

RESOLUTION AGREEMENT

I. Recitals

1. Parties. The Parties to this Resolution Agreement (“Agreement”) are:

- A. The United States Department of Health and Human Services, Office for Civil Rights (“HHS”), which enforces the Federal standards that govern the privacy of individually identifiable health information (45 C.F.R. Part 160 and Subparts A and E of 45 C.F.R. Part 164, the “Privacy Rule”), the Federal standards that govern the security of electronic individually identifiable health information (45 C.F.R. Part 160 and Subparts A and C of 45 C.F.R. Part 164, the “Security Rule”), and the Federal standards for notification in the case of breach of unsecured protected health information (45 C.F.R. Part 160 and Subparts A and D of 45 C.F.R. Part 164, the “Breach Notification Rule”). HHS has the authority to conduct compliance reviews and investigations of complaints alleging violations of the Privacy, Security, and Breach Notification Rules (the “HIPAA Rules”) by covered entities and business associates, and covered entities and business associates must cooperate with HHS compliance reviews and investigations. *See* 45 C.F.R. §§ 160.306(c), 160.308, and 160.310(b).
- B. Anthem, Inc. (“Anthem”), which is a business associate, as defined at 45 C.F.R. § 160.103, and therefore is required to comply with the HIPAA Rules. Anthem is a publicly traded corporation. It provides administrative services as a business associate to the Anthem Affiliated Covered Entities (Anthem ACE) and is one of the nation’s leading health benefits companies, with health plans in more than a dozen states and customers in other states through its subsidiaries.
- C. HHS and Anthem shall together be referred to herein as the “Parties.”

2. No Admission. This Agreement is not an admission, concession, or evidence of liability by Anthem.

3. No Concession. This Agreement is not a concession by HHS that Anthem is not in violation of the HIPAA Rules and that Anthem is not liable for civil money penalties (“CMPs”).

4. Intention of Parties to Effect Resolution. This Agreement is intended to resolve HHS Transaction Number: 01-15-204066 and any potential violations of the HIPAA Rules related to the Covered Conduct specified in section I.5 of this Agreement. In consideration of the Parties’ interest in avoiding the uncertainty, burden, and expense of further investigation and formal proceedings, the Parties agree to resolve this matter according to the Terms and Conditions below.

5. Factual Background and Covered Conduct.

On February 13, 2015, HHS opened a compliance review of Anthem based on February 5, 2015 media reports and information on Anthem's website that Anthem had experienced a "sophisticated external cyber attack." On March 13, 2015, HHS received notification from Anthem that cyber-attackers gained impermissible access to the electronic protected health information (ePHI) of 78,800,000 individuals maintained on Anthem's enterprise data warehouse. On February 23, 2015, HHS notified Anthem of its investigation regarding Anthem's compliance with the HIPAA Rules. HHS' investigation indicated potential violations of the following provisions ("Covered Conduct"):

- A. The requirement to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI held by Anthem (*see 45 C.F.R. § 164.308 (a)(1)(ii)(A)*).
- B. The requirement to implement sufficient procedures to regularly review records of information system activity (*see 45 C.F.R. § 164.308 (a)(1)(ii)(D)*).
- C. The requirement to identify and respond to detections of the security incident leading to this breach (*see 45 C.F.R. § 164.308 (a)(6)(ii)*).
- D. The requirement to implement sufficient technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4) (*see 45 C.F.R. § 164.312(a)*).
- E. The requirement to prevent unauthorized access to the ePHI of 78,800,000 individuals whose information was maintained in Anthem's enterprise data warehouse (*see 45 C.F.R. § 164.502(a)*).

II. Terms and Conditions

6. Payment. HHS has agreed to accept, and Anthem has agreed to pay HHS, the amount of \$16,000,000 ("Resolution Amount"). Anthem agrees to pay the Resolution Amount on October 15, 2018 by automated clearing house transaction pursuant to written instructions to be provided by HHS.

7. Corrective Action Plan. Anthem has entered into and agrees to comply with the Corrective Action Plan ("CAP"), attached as Appendix A, which is incorporated into this Agreement by reference. If Anthem breaches the CAP, and fails to cure the breach as set forth in the

CAP, then Anthem will be in breach of this Agreement and HHS will not be subject to the Release set forth in section II.8 of this Agreement.

8. Release by HHS. In consideration of and conditioned upon Anthem's performance of its obligations under this Agreement, HHS releases Anthem from any actions it may have against Anthem under the HIPAA Rules arising out of or related to the Factual Background and Covered Conduct identified in section I.5 of this Agreement. HHS does not release Anthem from, nor waive any rights, obligations, or causes of action other than those arising out of or related to the Covered Conduct and referred to in this paragraph. This release does not extend to actions that may be brought under section 1177 of the Social Security Act, 42 U.S.C. § 1320d-6.

9. Agreement by Released Parties. Anthem shall not contest the validity of its obligation to pay, nor the amount of, the Resolution Amount or any other obligations agreed to under this Agreement. Anthem waives all procedural rights granted under Section 1128A of the Social Security Act (42 U.S.C. § 1320a-7a) and 45 C.F.R. Part 160 Subpart E, and HHS claims collection regulations at 45 C.F.R. Part 30, including, but not limited to, notice, hearing, and appeal with respect to the Resolution Amount.

10. Binding on Successors. This Agreement is binding on Anthem and its successors, heirs, transferees, and assigns.

11. Costs. Each Party to this Agreement shall bear its own legal and other costs incurred in connection with this matter, including the preparation and performance of this Agreement.

12. Effect of Agreement. This Agreement constitutes the complete agreement between the Parties. All material representations, understandings, and promises of the Parties are contained in this Agreement. Any modifications to this Agreement shall be set forth in writing and signed by all Parties.

13. Execution of Agreement and Effective Date. The Agreement shall become effective (*i.e.*, final and binding) upon the date of signing of this Agreement and the CAP by the last signatory ("Effective Date").

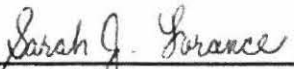
14. Tolling of Statute of Limitations. Pursuant to 42 U.S.C. § 1320a-7a(c)(1), a CMP must be imposed within six (6) years from the date of the occurrence of the violation. To ensure that this six-year period does not expire during the term of this Agreement, Anthem agrees that the time between the Effective Date of this Agreement (as set forth in Paragraph 13) and the date the Agreement may be terminated by reason of Anthem's breach, plus one-year thereafter, will not be included in calculating the six (6) year statute of limitations applicable to the violations which are the subject of this Agreement. Anthem waives and will not plead any statute of limitations, laches, or similar defenses to any administrative action relating to the Covered Conduct identified in section I.5 that is filed by HHS within the time period set forth above, except to the extent that such defenses would have been available had an administrative action been filed on the Effective Date of this Agreement.

15. Disclosure. HHS places no restriction on the publication of the Agreement.

16. Execution in Counterparts. This Agreement may be executed in counterparts, each of which constitutes an original, and all of which shall constitute one and the same agreement.

17. Authorizations. The individual(s) signing this Agreement on behalf of Anthem represent and warrant that they are authorized by Anthem to execute this Agreement. The individual(s) signing this Agreement on behalf of HHS represent and warrant that they are signing this Agreement in their official capacities and that they are authorized to execute this Agreement.


For Anthem, Inc.



Sarah J. Lorange
Senior Vice President & Chief Compliance Officer
Anthem, Inc.

10/15/2018
Date

For Department of Health and Human Services



Susan M. Pezzullo Rhodes
Regional Manager, New England Region
Office for Civil Rights

10/15/18
Date

Appendix A
CORRECTIVE ACTION PLAN
BETWEEN THE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
AND
ANTHEM, INC.

I. Preamble

Anthem, Inc. (hereinafter known as "Anthem") hereby enters into this Corrective Action Plan ("CAP") with the United States Department of Health and Human Services, Office for Civil Rights ("HHS"). Contemporaneously with this CAP, Anthem is entering into a Resolution Agreement ("Agreement") with HHS, and this CAP is incorporated by reference into the Resolution Agreement as Appendix A. Anthem enters into this CAP as part of consideration for the release set forth in section II.8 of the Agreement.

II. Contact Persons and Submissions

A. Contact Persons

Anthem has identified the following individual as its authorized representative and contact person regarding the implementation of this CAP and for receipt and submission of notifications and reports:

Sarah J. Lorance
Senior Vice President & Chief Compliance Officer
700 Broadway
Denver, CO 80273
Telephone: (303) 764-7277
Sarah.j.lorance@anthem.com

HHS has identified the following individual as its authorized representative and contact person with whom Anthem is to report information regarding the implementation of this CAP:

Susan M. Pezzullo Rhodes
Office for Civil Rights, New England Region
U.S. Department of Health and Human Services
JFK Federal Building, Room 1875
Boston, MA 02203
Telephone: 617-565-1347
Fax: 617-565-3809

Anthem and HHS agree to promptly notify each other of any changes in the contact persons or the other information provided above.

B. Proof of Submissions. Unless otherwise specified, all notifications and reports required by this CAP may be made by any means, including certified mail, overnight mail, or hand delivery, provided that there is proof that such notification was received. For purposes of this requirement, internal facsimile confirmation sheets do not constitute proof of receipt.

III. Effective Date and Term of CAP

The Effective Date for this CAP shall be calculated in accordance with paragraph II.13 of the Agreement ("Effective Date"). The period for compliance ("Compliance Term") with the obligations assumed by Anthem under this CAP shall begin on the Effective Date of this CAP and end two (2) years from the Effective Date, unless before the end of this two (2) year period, HHS has notified Anthem under section VIII.B. hereof of its position that Anthem has breached this CAP. In the event of such a notification by HHS under section VIII.B. hereof, the Compliance Term shall not end until HHS either (1) notifies Anthem that it has determined that the breach has been cured or (2) notifies Anthem under section VIII.D. hereof that it will seek imposition of a CMP. After the Compliance Term ends, Anthem shall still be obligated to submit the final Annual Report as required by Section VI and comply with the document retention requirement in Section VII.

IV. Time

In computing any period of time prescribed or allowed by this CAP, all days referred to shall be calendar days. The day of the act, event, or default from which the designated period of time begins to run shall not be included. The last day of the period so computed shall be included, unless it is a Saturday, a Sunday, or a legal holiday, in which event the period runs until the end of the next day which is not one of the aforementioned days.

V. Corrective Action Obligations

Anthem agrees to the following:

A. Security Management Process

1. Anthem shall conduct an accurate and thorough Risk Analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by Anthem. Within ninety (90) days of the Effective Date, Anthem shall provide to HHS a Statement of Work (SOW) for the Risk Analysis. Within thirty (30) days of its receipt of Anthem's Risk Analysis SOW, if HHS identifies deficiencies in the Risk Analysis SOW, HHS shall provide Anthem with written technical assistance, as necessary, such as through suggested edits to the SOW, so that Anthem may revise its SOW accordingly. Within thirty (30) days of HHS providing such written technical assistance, if any, the Parties shall meet and confer in good faith to determine the deadline by which Anthem shall submit a

revised SOW for HHS review. Within thirty (30) days of Anthem submitting any such revised SOW, the Parties shall meet and confer in good faith to determine the deadline by which HHS shall review the revised SOW and provide Anthem with written technical assistance, if any. This submission and review process shall continue until HHS approves the SOW.

2. Anthem shall provide the Risk Analysis, consistent with section V.A.1, to HHS within two-hundred ten (210) days of HHS's approval of the Risk Analysis SOW, as required by section V.A.1, for HHS' review. Anthem may submit a Risk Analysis currently underway or previously completed for consideration by HHS for compliance with this provision. Within thirty (30) days of its receipt of Anthem's Risk Analysis, HHS will inform Anthem whether it has any technical assistance to provide for the submitted Risk Analysis. Upon receiving any recommended changes to the Risk Analysis to confirm compliance with the SOW and the Security Rule, Anthem shall have thirty (30) days to revise the Risk Analysis and provide the revised Risk Analysis to HHS for review. This process shall continue until HHS determines the Risk Analysis has been completed in accordance with the SOW and the Security Rule. Anthem will within one-hundred fifty (150) days then incorporate the results of the Risk Analysis into its existing process for implementing security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level as required by the Security Rule and will provide such documentation to HHS upon request.

B. Policies and Procedures

1. Anthem shall review and revise, as necessary, the written policies and procedures addressing the Minimum Content set forth in Section V.D. to confirm compliance with the Federal standards that govern the security of individually identifiable health information (45 C.F.R. Part 164, Subpart C) (the "Security Rule").

2. Anthem shall provide the policies and procedures identified in section V.B.1 above to HHS for review within one-hundred fifty (150) days of the Effective Date. Within sixty (60) days of its receipt of Anthem's submitted policies and procedures, HHS will inform Anthem whether it has any feedback on the submitted policies and procedures. Upon receiving any recommended changes to such policies and procedures from HHS to confirm compliance with the Security Rule, Anthem shall have forty-five (45) days to revise such policies and procedures and provide the revised policies and procedures to HHS for review. This process shall continue until HHS confirms that such policies and procedures comply with the requirements of the Security Rule.

3. Anthem shall adopt any necessary amendments to its policies and procedures pursuant to section V.B.2 within ninety (90) days of receipt of HHS' final feedback.

C. Distribution of Policies and Procedures

1. Anthem shall make available, for example through publication on its intranet, the policies and procedures identified in section V.B. to members of the Anthem's workforce subject to those policies and procedures who use or disclose ePHI within thirty (30) days of Anthem's adoption of such policies and procedures, and thereafter to new members of the workforce who

will be subject to those policies and procedures and who will use or disclose ePHI within thirty (30) days of their becoming a member of the workforce.

D. Minimum Content of the Policies and Procedures

The Policies and Procedures subject to this CAP shall include and be limited to policies and procedures that address the following Security Rule provisions:

1. Information System Activity Review – 45 C.F.R. § 164.308(a)(1)(ii)(D), including a process(es) for the regular review of records of information system activity collected by Anthem and processes for evaluating when the collection of new or different records needs to be included in the review;

2. Access Control – 45 C.F.R. § 164.312(a)(1), with respect to provisions to address access between Anthem systems containing ePHI, such as network or portal segmentation, and provisions to enforce password management requirements, such as password age.

E. Reportable Events

1. During the Compliance Term, in the event that Anthem receives information that a workforce member subject to the policies and procedures adopted by Anthem under section V.B.3 may have failed to comply with those policies and procedures, Anthem shall promptly investigate this matter. If Anthem determines, after such investigation, that during the Compliance Term a member of its Workforce subject to the policies and procedures adopted by Anthem under section V.B.3 failed to comply with those policies and procedures, and such failure was material (e.g., a violation that results in a presumed Breach of Unsecured PHI), Anthem shall notify HHS in writing within sixty (60) days. Such violations shall be known as Reportable Events. The report to HHS shall include the following information:

a. A description of the event, including the relevant facts, the role(s) of the persons involved, and the provision(s) of the policies and procedures under section V.B. implicated; and

b. A description of the actions taken and any further steps Anthem plans to take to address the matter to mitigate any harm, and to prevent it from recurring, including sanctions, if any.

2. If no Reportable Events occur within the Compliance Term, Anthem shall so inform HHS in its Annual Report as specified in section VI below.

VI. Implementation Report and Annual Reports

A. Implementation Report. Within one-hundred and twenty (120) days after HHS finalizes its review of the Policies and Procedures specified in section V.B. above, Anthem shall submit a written report with the documentation described below to HHS (“Implementation Report”). The Implementation Report shall include:

1. An attestation signed by an officer of Anthem attesting that the policies and procedures submitted to HHS under section V.B. are being implemented;

2. An attestation signed by an officer of Anthem attesting that he or she has reviewed the Implementation Report, has made a reasonable inquiry regarding its content and believes, based upon such inquiry, that the information is accurate and truthful.

B. Annual Reports. The one-year period beginning on the Effective Date and each subsequent one-year period during the course of the Compliance Term shall be referred to as "the Reporting Periods." Anthem shall submit to HHS an Annual Report with respect to the status of and findings regarding Anthem's compliance with this CAP. Anthem shall submit the Annual Report to HHS no later than sixty (60) days after the end of each corresponding Reporting Period. The Annual Report shall include:

1. A summary of Reportable Events (defined in Section V.E.1) identified during the Reporting Period and the status of any corrective and preventative action relating to all such Reportable Events;

2. An attestation signed by an owner or officer of Anthem attesting that he or she has reviewed the Annual Report, has made a reasonable inquiry regarding its content and believes that, upon such inquiry, the information is accurate and truthful.

VII. Document Retention

Anthem shall maintain for inspection and copying, and shall provide to HHS, upon request, all documents and records relating to compliance with this CAP for six (6) years from the Effective Date.

VIII. Breach Provisions

Anthem is expected to fully and timely comply with all provisions contained in this CAP.

A. Timely Written Requests for Extensions

Anthem may, in advance of any due date set forth in this CAP, submit a timely written request for an extension of time to perform any act required by this CAP. A "timely written request" is defined as a request in writing received by HHS at least five (5) days prior to the date such an act is required or due to be performed.

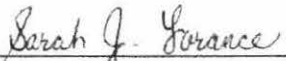
B. Notice of Breach of this CAP and Intent to Impose Civil Money Penalty. The Parties agree that a breach of this CAP by Anthem constitutes a breach of the Agreement. Should HHS believe that Anthem has breached this CAP, HHS will notify Anthem of: (1) its belief that Anthem has breached the agreement and the basis thereof; and (2) HHS' intent to impose a CMP pursuant to 45 C.F.R. Part 160 for the Covered Conduct set forth in section I.5 of the Agreement ("Notice of Breach and Intent to Impose CMP"), including the amount of such CMP.

C. Anthem's Response. Anthem shall have thirty (30) days from the date of receipt of the Notice of Breach and Intent to Impose CMP to demonstrate to HHS' satisfaction that:

1. Anthem is in compliance with the obligations of the CAP that HHS cited as the basis for the breach;
2. The alleged breach has been cured; or
3. The alleged breach cannot be cured within the thirty (30) day period, but that:
(a) Anthem has begun to take action to cure the breach; (b) Anthem is pursuing such action with due diligence; and (c) Anthem has provided HHS a reasonable timetable for curing the breach.

D. Imposition of CMP. If at the conclusion of the thirty (30) day period, Anthem fails to meet the requirements of section VIII.C. of this CAP to HHS' satisfaction, HHS may seek imposition of a CMP against Anthem pursuant to 45 C.F.R. Part 160 for any violations of the HIPAA Rules related to the Covered Conduct set forth in section I.5 of the Agreement. HHS shall promptly notify Anthem in writing of its determination to seek the imposition of a CMP pursuant to 45 C.F.R. Part 160. HHS must offset any CMP amount levied under this section by the amounts already paid by Anthem in lieu of CMPs under the Resolution Agreement. Any such offset will apply only to Covered Conduct up to and including the Effective Date.

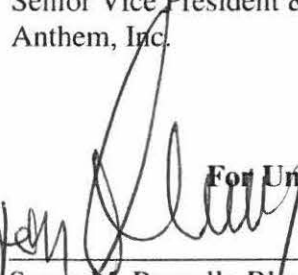
For Anthem, Inc.



Sarah J. Lorance
Senior Vice President & Chief Compliance Officer
Anthem, Inc.

10/15/2018
Date

For United States Department of Health and Human Services



Susan M. Pezzullo Rhodes
Regional Manager, New England Region
Office for Civil Rights

10/15/18
Date