

TIMOTHY C. FOX
Montana Attorney General
KELLEY L. HUBBARD
Assistant Attorney General
P.O. Box 200151
555 Fuller Ave.
Helena, MT 59620-0151
(406) 444-2026
khubbard@mt.gov

**MONTANA FIRST JUDICIAL DISTRICT COURT
LEWIS AND CLARK COUNTY**

STATE OF MONTANA,

Plaintiff,

v.

PREMERA BLUE CROSS,

Defendant.

Cause No. ADV-2019-934

**CONSENT JUDGMENT
AND ORDER**

I.

1.1 Plaintiff State of Montana (“the State”) conducted an investigation and commenced this action pursuant to the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the Department of Health and Human Services (“HHS”) Regulations, 45 C.F.R. §§ 160 *et seq.* (“HIPAA”) and the Montana Unfair Trade Practices and Consumer Protection Act, Mont. Code Ann. § 30-14-101 *et seq.* (“Consumer Protection Act”).

1.2 Plaintiff appears by and through its attorneys Timothy C. Fox, Montana Attorney General and Kelley L. Hubbard, Assistant Attorney General; and Premera Blue Cross as defined

1 in Paragraph 3.14 (“PREMERA”), appears by and through their attorneys, Nathan A. Schacht,
2 Theodore J. Kobus, III, and Patrick H. Haggerty.

3 1.3 Plaintiff and PREMERA stipulate to the entry of this Consent Judgment by the
4 Court without the taking of proof and without trial or adjudication of any fact or law.

5 1.4 Plaintiff alleges that on March 17, 2015, Premera publicly announced a data security
6 incident involving its computer network system which resulted in the unauthorized disclosure of
7 certain consumers’ personal information and protected health information.

8 1.5 Plaintiff and PREMERA agree that this Consent Judgment does not constitute
9 evidence or an admission regarding the existence or non-existence of any issue, fact, or violation of
10 any law alleged by Plaintiff.

11 1.6 PREMERA recognizes and states that this Consent Judgment is entered into
12 voluntarily and that no promises or threats have been made by the Attorney General’s Office or any
13 member, officer, agent or representative thereof to induce it to enter into this Consent Judgment,
14 except as provided herein.

15 1.7 PREMERA waives any right they may have to appeal from this Consent Judgment.

16 1.8 PREMERA further agrees that it will not oppose the entry of this Consent Judgment
17 on the grounds the Consent Judgment fails to comply with Rule 65(d) of the Rules of Civil
18 Procedure, and hereby waives any objections based thereon.

19 1.9 PREMERA further agrees that this Court shall retain jurisdiction of this action for
20 the purpose of implementing and enforcing the terms and conditions of the Consent Judgment and
21 for all other purposes.

22 The Court finding no just reason for delay;

23 NOW, THEREFORE, it is hereby **ORDERED, ADJUDGED, AND DECREED** as
24 follows:
25
26

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

II. PARTIES AND JURISDICTION

2.1 The State of Montana is the Plaintiff in this case.

2.2 Premera Blue Cross is a Washington non-profit corporation with its principal office located at 7001 220th St. SW, Building 1, Mountlake Terrace, Washington 98043.

2.3 This Court has jurisdiction of the subject matter of this action, jurisdiction over the parties to this action, and venue is proper in this Court. Mont. Code Ann. § 30-14-111.

2.4 Venue is proper pursuant to Mont. Code Ann. § 30-14-111(3) and PREMERA consents to the filing of this Consent Judgment in a county where the Attorney General maintains an office for the limited purpose of resolving the claims at issue.

2.5 For the purposes of this Consent Judgment, or any action to enforce this Consent Judgment, PREMERA consents to the Court’s jurisdiction over this Consent Judgment and consents to venue in this judicial district.

2.6 This Consent Judgment is entered pursuant to and subject to the Montana Consumer Protection Act.

III. DEFINITIONS

3.1 “COVERED SYSTEMS” shall mean all components, including but not limited to, assets, technology, and software, within the PREMERA NETWORK that are used to collect, process, transmit, and/or store PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION.

3.2 “CONSUMER PROTECTION LAWS” shall mean the Montana Unfair Trade Practices and Consumer Protection Act, Mont. Code Ann. § 30-14-101 *et seq.*

3.3 “DESIGNATED PRIVACY OFFICIAL” shall mean the individual designated by PREMERA who is responsible for the development and implementation of the policies and procedures as required by 45 C.F.R. § 164.530(a).

1 3.4 “DESIGNATED SECURITY OFFICIAL” shall mean the individual designated
2 by PREMERA who is responsible for the development and implementation of the policies and
3 procedures as required by 45 C.F.R. § 164.308(a)(2).

4 3.5 “EFFECTIVE DATE” shall be July 11, 2019.

5 3.6 “ENCRYPTED” shall refer to the existing industry standard to encode or obscure
6 data at rest or in transit. As of the EFFECTIVE DATE, the existing industry standard shall be
7 AES 256-bit encryption or Transport Layer Security (TLS) 1.2, or their equivalents.

8 3.7 “GLBA” shall mean the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113
9 Stat. 1338.

10 3.8 “HIPAA” shall mean the Health Insurance Portability and Accountability Act of
11 1996, Pub. L. No. 104-191, 110 Stat. 1938, as amended by the Health Information Technology
12 for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the
13 Department of Health and Human Services (“HHS”) Regulations, 45 C.F.R. §§ 160 *et seq.*

14 3.9 “HIPAA SECURITY RULE” shall mean the Security Standards for the
15 Protection of Electronic Protected Health Information, 45 C.F.R. Part 160 and Part 164, Subparts
16 A and E.

17 3.10 “HIPAA PRIVACY RULE” shall mean the Standards for Privacy of Individually
18 Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and E.

19 3.11 “MULTI-FACTOR AUTHENTICATION” means authentication through
20 verification of at least two of the following authentication factors: (i) Knowledge factors, such
21 as a password; or (ii) Possession factors, such a token or text message on a mobile phone; or (iii)
22 Inherence factors, such as a biometric characteristic.

23 3.12 “MULTISTATE EXECUTIVE COMMITTEE” shall mean the Attorneys
24 General of the States of Washington, Oregon, and California.

25 3.13 “PERSONAL INFORMATION” shall have the same meaning as listed in the
26 Impediment of Identity Theft Act, Mont. Code Ann. §30-14-1701 and -1704.

1
2 3.14 "PREMERA" shall mean Premera Blue Cross, its parent and its directly or
3 indirectly wholly-owned or controlled affiliates, subsidiaries and divisions, successors and
4 assigns.¹

5 3.15 "PREMERA NETWORK" shall mean all networking equipment, databases or
6 data stores, applications, servers, and endpoints that are capable of using and sharing software,
7 data, and hardware resources, and that are owned, operated, and/or controlled by PREMERA.

8 3.16 "PROTECTED HEALTH INFORMATION" shall mean "individually
9 identifiable health information" as defined by the Health Insurance Portability and
10 Accountability Act (HIPAA), as amended by the Health Information Technology and Clinical
11 Act (HITECH) and 45 C.F.R. § 160.103.

12 3.17 "SECURITY BREACH NOTIFICATION ACT" shall mean the Montana
13 Impediment of Identity Theft Act, Mont. Code Ann. § 30-14-1701 *et seq.*

14 3.18 "SECURITY INCIDENT" shall mean any compromise to the confidentiality,
15 integrity, or availability of a PREMERA information asset that includes PERSONAL
16 INFORMATION or PROTECTED HEALTH INFORMATION.

17 IV. INJUNCTIVE RELIEF

18 4.1 Application of Injunctions. The injunctive provisions of this Consent Judgment
19 shall apply to PREMERA and its officers, directors, and employees..

20 4.2 Injunctions. PREMERA shall engage in or refrain from engaging in the practices
21 as identified in this Consent Judgment.

22 4.3 COMPLIANCE WITH STATE AND FEDERAL LAW:

23
24
25 ¹ For purposes of this definition, "control" means the possession, directly or indirectly, of the power to
26 direct or cause the direction of the management and policies of an entity through majority ownership or voting
power.

1 a. PREMERA shall comply with all applicable CONSUMER PROTECTION LAWS
2 in connection with its collection, maintenance, and safeguarding of PERSONAL INFORMATION.

3 b. PREMERA shall comply with the SECURITY BREACH NOTIFICATION ACT.

4 c. PREMERA shall comply with the HIPAA in connection with its collection,
5 maintenance, and safeguarding of PROTECTED HEALTH INFORMATION.

6 d. PREMERA shall not make any representations or material omissions of fact that are
7 capable of misleading consumers regarding the extent to which PREMERA maintains and/or
8 protects the privacy, security, confidentiality, or integrity of any PERSONAL INFORMATION or
9 PROTECTED HEALTH INFORMATION collected from or about consumers.

10 **4.4 COMPLIANCE PROGRAM:**

11 a. PREMERA shall perform a comprehensive review and assessment of the
12 effectiveness of its compliance program (“Compliance Program”) pursuant to the terms of
13 Paragraph 5.2.

14 b. PREMERA shall ensure that its Compliance Program is reasonably designed to
15 ensure compliance with applicable federal and state laws related to data security and privacy.

16 c. PREMERA shall continue to employ an executive or officer who shall be
17 responsible for implementing, maintaining, and monitoring the Compliance Program (for ease,
18 hereinafter referred to as the “Compliance Officer”). The Compliance Officer shall have the
19 appropriate background or experience in compliance, including appropriate training in compliance
20 with HIPAA, GLBA, and applicable state laws relating to privacy or data security.

21 d. The Compliance Officer shall continue to oversee PREMERA’s Compliance
22 Program, and shall function as an independent and objective body that reviews and evaluates
23 compliance within PREMERA. The Compliance Officer shall develop a process for evaluating
24 compliance risks and determining priorities, reviewing compliance plans, and ensuring follow-up
25 to compliance issues identified occurs within a reasonable timeframe and that processes are in place
26

1 for determining and implementing appropriate disciplinary and corrective actions when violations
2 arise.

3 e. PREMERA shall continue to ensure that the Compliance Officer has direct access
4 to the Chief Executive Officer and the Audit and Compliance Committee of the Board of Directors.

5 f. PREMERA shall ensure that its Compliance Program continues to receive the
6 resources and support necessary to ensure that the Compliance Program functions as required and
7 intended by this Consent Judgment.

8 g. PREMERA may satisfy the implementation and maintenance of the Compliance
9 Program and the safeguards required by this Consent Judgment through review, maintenance, and,
10 if necessary, updating of an existing compliance program or existing safeguards, provided that such
11 existing compliance program and existing safeguards meet the requirements set forth in this
12 Consent Judgment.

13 4.5 **INFORMATION SECURITY PROGRAM:**

14 a. PREMERA may satisfy the implementation and maintenance of the Information
15 Security Program and the safeguards and controls required by this Consent Judgment through
16 review, maintenance, and, if necessary, updating of an existing information security program or
17 existing controls and safeguards, provided that such existing compliance program and existing
18 safeguards and controls meet the requirements set forth in this Consent Judgment.

19 b. PREMERA shall implement, maintain, regularly review and revise, and comply
20 with a comprehensive information security program (“Information Security Program”) that is
21 reasonably designed to protect the security, integrity, availability, and confidentiality of the
22 PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION that PREMERA
23 collects, stores, transmits, and/or maintains.

24 c. PREMERA’s Information Security Program shall document the administrative,
25 technical, and physical safeguards appropriate to:

26 (i). The size and complexity of PREMERA’s operations;

- 1 (ii). The nature and scope of PREMERA’s activities; and
- 2 (iii). The sensitivity of the PERSONAL INFORMATION or PROTECTED
- 3 HEALTH INFORMATION that PREMERA collects, stores, transmits, and/or maintains.
- 4 d. As part of its Information Security Program, PREMERA will not trust traffic on
- 5 the PREMERA NETWORK. In order to trust the traffic, PREMERA shall:
- 6 (i). Regularly monitor, log, and inspect all network traffic, including log-in
- 7 attempts, through the implementation of hardware, software, or procedural mechanisms that record
- 8 and examine such activity;
- 9 (ii). Ensure that every device, user, and network flow is authorized and
- 10 authenticated; and
- 11 (iii). Only allow access by users of the PREMERA NETWORK to the minimum
- 12 extent necessary and require appropriate authorization and authentication prior to allowing any such
- 13 access.
- 14 e. The Information Security Program shall be designed to:
- 15 (i). Protect the security, integrity, availability, and confidentiality of
- 16 PERSONAL INFORMATION and PROTECTED HEALTH INFORMATION;
- 17 (ii). Protect against any threats to the security, integrity, availability, or
- 18 confidentiality of PERSONAL INFORMATION and PROTECTED HEALTH INFORMATION;
- 19 (iii). Protect against unauthorized access to or use of PERSONAL
- 20 INFORMATION and PROTECTED HEALTH INFORMATION and minimize the likelihood of
- 21 harm to any consumer;
- 22 (iv). Define and periodically reevaluate a schedule for retention of PERSONAL
- 23 INFORMATION and PROTECTED HEALTH INFORMATION and for its destruction when such
- 24 information is no longer needed for business purposes;
- 25
- 26

1 (v). Restrict access within the PREMERA NETWORK based on necessity and
2 job function, including but not limited to by restricting access to the PERSONAL INFORMATION
3 and PROTECTED HEALTH INFORMATION within the PREMERA NETWORK;

4 (vi). Assess the number of users on PREMERA's applications and retire any
5 application with no active users and that no longer have a business purpose.

6 (vii). Restrict the ability of PREMERA employees and vendors to access the
7 PREMERA NETWORK via personal devices (e.g., smartphones, tablets, personal laptops);
8 PREMERA shall permit access only based on a business need. If required, the access shall be
9 restricted to only the data, systems, and other network resources required for the vendor's or
10 employee's job. Any access to the PREMERA NETWORK via a personal device shall be reviewed
11 on a regular basis to determine if the vendor's or employee's job function requires this access.
12 Furthermore, this access shall be provided via a secured connection to the PREMERA NETWORK
13 via VPN and MULTI-FACTOR AUTHENTICATION or other greater security safeguards; and

14 (viii). Restrict the ability of PREMERA's employees and vendors to use
15 PREMERA assets (critical and non-critical) to access personal email, and social media, and file-
16 sharing sites. For PREMERA's employees, PREMERA shall only permit access to non-
17 PREMERA resources based on a business need.

18 f. PREMERA may satisfy the implementation and maintenance of the Information
19 Security Program and the safeguards required by this Consent Judgment through review,
20 maintenance, and, if necessary, updating, of an existing information security program or existing
21 safeguards, provided that such existing information security program and existing safeguards
22 meet the requirements set forth in this Consent Judgment.

23 g. PREMERA shall employ an executive or officer who shall be responsible for
24 implementing, maintaining, and monitoring the Information Security Program (for ease,
25 hereinafter referred to as the "Chief Information Security Officer"). The Chief Information
26 Security Officer shall have the appropriate background or experience in information security and

1 HIPAA compliance. PREMERA shall ensure that the Chief Information Security Officer is a
2 separate position from the Chief Information Officer, and shall serve as PREMERA's
3 DESIGNATED SECURITY OFFICIAL. The Chief Information Security Officer shall have
4 direct access to the Chief Executive Officer and the Audit and Compliance Committee of the
5 Board of Directors.

6 h. PREMERA shall ensure that the role of the Chief Information Security Officer
7 includes directly advising PREMERA's Board of Directors, Chief Executive Officer, and Chief
8 Information Officer on the management of PREMERA's security posture, the security risks
9 faced by PREMERA, the security implications of PREMERA's decisions, and the adequacy of
10 PREMERA's Information Security Program. The Chief Information Security Officer shall meet
11 with, and provide an oral or written update to: (1) the Board of Directors on at least an annual
12 basis; (2) the Chief Executive Officer at least every two months; (3) the Chief Information
13 Officer on at least a twice per month basis; and (4) the DESIGNATED PRIVACY OFFICIAL
14 at least every two months. The Chief Information Security Officer shall inform the Chief
15 Executive Officer, the Chief Information Officer, and the DESIGNATED PRIVACY
16 OFFICIAL of any material unauthorized intrusion to the PREMERA NETWORK within forty-
17 eight (48) hours of discovery of the intrusion. A material unauthorized intrusion is any intrusion
18 to the PREMERA NETWORK that affects or may affect any PROTECTED HEALTH
19 INFORMATION or PERSONAL INFORMATION.

20 i. PREMERA shall ensure that the Chief Information Security Officer and
21 Information Security Program receive the resources and support necessary to ensure that the
22 Information Security Program functions as intended by this Consent Judgment.

23 j. PREMERA shall ensure that employees who are responsible for implementing,
24 maintaining, or monitoring the Information Security Program, including but not limited to the
25 Chief Information Officer and Chief Information Security Officer, have sufficient knowledge of
26 the requirements of the Consent Judgment.

1 k. At least once each year, PREMERA shall provide training on safeguarding and
2 protecting consumer PERSONAL INFORMATION and PROTECTED HEALTH
3 INFORMATION to all employees who handle such information, and its employees responsible
4 for implementing, maintaining, or monitoring the Information Security Program. PREMERA's
5 Information Security Program shall be designed and implemented to ensure the appropriate and
6 timely identification, investigation of, and response to SECURITY INCIDENTS.

7 l. PREMERA shall provide its DESIGNATED PRIVACY OFFICIAL with
8 appropriate training to ensure the official is able to implement the requirements of and ensure
9 compliance with the HIPAA PRIVACY AND SECURITY RULES.

10 m. PREMERA shall provide its DESIGNATED SECURITY OFFICAL with
11 appropriate training to ensure the official is able to implement the requirements of and ensure
12 compliance with the HIPAA SECURITY RULE.

13 n. PREMERA shall maintain a written incident response plan to prepare for and
14 respond to SECURITY INCIDENTS. PREMERA shall revise and update this response plan, as
15 necessary, to adapt to any changes to the PREMERA NETWORK and its COVERED
16 SYSTEMS. Such a plan shall, at a minimum, identify and describe the following phases:

- 17 (i). Preparation;
- 18 (ii). Investigation, Detection and Analysis;
- 19 (iii). Containment;
- 20 (iv). Notification and Coordination with Law Enforcement;
- 21 (v). Eradication;
- 22 (vi). Recovery;
- 23 (vii). Consumer and Regulator Notification and Remediation; and
- 24 (viii). Post-Incident Analysis (Lessons Learned).

25 o. For each SECURITY INCIDENT, PREMERA shall create a report that includes
26 a description of the SECURITY INCIDENT and PREMERA's response to that SECURITY

1 INCIDENT (“Security Incident Report”). The Security Incident Report shall be made available
2 for the Third-Party Assessment as described in Paragraph 5.1.

3 p. PREMERA shall make reasonable efforts to ensure that any service providers or
4 vendors it employs that handle PERSONAL INFORMATION or PROTECTED HEALTH
5 INFORMATION shall (1) have safeguards in place to protect any of PERSONAL
6 INFORMATION, or PROTECTED HEALTH INFORMATION, and (2) notify PREMERA
7 promptly after discovering any potential compromise of the confidentiality, integrity, or
8 availability of PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION that
9 is held, stored or processed by the service provider or vendor on behalf of PREMERA.

10 **4.6 PERSONAL INFORMATION AND PROTECTED HEALTH**
11 **INFORMATION SAFEGUARDS AND CONTROLS:**

12 a. On an annual basis, PREMERA shall review, and if necessary update, its data
13 retention policies to ensure that its PERSONAL INFORMATION and PROTECTED HEALTH
14 INFORMATION within the PREMERA NETWORK is only collected, stored, maintained,
15 and/or processed to the extent necessary to accomplish the intended purpose in using such
16 information.

17 b. PREMERA shall implement, maintain, regularly review and revise, and comply
18 with policies and procedures to ENCRYPT PERSONAL INFORMATION and PROTECTED
19 HEALTH INFORMATION, whether the information is transmitted electronically over a
20 network or is stored on any media, whether it be static, removable, or otherwise.

21 **4.7 SPECIFIC TECHNICAL SAFEGUARDS AND CONTROLS:**

22 a. Asset Inventory and Managing Critical Assets:

- 23 (i). PREMERA shall, within one hundred and eighty days (180) days of the
24 EFFECTIVE DATE of this Consent Judgment, implement and maintain a
25 configuration management database that contains an asset inventory for
26 all known Critical Assets that identifies: (a) the name of the asset; (b) the

1 version of the asset; (c) the owner of the asset; (d) the asset's location
2 within the PREMERA NETWORK; (e) whether the asset is a Critical
3 Asset; and (f) the date that each security update or patch was applied.
4 PREMERA shall apply the highest rating it uses for any asset that either
5 it uses to collect, store, transmit, or use PERSONAL INFORMATION or
6 PROTECTED HEALTH INFORMATION ("Critical Assets").

7 (ii). PREMERA shall, within one year of the EFFECTIVE DATE of this
8 Consent Judgment, implement and maintain an asset inventory for all
9 assets that identifies: (a) the name of the asset; (b) the version of the asset;
10 (c) the owner of the asset; (d) the asset's location within the PREMERA
11 NETWORK; (e) whether the asset is a Critical Asset; and (f) the date that
12 each security update or patch was applied.

13 b. Mapping and Encryption of Sensitive Data:

14 (i). PREMERA shall, within nine (9) months of the EFFECTIVE DATE,
15 identify and map all locations where PERSONAL INFORMATION or PROTECTED HEALTH
16 INFORMATION is collected, stored, received, maintained, processed or transmitted within the
17 PREMERA network. PREMERA shall perform this identification and mapping procedure at least
18 annually. Any such documentation must be made available for inspection for the Assessment as
19 described in Paragraph 5.1.

20 (ii). PREMERA shall ensure that electronic PERSONAL INFORMATION or
21 PROTECTED HEALTH INFORMATION that is stored at rest or is in transmission is
22 ENCRYPTED except where PREMERA determines that ENCRYPTION is not reasonable and
23 appropriate and it documents the rationale for this decision.

24 c. Segmentation: PREMERA shall implement and maintain segmentation protocols
25 and related policies that are reasonably designed to properly segment the PREMERA
26 NETWORK, which shall, at a minimum, ensure system functionality and performance to meet

1 business needs while also mitigating exposure to the enterprise network in the event of an attack
2 or malicious intruder access. Additionally, PREMERA shall regularly evaluate, and as
3 appropriate, restrict and disable any unnecessary ports of service on the PREMERA
4 NETWORK.

5 d. Penetration Testing: PREMERA shall engage a third-party vendor to perform an
6 annual penetration test to the PREMERA NETWORK, and shall ensure any risks or
7 vulnerabilities identified are risk assessed, prioritized, and addressed under PREMERA'S
8 Information Security Program. The parties understand and agree that addressing a risk may
9 include remediation or alternate risk mitigation efforts based on the risk assessment in Paragraph
10 4.7(e).

11 e. Risk Assessment: PREMERA shall conduct an accurate and thorough risk
12 assessment on any material risks and/or vulnerabilities identified by its internal auditors or
13 through penetration testing as required by Paragraph 4.7(d) within thirty (30) days of
14 identification of the risk or vulnerability to the PREMERA NETWORK and its COVERED
15 SYSTEMS. PREMERA shall rate each vulnerability on a risk-based rating scale developed by
16 PREMERA that takes into account cybersecurity best practices and risk to PERSONAL
17 INFORMATION and PROTECTED HEALTH INFORMATION. PREMERA shall ensure that
18 risks or vulnerabilities that threaten the safeguarding or security of any PERSONAL
19 INFORMATION or PROTECTED HEALTH INFORMATION maintained on the PREMERA
20 NETWORK shall be addressed and remediated as expeditiously as possible. PREMERA shall
21 document in writing any decision not to address a risk or vulnerability that threatens the
22 safeguarding or security of any PERSONAL INFORMATION or PROTECTED HEALTH
23 INFORMATION maintained on the PREMERA NETWORK.

24 (i). The risk assessment shall include an accurate and thorough assessment of
25 the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic
26

1 | protected health information held as required by HIPAA Security Rule, 45 C.F.R. §
2 | 164.308(a)(1)(ii)(A).

3 | (ii). PREMERA shall implement and maintain a corresponding risk-assessment
4 | program designed to identify and assess risks to the PREMERA NETWORK. In cases where
5 | PREMERA deems quantitative risk to be acceptable, PREMERA shall generate and retain a report
6 | demonstrating how such risks are to be managed in consideration of the risk to PERSONAL
7 | INFORMATION and PROTECTED HEALTH INFORMATION, if applicable, and the cost or
8 | difficulty in implementing effective countermeasures. All reports shall be maintained by the Chief
9 | Information Security Officer and be available for inspection by its DESIGNATED PRIVACY
10 | OFFICIAL, and the Third-Party Assessor described in Paragraph 5.1 of this Consent Judgment.

11 | f. Secure Network Communications: PREMERA shall implement and maintain
12 | controls that filter incoming emails for potential phishing attacks or other fraudulent emails and
13 | that establish strong peer-to-peer communications between its employees and vendors. In
14 | addition, PREMERA will secure external communications to limit the ability of an attacker or
15 | malicious intruder to communicate from the PREMERA NETWORK to unknown IP addresses.

16 | g. Access Control and Account Management: PREMERA shall implement and
17 | maintain appropriate controls to manage access to accounts and shall take into account whether the
18 | user is on a PREMERA device or a non-PREMERA device, such as a personal device, and whether
19 | the user is physically located at a PREMERA site or connecting to PREMERA through a remote
20 | connection.

21 | (i). PREMERA shall, within nine (9) months of the EFFECTIVE DATE,
22 | implement and maintain appropriate controls to manage access to, and use of, all administrator,
23 | service, and vendor accounts with access to PERSONAL INFORMATION or PROTECTED
24 | HEALTH INFORMATION. Such controls shall include, without limitation, (1) strong passwords,
25 | (2) password confidentiality policies, (3) password-rotation policies, (4) MULTI-FACTOR
26 |

1 AUTHENTICATION or any other equal or greater authentication protocol for identity
2 management, and (5) appropriate safeguards for administrative level passwords.

3 (ii). PREMERA shall implement and maintain appropriate controls to manage
4 access to, and use of, all PREMERA employee user accounts with access to PERSONAL
5 INFORMATION or PROTECTED HEALTH INFORMATION.

6 (iii). PREMERA shall implement and maintain appropriate administrative
7 processes and procedures to store and monitor the account credentials and access privileges of
8 employees who have privileges to design, maintain, operate, and update the PREMERA
9 NETWORK.

10 (iv). PREMERA shall implement and maintain appropriate policies for the
11 secure storage of account passwords, including, without limitation, hashing passwords stored online
12 using an appropriate hashing algorithm that is not vulnerable to a collision attack, and an appropriate
13 salting policy.

14 (v). PREMERA shall implement and maintain adequate access controls,
15 processes, and procedures, the purpose of which shall be to grant access to the PREMERA
16 NETWORK only if the user is properly authorized and authenticated.

17 (vi). PREMERA shall immediately disable access privileges for all persons
18 whose access to the PREMERA NETWORK is no longer required or appropriate. PREMERA shall
19 limit access to PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION by
20 persons accessing the PREMERA NETWORK on a least-privileged basis.

21 (vii). PREMERA shall regularly inventory the users who have access to the
22 PREMERA NETWORK in order to review and determine whether or not such access remains
23 necessary or appropriate. PREMERA shall regularly compare employee termination lists to user
24 accounts to ensure access privileges have been appropriately terminated. At a minimum, such
25 review shall be performed on a quarterly basis. When the privileges, including for any disabled
26

1 accounts, are determined to be no longer necessary for any business function, PREMERA shall
2 terminate access privileges for those accounts.

3 (viii). PREMERA shall implement and maintain network endpoint (e.g., devices
4 and PCs) security by using network access controls to identify devices accessing the PREMERA
5 NETWORK, such as an identity-based network access controller or a similar product.

6 h. File Integrity and End-point Monitoring: PREMERA shall deploy and maintain
7 controls designed to provide near real-time and/or real-time notification of unauthorized access
8 to PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION. PREMERA
9 shall, within six (6) months from the EFFECTIVE DATE of this Consent Judgment, deploy and
10 maintain controls designed to provide near real-time or real-time notification of modifications
11 to any applications or systems that either contain or provide access to PERSONAL
12 INFORMATION or PROTECTED HEALTH INFORMATION.

13 i. Controlling Permissible Applications: For servers in the PREMERA
14 NETWORK, PREMERA shall deploy and maintain controls within one year of the EFFECTIVE
15 DATE that are designed to block and/or prevent the execution of unauthorized applications
16 within the PREMERA NETWORK, as prescribed in the implementation standards of the
17 HITRUST framework. For clients (e.g., desktops, laptops, tablets), PREMERA shall maintain
18 the controls prescribed in the implemented HITRUST framework designed to block and/or
19 prevent the execution of unauthorized applications within the PREMERA NETWORK.
20 Additionally, the controls will provide alerts when unauthorized applications attempt to execute
21 on the PREMERA NETWORK.

22 j. Logging and Monitoring: PREMERA shall maintain reasonable policies,
23 procedures, and controls the purpose of which shall be to properly monitor and log activities on
24 the PREMERA NETWORK.

25 (i). PREMERA shall ensure that logs are automatically processed and
26 aggregated, and then actively monitored and analyzed in real time or near real time.

1 (ii). PREMERA shall test at least twice per year, any software, hardware, or
2 service used pursuant to this paragraph, to ensure it is properly configured, and regularly updated
3 and maintained to ensure that all COVERED SYSTEMS are adequately logged and monitored.

4 k. Change Control: PREMERA shall implement and maintain policies and
5 procedures reasonably designed to manage and document changes to the PREMERA
6 NETWORK.

7 l. Updates/Patch Management: PREMERA shall maintain, keep updated, and
8 support the software on the PREMERA NETWORK taking into consideration the impact a
9 software update will have on data security in the context of the entire PREMERA NETWORK and
10 its ongoing business and network operations, and the scope of the resources required to maintain,
11 update and support the software. PREMERA shall deploy and maintain reasonable controls to
12 ensure that risks posed by software no longer supported by the manufacturer are adequately
13 addressed and reasonably mitigated.

14 **V. ASSESSMENT AND REPORTING REQUIREMENTS TO THE ATTORNEY**

15 **GENERAL**

16 5.1 Information Security Assessment:

17 a. PREMERA shall, for a period of three years (3) after the EFFECTIVE DATE of
18 this Consent Judgment, obtain an annual information security assessment and report from a third-
19 party professional (“Third-Party Assessor”) using procedures and standards generally accepted in
20 the profession (“Third-Party Assessment”), commencing within one (1) year after the
21 EFFECTIVE DATE of this Consent Judgment. The Third-Party Assessor’s report on the Third-
22 Party Assessment shall:

23 (i). Set forth the specific administrative, technical, and physical safeguards
24 maintained by PREMERA;

25 (ii). Explain the extent to which such safeguards are appropriate in light of
26 PREMERA’s size and complexity, the nature and scope of PREMERA’s activities, and the

1 sensitivity of the PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION
2 maintained by PREMERA;

3 (iii). Assess and certify the extent to which the administrative, technical, and
4 physical safeguards that have been implemented by PREMERA meet the requirements of the
5 Information Security Program;

6 (iv). Assess and certify the extent to which PREMERA is complying with the
7 requirements of the Information Security Program;

8 (v). Specifically review and evaluate the reasonableness of any decision to not
9 encrypt PERSONAL INFORMATION and PERSONAL HEALTH INFORMATION, in
10 compliance with Paragraph 4.7(b).

11 (vi). Specifically review and evaluate PREMERA's response to SECURITY
12 INCIDENTS in the Security Incident Report (see Paragraph 4.5(o)); and

13 (vii). Specifically review and evaluate PREMERA's compliance with the
14 penetration testing requirements set forth in Paragraph 4.7(d); the risk assessment requirements set
15 forth in Paragraph 4.7(e); the logging and monitoring requirements set forth in Paragraph 4.7(j); the
16 change control requirements set forth in Paragraph 4.7(k); and the updates/patch management
17 requirements set forth in Paragraph 4.7(l).

18 b. The Third-Party Assessor shall be a Certified Information Systems Security
19 Professional ("CISSP") or a Certified Information Systems Auditor ("CISA"), or a similarly
20 qualified person or organization; have at least five (5) years of experience evaluating the
21 effectiveness of computer system security or information system security; and must be approved by
22 the MULTISTATE EXECUTIVE COMMITTEE.

23 c. Each Third-Party Assessment must be completed within sixty (60) days after the
24 end of the reporting period to which the Third-Party Assessment applies. PREMERA shall provide
25 a copy of the Third-Party Assessor's Report on the Third-Party Assessment to the Washington
26 Attorney General's Office within thirty (30) days of the completion of the report.

1 d. The State of Washington shall, to the extent permitted by the laws of the State of
2 Washington, treat such Third-Party Assessor's Report as exempt from disclosure under the relevant
3 public records laws.

4 e. The Washington Attorney General's Office may provide a copy of the Third-Party
5 Assessor's Report received from PREMERA to another Attorney General's Office upon request,
6 and that Attorney General shall, to the extent permitted by the laws of Montana, treat such Third-
7 Party Assessor's Report as exempt from disclosure under the relevant public records laws.

8 5.2 Compliance Program Assessment: Within one-hundred-and-eighty (180) days of
9 the EFFECTIVE DATE of this Consent Judgment, PREMERA shall conduct an assessment of
10 the structure of and personnel responsible for PREMERA's Compliance Program (the
11 "Compliance Program Assessment"). The Compliance Program Assessment required by this
12 paragraph shall be conducted by a third-party professional (the "Compliance Program
13 Assessor").

14 a. The Compliance Program Assessor shall use procedures and standards generally
15 accepted in the profession.

16 b. The Compliance Program Assessor shall:

17 (i). Examine the effectiveness of the PREMERA's Compliance Program;

18 (ii). Examine the independence and effectiveness of the structure of employees
19 responsible for PREMERA's Compliance Program;

20 (iii). Identify any potential conflicts-of-interest that may hinder PREMERA's
21 obligation to comply with state and federal laws related to data security and privacy; and

22 (iv). Examine PREMERA's HIPAA Risk Analysis Assessment and Mitigation
23 Plan, as required by 45 C.F.R. § 164.308(a)(1)(ii)(A) and relevant guidelines provided by the Office
24 for Civil Rights.

25 c. The findings of the Compliance Program Assessment shall be documented in a
26 report (the "Compliance Program Assessor's Report"). PREMERA shall provide a copy of the

1 Compliance Program Assessor's Report to the Washington Attorney General's Office within
2 thirty (30) days of the completion of the Compliance Program Assessment.

3 d. The State of Washington shall, to the extent permitted by the laws of the State of
4 Washington, treat such Compliance Program Assessor's Report as exempt from disclosure under
5 the relevant public records laws.

6 e. The Washington Attorney General's Office may provide a copy of the
7 Compliance Program Assessor's Report received from PREMERA to another Attorney
8 General's Office upon request, and that Attorney General shall, to the extent permitted by the
9 laws of Montana, treat such Compliance Program Assessor's Report as exempt from disclosure
10 under the relevant public records laws.

11 5.3 PREMERA will make reasonable good faith efforts to address any concerns and
12 implement recommendations made by the Third-Party Assessor or the Compliance Assessor.

13 VI. DOCUMENT RETENTION

14 6.1 PREMERA shall retain and maintain the reports, records, information and other
15 documentation required by this Consent Judgment for a period of no less than three (3) years
16 after the document is finalized, last edited, or last used.

17 VII. PAYMENT TO THE STATES

18 7.1 No later than thirty (30) days after the EFFECTIVE DATE, PREMERA shall pay
19 a total of Ten Million Dollars (\$10,000,000.00) to the Attorneys General. This amount is to be
20 divided and paid by PREMERA directly to the Montana Attorney General in an amount to be
21 designated by and in the sole discretion of the MULTISTATE EXECUTIVE COMMITTEE. The
22 distribution to Montana shall be \$124,356.22. Said payment shall be used by the Montana
23 Attorney General for additional consumer relief; attorneys' fees and other costs of investigation
24 and litigation; or to be placed in, or applied to, consumer protection enforcement funds, including
25 future consumer protection enforcement, consumer education, litigation or local consumer aid
26 fund or revolving fund, used to defray the costs of the inquiry leading hereto, or for any lawful

1 | purpose, at the sole discretion of each State Attorney General.

2 | **VIII. RELEASE**

3 | 8.1 Following full payment of the amount due under this Consent Judgment, the State
4 | of Montana shall release and discharge PREMERA from all civil claims that the Attorney
5 | General has or could have brought under the Consumer Protection Act, Mont. Code Ann. § 30-
6 | 14-101 *et seq.* and the Montana Impediment of Identity Theft Act, Mont. Code Ann. § 30-14-
7 | 1701 *et seq.*, the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-
8 | 191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and
9 | Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the Department of Health and
10 | Human Services (“HHS”) Regulations, 45 C.F.R. §§ 160 *et seq.* arising out of PREMERA’s
11 | conduct and the Attorney General’s investigation of the data security incident first publicly
12 | announced March 17, 2015. Nothing contained in this paragraph shall be construed to limit the
13 | ability of the Montana Attorney General to enforce the obligations that PREMERA has under
14 | this Consent Judgment. Further, nothing in this Consent Judgment shall be construed to create,
15 | waive, or limit any private right of action or any action brought by any state agency other than
16 | the Attorney General.

17 | 8.2 The obligations and other provisions of this Consent Judgment set forth in
18 | Sections 4.5 and 4.7 shall expire at the conclusion of the five (5) year period after the
19 | EFFECTIVE DATE of this Consent Judgment, unless they have expired at an earlier date
20 | pursuant to their specific terms. The obligations and other provisions of this Consent Judgment
21 | set forth in Paragraphs 4.3, 4.4, and 4.6 shall expire at the conclusion of the ten (10) year period
22 | after the EFFECTIVE DATE of this Consent Judgment, unless they have expired at an earlier
23 | date pursuant to their specific terms. Other sections and paragraph with specified time periods
24 | shall expire as detailed in those sections and paragraphs. Nothing in this paragraph should be
25 | construed or applied to excuse PREMERA from its obligation to comply with all applicable state
26 | and federal laws, regulations and rules.

1 response from PREMERA described in Paragraph 9.1, if the Attorney General determines that
2 an enforcement action is in the public interest.

3 X. ENFORCEMENT

4 10.1 Violation of any of the injunctions contained in this Consent Judgment, as
5 determined by the Court, shall constitute a violation of an injunction for which civil penalties
6 may be sought by the Attorney General pursuant to Mont. Code Ann. § 30-14-142(1).

7 10.2 This Consent Judgment is entered pursuant to the Montana Consumer Protection
8 Act, Mont. Code Ann. § 30-14-101 *et seq.* Jurisdiction is retained for the purpose of enabling
9 any party to this Consent Judgment with or without the prior consent of the other party to apply
10 to the Court at any time for enforcement of compliance with this Consent Judgment, to punish
11 violations thereof, or to modify or clarify this Consent Judgment.

12 10.3 Under no circumstances shall this Consent Judgment or the name of the State of
13 Montana, the Office of the Attorney General, Consumer Protection Division, or any of their
14 employees or representatives be used by PREMERA in connection with any selling, advertising,
15 or promotion of products or services, or as an endorsement or approval of PREMERA's acts,
16 practices or conduct of business.

17 10.4 Nothing in this Consent Judgment shall be construed to limit the authority or
18 ability of the Montana Attorney General to protect the interests of Montana or the people of
19 Montana. This Consent Judgment shall not bar the Montana Attorney General or any other
20 governmental entity from enforcing laws, regulations, or rules against PREMERA for conduct
21 subsequent to or otherwise not covered by this Consent Judgment. Further, nothing in this
22 Consent Judgment shall be construed to limit the ability of the Montana Attorney General to
23 enforce the obligations that PREMERA has under this Consent Judgment.

24 10.5 Nothing in this Consent Judgment shall be construed as relieving PREMERA of
25 the obligation to comply with all state and federal laws, regulations, and rules, nor shall any of
26 the provisions of this Consent Judgment be deemed to be permission to engage in any acts or

1 practices prohibited by such laws, regulations, and rules.

2 10.6 PREMERA shall deliver a copy of this Consent Judgment to, and otherwise fully
3 apprise, its Chief Executive Officer, Chief Information Officer, Chief Information Security
4 Officer, Compliance Officer, DESIGNATED PRIVACY OFFICIAL, DESIGNATED
5 SECURITY OFFICIAL, Chief Legal Officer, and its Board of Directors within (30) days of the
6 EFFECTIVE DATE. To the extent PREMERA hires or replaces any of the above listed officers,
7 counsel or Directors, PREMERA shall deliver a copy of this Consent Judgment to their
8 replacements within thirty (30) days from the date on which such person assumes his/her position
9 with PREMERA.

10 10.7 No court costs, if any, shall be taxed upon the Attorney General. To the extent
11 there are any court costs associated with the filing of this Consent Judgment, PREMERA shall
12 pay all such court costs.

13 10.8 PREMERA shall not participate in any activity or form a separate entity or
14 corporation for the purpose of engaging in acts or practices in whole or in part that are prohibited
15 by this Consent Judgment or for any other purpose that would otherwise circumvent any term of
16 this Consent Judgment. PREMERA shall not knowingly cause, permit, or encourage any other
17 persons or entities acting on its behalf, to engage in practices prohibited by this Consent
18 Judgment.

19 10.9 PREMERA agrees that this Consent Judgment does not entitle it to seek or to
20 obtain attorneys' fees as a prevailing party under any statute, regulation, or rule, and PREMERA
21 further waives any right to attorneys' fees that may arise under such statute, regulation, or rule.

22 10.10 This Consent Judgment shall not be construed to waive any claims of sovereign
23 immunity Montana may have in any action or proceeding.

24 10.11 If any portion of this Consent Judgment is held invalid by operation of law, the
25 remaining terms of this Consent Judgment shall not be affected and shall remain in full force and
26 effect.

1 10.12 Whenever PREMERA shall provide reports to the Washington Attorney General
2 under Section V of this Consent Judgment, those requirements shall be satisfied by sending the
3 report to: ATTN: Tiffany Lee and Andrea Alegrett, Assistant Attorney General, Consumer
4 Protection Division, Office of the Attorney General, 800 Fifth Avenue #2000, Seattle, WA
5 98104.

6 10.13 Any notice or report provided by the Attorney General to PREMERA under
7 Section IX of this Consent Judgment shall be satisfied by sending notice to: Chief Legal Officer,
8 Premera Blue Cross, 7001 220th St., SW, MS 316, Mountlake Terrace, WA 98043.

9 10.14 All documents to be provided under this Consent Judgment shall be sent by United
10 States mail, certified mail return receipt requested, or other nationally recognized courier service
11 that provides for tracking services and identification of the person signing for the notice or
12 document, and shall have been deemed to be sent upon mailing. The parties may update their
13 designee or address by sending written notice to the other party informing it of the change.

14 10.15 Jurisdiction is retained by the Court for the purpose of enabling any party to the
15 Consent Judgment to apply to the Court at any time for such further orders and directions as may
16 be necessary or appropriate for the construction or the carrying out of this Consent Judgment, for
17 the modification of any of the injunctive provisions hereof, for enforcement of compliance
18 herewith, and for the punishment of violations hereof, if any.

19 10.16 The clerk is ordered to enter this Consent Judgment forthwith.

20 **XI. DISMISSAL AND WAIVER OF CLAIMS**

21 11.1 Upon entry of this Consent Judgment, all claims in this matter, not otherwise
22 addressed by this Consent Judgment are dismissed.

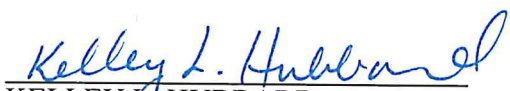
23
24 Dated this _____ day of _____, 2019.

25
26 _____
JUDGE

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

Approved for entry and presented by:

TIMOTHY C. FOX
Montana Attorney General



KELLEY L. HUBBARD
Assistant Attorney General
Office of Consumer Protection
P.O. Box 200151
555 Fuller Ave.
Helena, MT 59620-0151
(406) 444-2026
khubbard@mt.gov

Approved for Entry, Notice of Presentation
Waived:



NATHAN A. SCHACHT
Baker & Hostetler LLP
1801 California Street, Suite 4400
Denver, CO 80202
(303) 764-4029
nschacht@bakerlaw.com

THEODORE J. KOBUS III
Baker & Hostetler LLP
45 Rockefeller Plaza
New York, NY 10111
(212) 271-1504
Email: tkobus@bakerlaw.com

PATRICK H. HAGGERTY
Baker & Hostetler LLP
312 Walnut St., Suite 3200
Cincinnati, OH 45202
(513) 929-3412
Email: phaggerty@bakerlaw.com