.C. Code Ann. §§ 39-5-10 *et seq.* |
| Tennessee | Tennessee Consumer Protection Act of 1977, Tenn. Code Ann. §§ 47-18-101 to -131 |
| Texas | Texas Deceptive Trade Practices – Consumer Protection Act, Tex. Bus. & Com. Code Ann.§§ 17.41 – 17.63 |
| Virginia | Virginia Consumer Protection Act, Virginia Code §§ 59.1-196 through 59.1-207 |

# Appendix A

| | |
|---|---|
| Washington | Washington Consumer Protection Act, RCW 19.86.020 |
| West Virginia | West Virginia Consumer Credit and Protection Act ("WVCCPA"), W. Va. Code §§ 46A-1-101 *et seq.* [W.Va. Code §§ 46A-6-104, 46A-6-102(7)(6), 46A-6-102(7)(M)] |
| Wisconsin | Fraudulent Representations. Wis. Stat. § 100.18(1) |

## Appendix B

| STATE | PERSONAL INFORMATION PROTECTION ACTS & SECURITY BREACH NOTIFICATION ACTS |
|---|---|
| Alaska | Personal Information Protection Act, AS §§ 45.48.010 *et seq.* |
| Arizona | Ariz. Rev. Stat. § 18-552 |
| Arkansas | Personal Information Protection Act, Ark. Code Ann. §§ 4-110-101 *et seq.* |
| Colorado | Security Breach Notification, C.R.S. § 6-1-716 |
| Connecticut | Safeguarding of Personal Information, Conn. Gen. Stat. § 42-471; Breach of Security, Conn. Gen. Stat. § 36a-701b |
| Delaware | Delaware Data Breach Notification Law, 6 Del. C. § 12B-100 *et seq.* |
| District of Columbia | District of Columbia Consumer Security Breach Notification Act, D.C. Code §§ 28-3851 *et seq.* |
| Florida | Florida Information Protection Act, Section 501.171, Florida Statutes |
| Georgia | Georgia Personal Identity Protection Act, O.C.G.A §§ 10-1-910 through 915 |
| Hawaii | Security Breach of Personal Information, Haw. Rev. Stat. Chpt. 487N |
| Idaho | Identity Theft, Idaho Code §§ 28-51-104 *et seq.* |
| Illinois | Illinois Personal Information Protection Act, 815 ILCS 530/1 *et seq.* |
| Indiana | Disclosure of Security Breach Act, Indiana Code §§ 24-4.9-1-1 *et seq.* |
| Iowa | Personal Information Security Breach Protection Act, Iowa Code § 715C |
| Kansas | The Wayne Owen Act, K.S.A. § 50-6,139b; Security Breach Notification Act, K.S.A. §§ 50-7a01 *et seq.* |
| Kentucky | KRS 365.732 |
| Louisiana | Database Security Breach Notification Law, La. R.S. §§ 51:3071 *et seq.* |
| Maine | Maine Notice of Risk to Personal Data Act, 10 M.R.S.A. §§ 1346 *et seq.* |
| Maryland | Maryland Personal Information Protection Act, Md. Code Ann., Com. Law § 14-3501 *et seq.* (2013 Repl. Vol and 2019 Supp.) |

## Appendix B

| | |
|---|---|
| Massachusetts | Mass. Gen. Laws ch. 93H; 201 Code Mass. Regs. 17.00 *et seq.* |
| Michigan | Identity Theft Protection Act, MCL §§ 445.61 *et seq.* (Breach notification only; no applicable State personal information protection Act) |
| Minnesota | Minnesota Data Breach Notification Statute, Minn. Stat. § 325E.61 |
| Mississippi | Miss. Code Ann. § 75-24-29 |
| Missouri | Mo. Rev. Stat. § 407.1500 |
| Nebraska | Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, Neb. Rev. Stat. § 87-801 *et seq.* |
| Nevada | Nevada Security and Privacy of Personal Information Act; Nev. Rev. Stat. §§ 603A.010 – 603A.290 |
| New Hampshire | NH RSA 359-C:20 |
| New Jersey | New Jersey Identity Theft Prevention Act, N.J.S.A. 56:8-161 to -166 |
| New York | General Business Law 899-aa and 899-bb |
| North Carolina | North Carolina Identity Theft Protection Act, N.C.G.S. §§ 75-60 *et seq.* |
| North Dakota | Notice of Security Breach for Personal Information N.D.C.C. §§ 51-30-01 *et seq.* |
| Ohio | Security Breach Notification Act, R.C. §§ 1349.19 *et seq.* |
| Oklahoma | Security Breach Notification Act, 24 O.S. §§ 161 *et seq.* |
| Oregon | Oregon Consumer Information Protection Act, ORS 646A.600 *et seq.* |
| Pennsylvania | Breach of Personal Information Notification Act, 73 P.S. §§ 2301 *et seq.* |
| Rhode Island | Rhode Island Identity Theft Protection Act, R.I. Gen. Laws §§ 11-49.3-1 *et seq.* |
| South Carolina | Data Breach Notification, S.C. Code Ann. § 39-1-90 |
| Tennessee | Tennessee Identity Theft Deterrence Act of 1999, Tenn. Code. Ann. §§ 47-18-2101 to -2111 |
| Texas | Identity Theft Enforcement and Protection Act, Tex. Bus. & Com. Code Ann. § 521.001 – 152 |
| Virginia | Virginia Breach of Personal Information Notification Law, § 18.2-186.6 |
| Washington | Washington Data Breach Notification Law, RCW 19.255.010 |

## Appendix B

| | |
|---|---|
| West Virginia | West Virginia Consumer Credit and Protection Act ("WVCCPA"), W. Va. Code §§ 46A-1-101 *et seq.* |
| Wisconsin | Notice of Unauthorized Acquisition of Personal Information. Wis. Stat. § 134.98<br>Confidentiality of Patient Health Care Records. Wis. Stat. § 146.82<br>Violations Related to Patient Health Care Records. Wis. Stat. §146.84(2) |