

1 **CONS**

2 AARON D. FORD

Attorney General

3 ERNEST D. FIGUEROA

Consumer Advocate

4 LUCAS J. TUCKER (Bar No. 010252)

Senior Deputy Attorney General

5 LAURA M. TUCKER (Bar No. 013268)

6 Senior Deputy Attorney General

7 State of Nevada, Office of the Attorney General

Bureau of Consumer Protection

8 8945 W. Russell Road, #204

Las Vegas, Nevada 89148

9 702-486-3256 ph

10 ltucker@ag.nv.gov

lmtucker@ag.nv.gov

11 Attorneys for Plaintiff, State of Nevada

12 **DISTRICT COURT**
13 **CLARK COUNTY, NEVADA**

14 STATE OF NEVADA,)

15 Plaintiff,)

16 vs.)

17 **PREMERA BLUE CROSS,**)

18 Defendants.)

CASE NO.: A-19-798251-B

DEPT NO.: 11

BUSINESS COURT REQUESTED

ARBITRATION EXEMPTION—

Action in Equity

19 _____)
20 **FINAL JUDGMENT AND CONSENT DECREE**

21 Plaintiff, STATE OF NEVADA, by AARON D. FORD, Attorney General, LUCAS
22 J. TUCKER, Senior Deputy Attorney General, and LAURA M. TUCKER, Senior Deputy
23 Attorney General, has filed a Complaint for a permanent injunction and other relief in
24 this matter pursuant to the Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. §§
25 598.0903, et seq. (“the Nevada DTPA”), the Nevada Security of Personal Information
26 Act., Nev. Rev. Stat. §§ 603A.010, et seq., and the Health Insurance Portability and
27 Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the
28 Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5,

1 123 Stat. 226, as well as the Department of Health and Human Services (“HHS”)
2 Regulations, 45 C.F.R. §§ 160 *et seq.* (“HIPAA”). The Complaint alleges that Defendant
3 Premera Blue Cross committed violations of the Nevada DTPA, the Nevada Security of
4 Personal Information Act and HIPAA.

5 Plaintiff and Premera Blue Cross have agreed to the Court’s entry of this Final
6 Judgment and Consent Decree (“Consent Decree”) without the taking of proof, without
7 trial or adjudication of any issue of fact or law, and without admission of any facts
8 alleged or liability of any kind.

9 **I. PREAMBLE**

10 1.1 The Attorney General of Nevada conducted an investigation and commenced
11 this action pursuant to HIPAA and the Consumer Protection Laws (as defined in Section
12 3.2).

13 1.2 Plaintiff appears by and through its attorneys AARON D. FORD, Attorney
14 General, ERNEST D. FIGUEROA, Consumer Advocate, LUCAS J. TUCKER, Senior
15 Deputy Attorney General and LAURA M. TUCKER, Senior Deputy Attorney General;
16 and Premera Blue Cross as defined in Paragraph 3.14 (“PREMERA”), appears by and
17 through their attorneys, Matthew L. Durham, Theodore Kobus, III, and Patrick H.
18 Haggerty.

19 1.3 Plaintiff alleges that on March 17, 2015, Premera publicly announced a data
20 security incident involving its computer network system which resulted in the unauthorized
21 disclosure of certain consumers’ personal information and protected health information.

22 1.4 Plaintiff and PREMERA agree that this Consent Decree does not constitute
23 evidence or an admission regarding the existence or non-existence of any issue, fact, or
24 violation of any law alleged by Plaintiff.

25 1.5 PREMERA recognizes and states that this Consent Decree is entered into
26 voluntarily and that no promises or threats have been made by the Attorney General’s
27 Office or any member, officer, agent or representative thereof to induce it to enter into this
28 Consent Decree, except as provided herein.

1 1.6 PREMERA waives any right it may have to appeal from this Consent Decree.

2 1.7 PREMERA further agrees that it will not oppose the entry of this Consent
3 Decree on the grounds the Consent Decree fails to comply with Rule 65(d) of the Rules of
4 Civil Procedure, and hereby waives any objections based thereon.

5 1.8 PREMERA further agrees that this Court shall retain jurisdiction of this
6 action for the purpose of implementing and enforcing the terms and conditions of the
7 Consent Decree and for all other purposes.

8 The Court finding no just reason for delay;

9 NOW, THEREFORE, it is hereby ORDERED, ADJUDGED, AND DECREED
10 as follows:

11 **II. PARTIES AND JURISDICTION**

12 2.1 The State of Nevada is the Plaintiff in this case.

13 2.2 Premera Blue Cross is a Washington non-profit corporation with its
14 principal office located at 7001 220th St. SW, Building 1, Mountlake Terrace, Washington
15 98043.

16 2.3 This Court has jurisdiction of the subject matter of this action pursuant to
17 the Nevada DTPA, specifically Nev. Rev. Stat. §§ 598.0963 and 598.0999.

18 2.4 The exercise of personal jurisdiction over PREMERA is consistent with due
19 process.

20 2.5 Venue is proper in this Court pursuant to Nev. Rev. Stat. § 598.0989(3), and
21 PREMERA consents to the filing of this Consent Decree in a county where the Attorney
22 General maintains an office for the limited purpose of resolving the claims at issue.

23 2.6 For the purposes of this Consent Decree, or any action to enforce this Decree,
24 PREMERA consents to the Court's jurisdiction over this Decree and consents to venue in
25 this judicial district.

26 2.7 This Consent Decree is entered pursuant to and subject to the Nevada
27 DTPA.

28 ///

1 **III. DEFINITIONS**

2 3.1 "COVERED SYSTEMS" shall mean all components, including but not
3 limited to, assets, technology, and software, within the PREMERA NETWORK that are
4 used to collect, process, transmit, and/or store PERSONAL INFORMATION or
5 PROTECTED HEALTH INFORMATION.

6 3.2 "CONSUMER PROTECTION LAWS" shall collectively mean the Nevada
7 DTPA and Nev. Rev. Stat. §§ 603A.010, et seq.

8 3.3 "DESIGNATED PRIVACY OFFICIAL" shall mean the individual designated
9 by PREMERA who is responsible for the development and implementation of the policies
10 and procedures as required by 45 C.F.R. § 164.530(a).

11 3.4 "DESIGNATED SECURITY OFFICIAL" shall mean the individual
12 designated by PREMERA who is responsible for the development and implementation of
13 the policies and procedures as required by 45 C.F.R. § 164.308(a)(2).

14 3.5 "EFFECTIVE DATE" shall be July 11, 2019.

15 3.6 "ENCRYPTED" shall refer to the existing industry standard to encode or
16 obscure data at rest or in transit. As of the EFFECTIVE DATE, the existing industry
17 standard shall be AES 256-bit encryption or Transport Layer Security (TLS) 1.2, or their
18 equivalents.

19 3.7 "GLBA" shall mean the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338.

20 3.8 "HIPAA" shall mean the Health Insurance Portability and Accountability
21 Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information
22 Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as
23 well as the Department of Health and Human Services ("HHS") Regulations, 45 C.F.R. §§
24 160 *et seq.*

25 3.9 "HIPAA SECURITY RULE" shall mean the Security Standards for the
26 Protection of Electronic Protected Health Information, 45 C.F.R. Part 160 and Part 164,
27 Subparts A and E.

28 ///

1 3.10 “HIPAA PRIVACY RULE” shall mean the Standards for Privacy of
2 Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subparts
3 A and E.

4 3.11 “MULTI-FACTOR AUTHENTICATION” means authentication through
5 verification of at least two of the following authentication factors: (i) knowledge factors,
6 such as a password; or (ii) possession factors, such a token or text message on a mobile
7 phone; or (iii) inherence factors, such as a biometric characteristic.

8 3.12 “MULTISTATE EXECUTIVE COMMITTEE” shall mean the Attorneys
9 General of the States of Washington, Oregon, and California.

10 3.13 “PERSONAL INFORMATION” shall have the same meaning prescribed in
11 Nev. Rev. Stat. § 603A.040.

12 3.14 “PREMERA” shall mean Premera Blue Cross, its parent and its directly or
13 indirectly wholly-owned or controlled affiliates, subsidiaries and divisions, successors and
14 assigns.¹

15 3.15 “PREMERA NETWORK” shall mean all networking equipment, databases
16 or data stores, applications, servers, and endpoints that are capable of using and sharing
17 software, data, and hardware resources, and that are owned, operated, and/or controlled
18 by PREMERA.

19 3.16 “PROTECTED HEALTH INFORMATION” shall mean “individually
20 identifiable health information” as defined by the Health Insurance Portability and
21 Accountability Act (HIPAA), as amended by the Health Information Technology and
22 Clinical Act (HITECH) and 45 C.F.R. § 160.103.

23 3.17 “SECURITY BREACH NOTIFICATION ACT” shall mean Nev. Rev. Stat. §
24 603A.220.

25 ///

26 ///

27 _____
28 ¹ For purposes of this definition, “control” means the possession, directly or indirectly, of the power to direct
or cause the direction of the management and policies of an entity through majority ownership or voting
power.

1 c. PREMERA shall continue to employ an executive or officer who shall be
2 responsible for implementing, maintaining, and monitoring the Compliance Program (for
3 ease, hereinafter referred to as the "Compliance Officer"). The Compliance Officer shall
4 have the appropriate background or experience in compliance, including appropriate
5 training in compliance with HIPAA, GLBA, and applicable state laws relating to privacy or
6 data security.

7 d. The Compliance Officer shall continue to oversee PREMERA's Compliance
8 Program and shall function as an independent and objective body that reviews and
9 evaluates compliance within PREMERA. The Compliance Officer shall develop a process
10 for evaluating compliance risks and determining priorities, reviewing compliance plans, and
11 ensuring that follow-up to compliance issues identified occurs within a reasonable
12 timeframe and that processes are in place for determining and implementing appropriate
13 disciplinary and corrective actions when violations arise.

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

17 f. PREMERA shall ensure that its Compliance Program continues to receive the
18 resources and support necessary to ensure that the Compliance Program functions as
19 required and intended by this Consent Decree.

20 g. PREMERA may satisfy the implementation and maintenance of the
21 Compliance Program and the safeguards required by this Consent Decree through review,
22 maintenance, and, if necessary, updating of an existing compliance program or existing
23 safeguards, provided that such existing compliance program and existing safeguards meet
24 the requirements set forth in this Consent Decree.

25 **4.5 INFORMATION SECURITY PROGRAM:**

26 a. PREMERA may satisfy the implementation and maintenance of the
27 Information Security Program and the safeguards and controls required by this Consent
28 Decree through review, maintenance, and, if necessary, updating of an existing information

1 security program or existing controls and safeguards, provided that such existing
2 compliance program and existing safeguards and controls meet the requirements set forth
3 in this Consent Decree.

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

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

- 11 (i). The size and complexity of PREMERA’s operations;
- 12 (ii). The nature and scope of PREMERA’s activities; and
- 13 (iii). The sensitivity of the PERSONAL INFORMATION or PROTECTED
14 HEALTH INFORMATION that PREMERA collects, stores, transmits, and/or maintains.

15 d. As part of its Information Security Program, PREMERA will not trust traffic
16 on the PREMERA NETWORK. In order to trust the traffic, PREMERA shall:

- 17 (i). Regularly monitor, log, and inspect all network traffic, including log-in
18 attempts, through the implementation of hardware, software, or procedural mechanisms
19 that record and examine such activity;
- 20 (ii). Ensure that every device, user, and network flow is authorized and
21 authenticated; and
- 22 (iii). Only allow access by users of the PREMERA NETWORK to the
23 minimum extent necessary and require appropriate authorization and authentication prior
24 to allowing any such access.

25 e. The Information Security Program shall be designed to:

- 26 (i). Protect the security, integrity, availability, and confidentiality of
27 PERSONAL INFORMATION and PROTECTED HEALTH INFORMATION;

28 ///

1 (ii). Protect against any threats to the security, integrity, availability, or
2 confidentiality of PERSONAL INFORMATION and PROTECTED HEALTH
3 INFORMATION;

4 (iii). Protect against unauthorized access to or use of PERSONAL
5 INFORMATION and PROTECTED HEALTH INFORMATION and minimize the likelihood
6 of harm to any consumer;

7 (iv). Define and periodically reevaluate a schedule for retention of
8 PERSONAL INFORMATION and PROTECTED HEALTH INFORMATION and for its
9 destruction when such information is no longer needed for business purposes;

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

14 (vi). Assess the number of users on PREMERA's applications and retire
15 any application with no active users and that no longer has a business purpose;

16 (vii). Restrict the ability of PREMERA employees and vendors to access the
17 PREMERA NETWORK via personal devices (e.g., smartphones, tablets, personal laptops)
18 and permit such access only based on a business need. If required, the access shall be
19 restricted to only the data, systems, and other network resources required for the vendor's
20 or employee's job. Any access to the PREMERA NETWORK via a personal device shall be
21 reviewed on a regular basis to determine if the vendor's or employee's job function requires
22 this access. Furthermore, this access shall be provided via a secured connection to the
23 PREMERA NETWORK via VPN and MULTI-FACTOR AUTHENTICATION or other
24 greater security safeguards; and

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

1 f. PREMERA may satisfy the implementation and maintenance of the
2 Information Security Program and the safeguards required by this Consent Decree
3 through review, maintenance, and, if necessary, updating, of an existing information
4 security program or existing safeguards, provided that such existing information security
5 program and existing safeguards meet the requirements set forth in this Consent Decree.

6 g. PREMERA shall employ an executive or officer who shall be responsible for
7 implementing, maintaining, and monitoring the Information Security Program (for ease,
8 hereinafter referred to as the "Chief Information Security Officer"). The Chief
9 Information Security Officer shall have the appropriate background or experience in
10 information security and HIPAA compliance. PREMERA shall ensure that the Chief
11 Information Security Officer is a separate position from the Chief Information Officer and
12 that the Chief Information Security Officer serve as PREMERA's DESIGNATED
13 SECURITY OFFICIAL. The Chief Information Security Officer shall have direct access to
14 the Chief Executive Officer and the Audit and Compliance Committee of the Board of
15 Directors.

16 h. PREMERA shall ensure that the role of the Chief Information Security
17 Officer includes directly advising PREMERA's Board of Directors, Chief Executive
18 Officer, and Chief Information Officer on the management of PREMERA's security
19 posture, the security risks faced by PREMERA, the security implications of PREMERA's
20 decisions, and the adequacy of PREMERA's Information Security Program. The Chief
21 Information Security Officer shall meet with, and provide an oral or written update to: (1)
22 the Board of Directors on at least an annual basis; (2) the Chief Executive Officer at least
23 every two months; (3) the Chief Information Officer on at least a twice per month basis;
24 and (4) the DESIGNATED PRIVACY OFFICIAL at least every two months. The Chief
25 Information Security Officer shall inform the Chief Executive Officer, the Chief
26 Information Officer, and the DESIGNATED PRIVACY OFFICIAL of any material
27 unauthorized intrusion to the PREMERA NETWORK within forty-eight (48) hours of
28 discovery of the intrusion. A material unauthorized intrusion is any intrusion to the

1 PREMERA NETWORK that affects or may affect any PROTECTED HEALTH
2 INFORMATION or PERSONAL INFORMATION.

3 i. PREMERA shall ensure that the Chief Information Security Officer and
4 Information Security Program receive the resources and support necessary to ensure that
5 the Information Security Program functions as intended by this Consent Decree.

6 j. PREMERA shall ensure that employees who are responsible for
7 implementing, maintaining, or monitoring the Information Security Program, including
8 but not limited to the Chief Information Officer and Chief Information Security Officer,
9 have sufficient knowledge of the requirements of the Consent Decree.

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

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

20 m. PREMERA shall provide its DESIGNATED SECURITY OFFICIAL with
21 appropriate training to ensure the official is able to implement the requirements of and
22 ensure compliance with the HIPAA SECURITY RULE.

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

28 (i). Preparation;

- (ii). Investigation, Detection and Analysis;
- (iii). Containment;
- (iv). Notification and Coordination with Law Enforcement;
- (v). Eradication;
- (vi). Recovery;
- (vii). Consumer and Regulator Notification and Remediation; and
- (viii). Post-Incident Analysis (Lessons Learned).

o. For each SECURITY INCIDENT, PREMERA shall create a report that includes a description of the SECURITY INCIDENT and PREMERA's response to that SECURITY INCIDENT ("Security Incident Report"). The Security Incident Report shall be made available for the Third-Party Assessment as described in Paragraph 5.1.

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

4.6 PERSONAL INFORMATION AND PROTECTED HEALTH INFORMATION SAFEGUARDS AND CONTROLS:

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

b. PREMERA shall implement, maintain, regularly review and revise, and comply with policies and procedures to ENCRYPT PERSONAL INFORMATION and

1 PROTECTED HEALTH INFORMATION, whether the information is transmitted
2 electronically over a network or is stored on any media, whether it be static, removable,
3 or otherwise.

4 4.7 SPECIFIC TECHNICAL SAFEGUARDS AND CONTROLS:

5 a. Asset Inventory and Managing Critical Assets:

6 (i). PREMERA shall, within one hundred and eighty (180) days of the
7 EFFECTIVE DATE, implement and maintain a configuration management database
8 that contains an asset inventory for all known Critical Assets that identifies: (a) the name
9 of the asset; (b) the version of the asset; (c) the owner of the asset; (d) the asset's location
10 within the PREMERA NETWORK; (e) whether the asset is a Critical Asset; and (f) the
11 date that each security update or patch was applied. PREMERA shall apply the highest
12 rating it uses for any asset that it uses to collect, store, transmit, or use PERSONAL
13 INFORMATION or PROTECTED HEALTH INFORMATION ("Critical Assets").

14 (ii). PREMERA shall, within one year of the EFFECTIVE DATE,
15 implement and maintain an asset inventory for all assets that identifies: (a) the name of
16 the asset; (b) the version of the asset; (c) the owner of the asset; (d) the asset's location
17 within the PREMERA NETWORK; (e) whether the asset is a Critical Asset; and (f) the
18 date that each security update or patch was applied.

19 b. Mapping and Encryption of Sensitive Data:

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

26 (ii). PREMERA shall ensure that electronic PERSONAL INFORMATION or
27 PROTECTED HEALTH INFORMATION that is stored at rest or is in transmission is
28 ENCRYPTED except where PREMERA determines that ENCRYPTION is not reasonable

1 and appropriate, and it documents the rationale for this decision.

2 c. Segmentation: PREMERA shall implement and maintain segmentation
3 protocols and related policies that are reasonably designed to properly segment the
4 PREMERA NETWORK, which shall, at a minimum, ensure system functionality and
5 performance to meet business needs while also mitigating exposure to the enterprise
6 network in the event of an attack or malicious intruder access. Additionally, PREMERA
7 shall regularly evaluate, and as appropriate, restrict and disable any unnecessary ports of
8 service on the PREMERA NETWORK.

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

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

1 (i). The risk assessment shall include an accurate and thorough assessment
2 of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of
3 electronic protected health information held as required by HIPAA SECURITY RULE, 45
4 C.F.R. § 164.308(a)(1)(ii)(A).

5 (ii). PREMERA shall implement and maintain a corresponding risk-
6 assessment program designed to identify and assess risks to the PREMERA NETWORK. In
7 cases where PREMERA deems quantitative risk to be acceptable, PREMERA shall generate
8 and retain a report demonstrating how such risks are to be managed in consideration of the
9 risk to PERSONAL INFORMATION and PROTECTED HEALTH INFORMATION, and
10 the cost or difficulty in implementing effective countermeasures. All reports shall be
11 maintained by the Chief Information Security Officer and be available for inspection by its
12 DESIGNATED PRIVACY OFFICIAL and the Third-Party Assessor described in Paragraph
13 5.1 of this Consent Decree.

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

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

25 (i). PREMERA shall, within nine (9) months of the EFFECTIVE DATE,
26 implement and maintain appropriate controls to manage access to, and use of, all
27 administrator, service, and vendor accounts with access to PERSONAL INFORMATION or
28 PROTECTED HEALTH INFORMATION. Such controls shall include, without limitation,

1 (1) strong passwords, (2) password confidentiality policies, (3) password-rotation policies, (4)
2 MULTI-FACTOR AUTHENTICATION or any other equal or greater authentication
3 protocol for identity management, and (5) appropriate safeguards for administrative level
4 passwords.

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

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

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

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

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

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

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

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

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

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

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

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

28 ///

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
3 updated and maintained to ensure that all COVERED SYSTEMS are adequately logged
4 and monitored.

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

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

15 **V. ASSESSMENT AND REPORTING REQUIREMENTS TO THE**
16 **ATTORNEY GENERAL**

17 5.1 Information Security Assessment:

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

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

26 (ii). Explain the extent to which such safeguards are appropriate in light of
27 PREMERA's size and complexity, the nature and scope of PREMERA's activities, and the
28 sensitivity of the PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION

1 maintained by PREMERA;

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

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

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

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

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

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

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

27 ///

28 ///

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

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

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

14 a. The Compliance Program Assessor shall use procedures and standards
15 generally 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
19 employees 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
23 Mitigation Plan, as required by 45 C.F.R. § 164.308(a)(1)(ii)(A) and relevant guidelines
24 provided by the Office for Civil Rights.

25 c. The findings of the Compliance Program Assessment shall be documented in
26 a report (the "Compliance Program Assessor's Report"). PREMERA shall provide a copy
27 of the Compliance Program Assessor's Report to the Washington Attorney General's
28 Office within thirty (30) days of the completion of the Compliance Program Assessment.

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

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

9 5.3 PREMERA will make reasonable good faith efforts to address any concerns
10 and implement recommendations made by the Third Party Assessor or the Compliance
11 Assessor.

12 **VI. DOCUMENT RETENTION**

13 6.1 PREMERA shall retain and maintain the reports, records, information and
14 other documentation required by this Consent Decree for a period of no less than three (3)
15 years after the document is finalized, last edited, or last used.

16 **VII. PAYMENT TO THE STATES**

17 7.1 No later than thirty (30) days after the EFFECTIVE DATE, PREMERA
18 shall pay a total of Ten Million Dollars (\$10,000,000.00) to the Attorneys General. This
19 amount is to be divided and paid by PREMERA directly to the Nevada Attorney General
20 in an amount to be designated by and in the sole discretion of the MULTISTATE
21 EXECUTIVE COMMITTEE. The distribution to Nevada shall be Seventy-Nine
22 Thousand One Hundred Twenty Dollars and Two Cents (\$79,120.02). Said payment may
23 be used by the Nevada Attorney General for purposes that may include, but are not
24 limited to, attorneys' fees and other costs of investigation and litigation, or to be placed
25 in, or applied to, consumer protection enforcement funds, including future consumer

26 ///

27 ///

28 ///

1 protection or privacy law enforcement, consumer education, litigation or local consumer
2 aid fund or revolving fund, used to defray the costs of the inquiry leading hereto, or for
3 any other uses permitted by state law, at the sole discretion of the Nevada Attorney
4 General.

5 **VIII. RELEASE**

6 8.1 Following full payment of the amount due under this Consent Decree, the
7 Attorney General of Nevada shall release and discharge PREMERA from all civil claims
8 that the Attorney General has or could have brought under the CONSUMER
9 PROTECTION LAWS, SECURITY BREACH NOTIFICATION ACT, and HIPAA arising
10 out of PREMERA's conduct and the Attorney General's investigation of the data security
11 incident first publicly announced March 17, 2015. Nothing contained in this paragraph
12 shall be construed to limit the ability of the Nevada Attorney General to enforce the
13 obligations that PREMERA has under this Consent Decree. Further, nothing in this
14 Consent Decree shall be construed to create, waive, or limit any private right of action or
15 any action brought by any state agency other than the Attorney General.

16 8.2 The obligations and other provisions of this Consent Decree set forth in
17 Sections 4.5 and 4.7 shall expire at the conclusion of the five (5) year period after the
18 EFFECTIVE DATE, unless they have expired at an earlier date pursuant to their specific
19 terms. The obligations and other provisions of this Consent Decree set forth in
20 Paragraphs 4.3, 4.4, and 4.6 shall expire at the conclusion of the ten (10) year period after
21 the EFFECTIVE DATE, unless they have expired at an earlier date pursuant to their
22 specific terms. Other sections and paragraph with specified time periods shall expire as
23 detailed in those sections and paragraphs. Nothing in this paragraph should be
24 construed or applied to excuse PREMERA from its obligation to comply with all
25 applicable state and federal laws, regulations and rules.

26 8.3 Notwithstanding any term of this Consent Decree, any and all of the
27 following forms of liability are specifically reserved and excluded from the release as to
28 any entity or person, including PREMERA:

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

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

- 6 (i). State or federal antitrust violations;
- 7 (ii). State or federal securities violations; or
- 8 (iii). State or federal tax claims.

9 **IX. MEET AND CONFER**

10 9.1 If any Attorney General determines that PREMERA has failed to comply
11 with any of Sections IV and V of this Consent Decree, and if in the Attorney General's sole
12 discretion the failure to comply with this Consent Decree does not threaten the health or
13 safety of the citizens of the Attorney General's State and/or does not create an emergency
14 requiring immediate action, the Attorney General will notify PREMERA in writing of
15 such failure to comply and PREMERA shall have thirty (30) days from receipt of such
16 written notice to provide a good faith written response to that Attorney General,
17 including either a statement that PREMERA believes it is in full compliance or otherwise
18 a statement explaining how the violation occurred, how it has been addressed or when it
19 will be addressed, and what PREMERA will do to make sure the violation does not
20 happen again. The Attorney General may agree to provide PREMERA more than thirty
21 (30) days to respond.

22 9.2 Nothing herein shall be construed to exonerate any failure to comply with
23 any provision of this Consent Decree, or limit the right and authority of an Attorney
24 General to initiate a proceeding for any failure to comply with this Consent Decree after
25 receiving the response from PREMERA described in Paragraph 9.1, if the Attorney
26 General determines that an enforcement action is in the public interest.

27 ///

28 ///

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
27
28

X. ENFORCEMENT

10.1 Violation of any of the injunctions contained in this Consent Decree, as determined by the Court, shall constitute a violation of an injunction for which civil penalties may be sought by the Attorney General pursuant to Nev. Rev. Stat. § 598.0999.

10.2 This Consent Decree is entered pursuant to the Nevada DTPA. Jurisdiction is retained for the purpose of enabling any party to this Consent Decree with or without the prior consent of the other party to apply to the Court at any time for enforcement of compliance with this Consent Decree, to punish violations thereof, or to modify or clarify this Consent Decree.

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

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

10.5 Nothing in this Consent Decree shall be construed as relieving PREMERA of the obligation to comply with all state and federal laws, regulations, and rules, nor shall any of the provisions of this Consent Decree be deemed to be permission to engage in any acts or practices prohibited by such laws, regulations, and rules.

10.6 PREMERA shall deliver a copy of this Consent Decree to, and otherwise fully apprise, its Chief Executive Officer, Chief Information Officer, Chief Information Security Officer, Compliance Officer, DESIGNATED PRIVACY OFFICIAL, DESIGNATED

1 SECURITY OFFICIAL, Chief Legal Officer, and its Board of Directors within (30) days of
2 the EFFECTIVE DATE. To the extent PREMERA hires or replaces any of the above
3 listed officers, counsel or Directors, PREMERA shall deliver a copy of this Consent Decree
4 to their replacements within thirty (30) days from the date on which such person assumes
5 his/her position with PREMERA.

6 10.7 No court costs, if any, shall be taxed upon the Attorney General. To the
7 extent there are any court costs associated with the filing of this Consent Decree,
8 PREMERA shall pay all such court costs.

9 10.8 PREMERA shall not participate in any activity or form a separate entity or
10 corporation for the purpose of engaging in acts or practices in whole or in part that are
11 prohibited by this Consent Decree or for any other purpose that would otherwise
12 circumvent any term of this Consent Decree. PREMERA shall not knowingly cause,
13 permit, or encourage any other persons or entities acting on its behalf, to engage in
14 practices prohibited by this Consent Decree.

15 10.9 PREMERA agrees that this Consent Decree does not entitle it to seek or to
16 obtain attorneys' fees as a prevailing party under any statute, regulation, or rule, and
17 PREMERA further waives any right to attorneys' fees that may arise under such statute,
18 regulation, or rule.

19 10.10 This Consent Decree shall not be construed to waive any claims of sovereign
20 immunity Nevada may have in any action or proceeding.

21 10.11 If any portion of this Consent Decree is held invalid by operation of law, the
22 remaining terms of this Consent Decree shall not be affected and shall remain in full force
23 and effect.

24 10.12 Whenever PREMERA shall provide reports to the Washington Attorney
25 General under Section V of this Consent Decree, those requirements shall be satisfied by
26 sending the report to: ATTN: Tiffany Lee and Andrea Alegrett, Assistant Attorney
27 General, Consumer Protection Division, Office of the Attorney General, 800 Fifth Avenue
28 #2000, Seattle, WA 98104.

1 10.13 Any notice or report provided by the Attorney General to PREMERA under
2 Section IX of this Consent Decree shall be satisfied by sending notice to: Chief Legal
3 Officer, Premera Blue Cross, 7001 220th St., SW, MS 316, Mountlake Terrace, WA 98043.

4 10.14 All documents to be provided under this Consent Decree shall be sent by
5 United States mail, certified mail return receipt requested, or other nationally recognized
6 courier service that provides for tracking services and identification of the person signing
7 for the notice or document, and shall have been deemed to be sent upon mailing. The
8 parties may update their designee or address by sending written notice to the other party
9 informing it of the change.

10 10.15 Jurisdiction is retained by the Court for the purpose of enabling any party to
11 the Consent Decree to apply to the Court at any time for such further orders and
12 directions as may be necessary or appropriate for the construction or the carrying out of
13 this Consent Decree, for the modification of any of the injunctive provisions hereof, for
14 enforcement of compliance herewith, and for the punishment of violations hereof, if any.

15 10.16 PREMERA represents that it has reviewed this Consent Decree, that its
16 legal counsel has full authority to sign this Consent Decree on its behalf, and that
17 signature by its counsel shall be bind PREMERA to its obligations under this Consent
18 Decree.

19 ///

20 ///

21 ///

22 ///

23 ///

24 ///

25 ///

26 ///

27 ///

28 ///

1 10.17 The clerk is ordered to enter this Consent Decree forthwith.

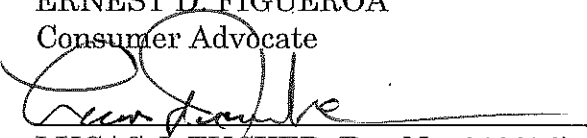
2 **XI. DISMISSAL AND WAIVER OF CLAIMS**

3 11.1 Upon entry of this Consent Decree, all claims in this matter, not otherwise
4 reserved by this Consent Decree are dismissed.

5 Dated this 11th day of July, 2019.

6 SUBMITTED BY:

7
8 AARON D. FORD
Attorney General
9 ERNEST D. FIGUEROA
Consumer Advocate

10 
11 LUCAS J. TUCKER (Bar No. 010252)
12 Senior Deputy Attorney General

13
14 Attorneys for Defendants

15 
16 MATTHEW L. DURHAM (Bar No. 10342)
17 KING DURHAM
18 6385 S. Rainbow Blvd., Suite 220
19 Las Vegas, NV 89118
20 Telephone: (702) 833-1103
21 Email: mdurham@kingdurham.com

22 THEODORE J. KOBUS III
23 Baker & Hostetler LLP
24 45 Rockefeller Plaza
25 New York, NY 10111-0100
26 Telephone: (212) 271-1504
27 Email: tkobus@bakerlaw.com

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