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 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 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. Premera Blue Cross (PBC) is a covered entity and business associate, as defined at 45 C.F.R. § 160.103, and therefore is required to comply with the HIPAA Rules. PBC is a not-for-profit health plan and independent licensee of the Blue Cross Blue Shield Association headquartered in Mountlake Terrace, Washington, with operations in Spokane, Washington, and Anchorage, Alaska. PBC is the largest health plan in the Pacific Northwest, providing health insurance to over 2 million people.

   C. HHS and PBC shall together be referred to herein as the "Parties."

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

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

4. Intention of Parties to Effect Resolution. This Agreement is intended to resolve OCR Transaction Number: 15-206552 and any potential violations of the HIPAA Rules related to the Covered Conduct specified in paragraph 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 March 17, 2015, PBC submitted a breach report indicating that it experienced a cyberattack beginning on May 5, 2014. The cyber-attackers gained impermissible access to the electronic protected health information (ePHI) of 10,466,692 individuals. The attackers initially gained unauthorized access to PBC's network through an email phishing campaign which installed malware on a system in the Premera network beginning on May 5, 2014 and went undetected until January 29, 2015. HHS's investigation indicated potential violations of the following provisions ("Covered Conduct"):

A. The requirement to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by PBC. *See* 45 C.F.R. § 164.308(a)(1)(ii)(A).

B. The requirement to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. *See* 45 C.F.R. § 164.308(a)(1)(ii)(B).

C. Until March 8, 2015, the requirement to implement sufficient hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. *See* 45 C.F.R. § 164.312(b).

D. The requirement to prevent unauthorized access to the ePHI of 10,466,692 individuals whose information was maintained in PBC's network. *See* 45 C.F.R. §164.502(a).

II. Terms and Conditions

6. Payment. HHS has agreed to accept, and PBC has agreed to pay HHS, the amount of **$6.850.000** ("Resolution Amount"). PBC agrees to pay the Resolution Amount on April 30, 2020, pursuant to written instructions to be provided by HHS.

7. Corrective Action Plan. PBC 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 PBC breaches the CAP, and fails to cure the breach as set forth in the CAP, then PBC will be in breach of this Agreement and HHS will not be subject to the Release set forth in paragraph II.8 of this Agreement.

8. Release by HHS. In consideration of and conditioned upon PBC's performance of its obligations under this Agreement, HHS releases PBC from any actions it may have against PBC under the HIPAA Rules arising out of or related to the Factual Background and Covered Conduct identified in paragraph I.5. of this Agreement. HHS does not release PBC 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. PBC 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. PBC 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 PBC 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. No Additional Releases. This Agreement is intended to be for the benefit of the Parties only, and by this instrument the Parties do not release any claims against or by any other person or entity.

13. 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.

14. 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").

15. 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, PBC agrees that the time between the Effective Date of this Agreement (as set forth in Paragraph 14) and the date the Agreement may be terminated by reason of PBC'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. PBC waives and will not plead any statute of limitations, laches, or similar defenses to any administrative action relating to the covered conduct identified in paragraph 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.

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

17. 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.

18. Authorizations. The individual(s) signing this Agreement on behalf of PBC represent and warrant that they are authorized by PBC 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 Premera Blue Cross

/s/ **3/27/2020**

Sven Peterson
Vice President of Compliance, Ethics and Regulatory Services
Corporate Compliance and Ethics Officer
Premera Blue Cross

Date

For the United States Department of Health and Human Services

/s/ **3/30/2020**

Michael Leoz
Regional Manager, Pacific Region
U.S. Department of Health and Human Services
Office for Civil Rights

Date

Appendix A CORRECTIVE ACTION PLAN BETWEEN THE DEPARTMENT OF HEALTH AND HUMAN SERVICES AND PREMERA BLUE CROSS

I. Preamble

Premera Blue Cross (PBC) 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, PBC is entering into a Resolution Agreement ("Agreement") with HHS, and this CAP is incorporated by reference into the Resolution Agreement as Appendix A. PBC enters into this CAP as part of consideration for the release set forth in paragraph II.8 of the Agreement.

II. Contact Persons and Submissions

A. Contact Persons

PBC 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:

Gabriel Bender
Dir. Privacy & Data Governance
Premera Blue Cross
7001 220th St. SW
Mountlake Terrace, WA 98043

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

Danielle Archuleta
Supervisory Equal Opportunity Specialist
Office for Civil Rights, Pacific Region
U.S. Department of Health and Human Services
701 5th Avenue, Suite 1600, MS-11
Seattle, WA 98104

PBC 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.14 of the Agreement ("Effective Date"). The period for compliance ("Compliance Term") with the obligations assumed by PBC 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 the two (2) year period, HHS has notified PBC under Section VIII.B hereof of its position that PBC 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 PBC that it has determined that the breach has been cured or (2) notifies PBC under VIII.D hereof that it will seek imposition of a CMP. After the Compliance Term ends, PBC 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. Nothing in this CAP is intended to eliminate or modify PBC's obligation to comply with the document retention requirements in 45 C.F.R. § 164.316(b) and § 164.530(j).

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

PBC agrees to the following:

A. Conduct Risk Analysis

1. PBC shall conduct an accurate and thorough Risk Analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by PBC.

2. PBC shall provide the Risk Analysis, consistent with section V.A.1 to HHS within ninety (90) days of the Effective Date for HHS's review. HHS shall approve, or, if necessary, require revisions to PBC's Risk Analysis. The risk analysis shall include all ePHI created, received, maintained, or transmitted by PBC, and include but not be limited to, ePHI stored on or accessed by electronic information systems, networks, and applications administered or controlled by PBC. PBC may submit a Risk Analysis currently underway or previously completed within the past 180 days for consideration by HHS for compliance with this provision.

3. Within sixty (60) days of its receipt of PBC's Risk Analysis, HHS will inform PBC in writing in writing as to whether HHS approves the Risk Analysis or HHS requires revisions. If HHS requires revisions to the Risk Analysis, HHS shall provide PBC with a written explanation of the basis of its revisions, including comments and recommendations that PBC can use to prepare a revised Risk Analysis.

4. Upon receiving HHS's notice of required revisions, if any, PBC shall have sixty (60) days to revise the Risk Analysis accordingly and forward to HHS for review and approval. This process shall continue until HHS approves the Risk Analysis.

5. PBC shall review the Risk Analysis annually (or more frequently, if appropriate) and shall promptly update the Risk Analysis in response to environmental or operational changes affecting the security of ePHI. Following an update to the Risk Analysis, PBC shall assess whether its existing security measures are sufficient to protect its ePHI and revise its Risk Management Plan, Policies and Procedures, and training materials and implement additional security measures, as needed.

B. Develop and Implement Risk Management Plan

1. PBC shall develop an enterprise-wide Risk Management Plan to address and mitigate any security risks and vulnerabilities found in the Risk Analysis specified in section V.A. above. The Risk Management Plan shall include a process and timeline for PBC's implementation, evaluation, and revision of its risk remediation activities.

2. Within sixty (60) days of HHS's final approval of the Risk Analysis described in section V.A. above, PBC shall submit a Risk Management Plan to HHS for HHS's review and approval. PBC may submit a Risk Management Plan developed in response to a Risk Analysis currently underway or previously completed for consideration by HHS for compliance with this provision.

3. Within sixty (60) days of receipt of PBC's Risk Management Plan, HHS will inform PBC in writing as to whether HHS approves the Risk Management Plan or HHS requires revisions. If HHS requires revisions to the Risk Management Plan, HHS shall provide PBC with a written explanation of the basis of its revisions, including comments and recommendation that PBC can use to prepare a revised Risk Management.

4 Upon receiving HHS's notice of required revisions, if any, PBC shall have sixty (60) days to revise the Risk Management Plan accordingly and forward for review and approval. This process shall continue until HHS approves the Risk Management Plan.

5. Within sixty (60) days of HHS's approval of the Risk Management Plan, PBC shall finalize and officially adopt the Risk Management Plan in accordance with its applicable administrative procedures. PBC shall then begin implementation of any steps to address or mitigate the risks and vulnerabilities as required by the Risk Management Plan.

C. Policies and Procedures

1. PBC shall review, and as necessary, develop, maintain, and revise, the written Privacy and Security Policies and Procedures ("policies and procedures") addressing the Minimum Content set forth in section V.E to confirm compliance with the Federal standards that govern the security of individually identifiable health information. (45 C.F.R. Part 160 and 164, Subpart C (the "Security Rules")).

2. PBC shall provide the policies and procedures identified in section V.C.1 above to HHS for review within one-hundred fifty (150) days of the Effective Date.

3. Within sixty (60) days of its receipt of PBC's submitted policies and procedures, HHS will inform PBC whether it has any feedback on the submitted policies and procedures.

4. Upon receiving any recommended changes to such policies and procedures from HHS to confirm compliance with the Security Rule, PBC 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.

5. Within thirty (30) days after receiving HHS' final approval of any revisions to the policies and procedures described in Section V.C.1, PBC shall implement the policies and procedures.

D. Distribution and Updating of Policies and Procedures

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

E. 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. Risk Analysis - 45 C.F.R. § 164.308(a)(1)(ii)(A)

2. Risk Management - 45 C.F.R. § 164.308(a)(1)(ii)(B)

3. Information System Activity Review - 45 C.F.R. § 308(a)(1)(ii)(D)

4. Access Controls - 45 C.F.R. § 164.312(a)

5. Audit Controls - 45 C.F.R. §164.312(b)

6. Integrity - 45 C.F.R. § 312(c)(1)

7. Person or Entity Authentication - 45 C.F.R. § 312(d)

8. Transmission Security - 45 C.F.R. § 312(e)

F. Reportable Events

1. During the Compliance Term, in the event PBC receives information that a workforce member subject to the policies and procedures adopted by PBC under section V.C.5 may have failed to comply with those policies and procedures, PBC shall promptly investigate this matter. If PBC determines, after such investigation, that during the Compliance Term a member of its workforce subject to the policies and procedures adopted by PBC under section V.C.5 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), PBC 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) persons involved, and the applicable provision(s) of PBC's policies and procedures implicated; and

b. A description of the actions taken and any further steps PBC 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 during the Compliance term, PBC shall so inform HHS in its Annual Report as specified in Section VI below.

VI. Implementation Report and Annual Reports

A. Implementation Report. Within 120 days after HHS approves the policies and procedures specified in Section V.C. above, PBC 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 PBC attesting that the policies and procedures submitted to HHS under Section V.C. are being implemented;

2. An attestation signed by an officer of PBC stating 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." PBC also shall submit to HHS Annual Reports with respect to the status of and findings regarding PBC's compliance with this CAP for each of the Reporting Periods. PBC shall submit each 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.F.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 officer of PBC 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

PBC 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

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

A. Timely Written Requests for Extensions. PBC 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 days prior to the date such an act is required or due to be performed. This requirement may be waived by HHS only.

B. Notice of Breach of this CAP and Intent to Impose Civil Monetary Penalty. The Parties agree that a breach of this CAP by PBC constitutes a breach of the Agreement. Upon a determination by HHS that PBC has breached this CAP, HHS may notify PBC of: (1) its belief that PBC 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 paragraph I.5 of the Agreement ("Notice of Breach and Intent to Impose CMP"), including the amount of such CMP.

C. PBC's Response. PBC 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. PBC 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 30-day period, but that: (a) PBC has begun to take action to cure the breach; (b) PBC is pursuing such action with due diligence; and (c) PBC has provided to HHS a reasonable timetable for curing the breach.

D. Imposition of CMP. If at the conclusion of the 30-day period, PBC fails to meet the requirements of Section VIII.C. of this CAP to HHS' satisfaction, HHS may proceed with the imposition of a CMP against PBC pursuant to 45 C.F.R. Part 160 for any violations of the HIPAA Rules related to Covered Conduct set forth in paragraph I.5 of the Agreement. HHS shall promptly notify PBC in writing of its determination to proceed with 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 PBC 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 Premera Blue Cross

/s/ **3/27/2020**

Sven Peterson
Vice President of Compliance, Ethics and
Regulatory Services
Corporate Compliance and Ethics Officer
Premera Blue Cross

Date

For the United States Department of Health and Human Services

/s/ **3/30/2020**

Michael Leoz
Regional Manager, Pacific Region
U.S. Department of Health and Human Services
Office for Civil Rights

Date