

1 XAVIER BECERRA
Attorney General of California
2 NICKLAS A. AKERS
Senior Assistant Attorney General
3 STACEY D. SCHESSER
Supervising Deputy Attorney General
4 YEN P. NGUYEN (SBN 239095)
Deputy Attorney General
5 455 Golden Gate Avenue, Suite 11000
San Francisco, CA 94102-7004
6 Telephone: (415) 510-3497
Fax: (415) 703-5480
7 E-mail: TiTi.Nguyen@doj.ca.gov

[EXEMPT FROM FILING FEES
PURSUANT TO GOVERNMENT
CODE SECTION 6103]

8 *Attorneys for The People of the State of California*

9 SUPERIOR COURT OF THE STATE OF CALIFORNIA

10 FOR THE COUNTY OF SONOMA

11 UNLIMITED JURISDICTION

13 **THE PEOPLE OF THE STATE OF
14 CALIFORNIA,**

15 Plaintiff,

16 v.

17 **PREMERA BLUE CROSS,**

18 Defendant.

Case No.

**[PROPOSED] FINAL JUDGMENT AND
PERMANENT INJUNCTION**

(CIVIL CODE, §§ 56.101, 56.10(a); BUS &
PROF. CODE, §§ 17200 et seq., 17500 et
seq.)

21 **I. JUDGMENT SUMMARY**

22 1.1 The People of the State of California (hereinafter “Plaintiff”), by and through
23 Xavier Becerra, Attorney General of the State of California, conducted an investigation and
24 commenced this action pursuant to: the Health Insurance Portability and Accountability Act of
25 1996, Pub. L. No. 104-191, 110 Stat. 1938, as amended by the Health Information Technology
26 for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the
27 Department of Health and Human Services (“HHS”) Regulations, 45 C.F.R. §§ 160 et seq.
28 (“HIPAA”); the Unfair Competition Law (UCL), Business and Professions Code section 17200 et

1 seq. (UCL); the False Advertising Law (FAL), Business and Professions Code section 17500 et
2 seq.; and the Confidentiality of Medical Information Act (CMIA), Civil Code section 56 et seq.

3 1.2 Plaintiff appears through its attorney, Xavier Becerra, Attorney General of the
4 State of California, by Yen P. Nguyen, Deputy Attorney General; and Premera Blue Cross as
5 defined in Paragraph 3.15 (“PREMERA”), appears by and through their attorneys, M. Scott
6 Koller, Theodore Kobus, III, and Patrick Haggerty of Baker & Hostetler LLP.

7 1.3 Plaintiff and PREMERA stipulate to the entry of this Final Judgment and
8 Permanent Injunction by the Court without the taking of proof and without trial or adjudication of
9 any fact or law.

10 1.4 Plaintiff alleges that on March 17, 2015, PREMERA publicly announced a data
11 security incident involving its computer network system which resulted in the unauthorized
12 disclosure of certain consumers’ personal information and protected health information.

13 1.5 Plaintiff and PREMERA agree that this Final Judgment and Permanent Injunction
14 does not constitute evidence or an admission regarding the existence or non-existence of any
15 issue, fact, or violation of any law alleged by Plaintiff.

16 1.6 PREMERA recognizes and states that this Final Judgment and Permanent
17 Injunction is entered into voluntarily and that no promises or threats have been made by the
18 Attorney General’s Office or any member, officer, agent or representative thereof to induce it to
19 enter into this Final Judgment and Permanent Injunction, except as provided herein.

20 1.7 PREMERA waives any right they may have to appeal from this Final Judgment
21 and Permanent Injunction.

22 1.8 PREMERA further agrees that it will not oppose the entry of this Final Judgment
23 and Permanent Injunction on the grounds the Final Judgment and Permanent Injunction fails to
24 comply with Rule 65(d) of the Federal Rules of Civil Procedure, and hereby waives any
25 objections based thereon.

26 1.9 PREMERA further agrees that this Court shall retain jurisdiction of this action for
27 the purpose of implementing and enforcing the terms and conditions of the Final Judgment and
28 Permanent Injunction and for all other purposes.

1 The Court finding no just reason for delay;
2 NOW, THEREFORE, it is hereby ORDERED, ADJUDGED, AND DECREED as
3 follows:

4 **II. PARTIES AND JURISDICTION**

5 2.1 The People of the State of California is the Plaintiff in this case.

6 2.2 Premera Blue Cross is the Defendant in this case. Premera Blue Cross is a
7 Washington non-profit corporation with its principal office located at 7001 220th St. SW,
8 Building 1, Mountlake Terrace, Washington 98043.

9 2.3 This Court has jurisdiction of the subject matter of this action, jurisdiction over the
10 parties to this action, and venue is proper in this Court.

11 2.4 Jurisdiction is proper because PREMERA has transacted business within the State
12 of California, and the County of Sonoma, or has engaged in conduct impacting the State of
13 California or its residents at all times relevant to the claims at issue.

14 2.5 This Final Judgment and Permanent Injunction is entered pursuant to and subject
15 to Business and Professions Code section 17200 et seq.

16 **III. DEFINITIONS**

17 3.1 “COVERED SYSTEMS” shall mean all components, including but not limited to,
18 assets, technology, and software, within the PREMERA NETWORK that are used to collect,
19 process, transmit, and/or store PERSONAL INFORMATION, PROTECTED HEALTH
20 INFORMATION, or MEDICAL INFORMATION.

21 3.2 “CONSUMER PROTECTION LAWS” shall mean Business and Professions Code
22 section 17200 et seq. and Civil Code section 56 et seq.

23 3.3 “DESIGNATED PRIVACY OFFICIAL” shall mean the individual designated by
24 PREMERA who is responsible for the development and implementation of the policies and
25 procedures as required by 45 C.F.R. § 164.530(a).

26 3.4 “DESIGNATED SECURITY OFFICIAL” shall mean the individual designated by
27 PREMERA who is responsible for the development and implementation of the policies and
28 procedures as required by 45 C.F.R. § 164.308(a)(2).

1 3.5 “EFFECTIVE DATE” shall be July 11, 2019.

2 3.6 “ENCRYPTED” shall refer to the existing industry standard to encode or obscure
3 data at rest or in transit. As of the EFFECTIVE DATE, the existing industry standard shall be
4 AES 256-bit encryption or Transport Layer Security (TLS) 1.2, or their equivalents.

5 3.7 “GLBA” shall mean the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat.
6 1338.

7 3.8 “HIPAA” shall mean the Health Insurance Portability and Accountability Act of
8 1996, Pub. L. No. 104-191, 110 Stat. 1938, as amended by the Health Information Technology
9 for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the
10 Department of Health and Human Services (“HHS”) Regulations, 45 C.F.R. §§ 160 et seq.

11 3.9 “HIPAA SECURITY RULE” shall mean the Security Standards for the Protection
12 of Electronic Protected Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and E.

13 3.10 “HIPAA PRIVACY RULE” shall mean the Standards for Privacy of Individually
14 Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and E.

15 3.11 “MEDICAL INFORMATION” shall have the same meaning as listed in the
16 Confidentiality of Medical Information Act, Civil Code section 56 et seq.

17 3.12 “MULTI-FACTOR AUTHENTICATION” means authentication through
18 verification of at least two of the following authentication factors: (i) Knowledge factors, such as
19 a password; or (ii) Possession factors, such a token or text message on a mobile phone; or (iii)
20 Inherence factors, such as a biometric characteristic.

21 3.13 “MULTISTATE EXECUTIVE COMMITTEE” shall mean the Attorneys General
22 of the States of Washington, Oregon, and California.

23 3.14 “PERSONAL INFORMATION” shall have the same meaning as listed in the
24 SECURITY BREACH NOTIFICATION ACT and/or CONSUMER PROTECTION LAWS.

25 3.15 “PREMERA” shall mean Premera Blue Cross, its parent and its directly or
26 indirectly wholly-owned or controlled affiliates, subsidiaries and divisions, successors and
27 assigns.

28

1 PROTECTED HEALTH INFORMATION, or MEDICAL INFORMATION collected from or
2 about consumers.

3 **4.4 COMPLIANCE PROGRAM:**

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

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

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

14 d. The Compliance Officer shall continue to oversee PREMERA’s Compliance
15 Program, and shall function as an independent and objective body that reviews and evaluates
16 compliance within PREMERA. The Compliance Officer shall develop a process for evaluating
17 compliance risks and determining priorities, reviewing compliance plans, and ensuring follow-up
18 to compliance issues identified occurs within a reasonable timeframe and that processes are in
19 place for determining and implementing appropriate disciplinary and corrective actions when
20 violations arise.

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

24 f. PREMERA shall ensure that its Compliance Program continues to receive the
25 resources and support necessary to ensure that the Compliance Program functions as required and
26 intended by this Final Judgment and Permanent Injunction.

27 g. PREMERA may satisfy the implementation and maintenance of the Compliance
28 Program and the safeguards required by this Final Judgment and Permanent Injunction through

1 review, maintenance, and, if necessary, updating of an existing compliance program or existing
2 safeguards, provided that such existing compliance program and existing safeguards meet the
3 requirements set forth in this Final Judgment and Permanent Injunction.

4 **4.5 INFORMATION SECURITY PROGRAM:**

5 a. PREMERA may satisfy the implementation and maintenance of the Information
6 Security Program and the safeguards and controls required by this Final Judgment and Permanent
7 Injunction through review, maintenance, and, if necessary, updating of an existing information
8 security program or existing controls and safeguards, provided that such existing compliance
9 program and existing safeguards and controls meet the requirements set forth in this Final
10 Judgment and Permanent Injunction.

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

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

- 18 (i). The size and complexity of PREMERA’s operations;
- 19 (ii). The nature and scope of PREMERA’s activities; and
- 20 (iii). The sensitivity of the PERSONAL INFORMATION, PROTECTED
21 HEALTH INFORMATION, or MEDICAL INFORMATION that PREMERA collects, stores,
22 transmits, and/or maintains.

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

- 25 (i). Regularly monitor, log, and inspect all network traffic, including log-in
26 attempts, through the implementation of hardware, software, or procedural mechanisms that
27 record and examine such activity;

28

1 (ii). Ensure that every device, user, and network flow is authorized and
2 authenticated; and

3 (iii). Only allow access by users of the PREMERA NETWORK to the minimum
4 extent necessary and require appropriate authorization and authentication prior to allowing any
5 such access.

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

7 (i). Protect the security, integrity, availability, and confidentiality of
8 PERSONAL INFORMATION, PROTECTED HEALTH INFORMATION, and MEDICAL
9 INFORMATION;

10 (ii). Protect against any threats to the security, integrity, availability, or
11 confidentiality of PERSONAL INFORMATION, PROTECTED HEALTH INFORMATION,
12 and MEDICAL INFORMATION;

13 (iii). Protect against unauthorized access to or use of PERSONAL
14 INFORMATION, PROTECTED HEALTH INFORMATION, MEDICAL INFORMATION and
15 minimize the likelihood of harm to any consumer;

16 (iv). Define and periodically reevaluate a schedule for retention of PERSONAL
17 INFORMATION, PROTECTED HEALTH INFORMATION, and MEDICAL INFORMATION
18 and for its destruction when such information is no longer needed for business purposes;

19 (v). Restrict access within the PREMERA NETWORK based on necessity and
20 job function, including but not limited to by restricting access to the PERSONAL
21 INFORMATION, PROTECTED HEALTH INFORMATION, and MEDICAL INFORMATION]
22 within the PREMERA NETWORK;

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

25 (vii). Restrict the ability of PREMERA employees and vendors to access the
26 PREMERA NETWORK via personal devices (e.g., smartphones, tablets, personal laptops);
27 PREMERA shall permit access only based on a business need. If required, the access shall be
28 restricted to only the data, systems, and other network resources required for the vendor's or

1 employee's job. Any access to the PREMERA NETWORK via a personal device shall be
2 reviewed on a regular basis to determine if the vendor's or employee's job function requires this
3 access. Furthermore, this access shall be provided via a secured connection to the PREMERA
4 NETWORK via VPN and MULTI-FACTOR AUTHENTICATION or other greater security
5 safeguards; and

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

10 f. PREMERA may satisfy the implementation and maintenance of the Information
11 Security Program and the safeguards required by this Final Judgment and Permanent Injunction
12 through review, maintenance, and, if necessary, updating, of an existing information security
13 program or existing safeguards, provided that such existing information security program and
14 existing safeguards meet the requirements set forth in this Final Judgment and Permanent
15 Injunction.

16 g. PREMERA shall employ an executive or officer who shall be responsible for
17 implementing, maintaining, and monitoring the Information Security Program (for ease,
18 hereinafter referred to as the "Chief Information Security Officer"). The Chief Information
19 Security Officer shall have the appropriate background or experience in information security and
20 HIPAA compliance. PREMERA shall ensure that the Chief Information Security Officer is a
21 separate position from the Chief Information Officer, and shall serve as PREMERA's
22 DESIGNATED SECURITY OFFICIAL. The Chief Information Security Officer shall have
23 direct access to the Chief Executive Officer and the Audit and Compliance Committee of the
24 Board of Directors.

25 h. PREMERA shall ensure that the role of the Chief Information Security Officer
26 includes directly advising PREMERA's Board of Directors, Chief Executive Officer, and Chief
27 Information Officer on the management of PREMERA's security posture, the security risks faced
28 by PREMERA, the security implications of PREMERA's decisions, and the adequacy of

1 PREMERA’s Information Security Program. The Chief Information Security Officer shall meet
2 with, and provide an oral or written update to: (1) the Board of Directors on at least an annual
3 basis; (2) the Chief Executive Officer at least every two months; (3) the Chief Information Officer
4 on at least a twice per month basis; and (4) the DESIGNATED PRIVACY OFFICIAL at least
5 every two months. The Chief Information Security Officer shall inform the Chief Executive
6 Officer, the Chief Information Officer, and the DESIGNATED PRIVACY OFFICIAL of any
7 material unauthorized intrusion to the PREMERA NETWORK within forty-eight (48) hours of
8 discovery of the intrusion. A material unauthorized intrusion is any intrusion to the PREMERA
9 NETWORK that affects or may affect any PROTECTED HEALTH INFORMATION,
10 PERSONAL INFORMATION, or MEDICAL INFORMATION.

11 i. PREMERA shall ensure that the Chief Information Security Officer and
12 Information Security Program receive the resources and support necessary to ensure that the
13 Information Security Program functions as intended by this Final Judgment and Permanent
14 Injunction.

15 j. PREMERA shall ensure that employees who are responsible for implementing,
16 maintaining, or monitoring the Information Security Program, including but not limited to the
17 Chief Information Officer and Chief Information Security Officer, have sufficient knowledge of
18 the requirements of the Final Judgment and Permanent Injunction.

19 k. At least once each year, PREMERA shall provide training on safeguarding and
20 protecting consumer PERSONAL INFORMATION, PROTECTED HEALTH INFORMATION,
21 and MEDICAL INFORMATION to all employees who handle such information, and its
22 employees responsible for implementing, maintaining, or monitoring the Information Security
23 Program. PREMERA’s Information Security Program shall be designed and implemented to
24 ensure the appropriate and timely identification, investigation of, and response to SECURITY
25 INCIDENTS.

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

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

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

8 (i). Preparation;

9 (ii). Investigation, Detection and Analysis;

10 (iii). Containment;

11 (iv). Notification and Coordination with Law Enforcement;

12 (v). Eradication;

13 (vi). Recovery;

14 (vii). Consumer and Regulator Notification and Remediation; and

15 (viii). Post-Incident Analysis (Lessons Learned).

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

20 p. PREMERA shall make reasonable efforts to ensure that any service providers or
21 vendors it employs that handle PERSONAL INFORMATION, PROTECTED HEALTH
22 INFORMATION, or MEDICAL INFORMATION shall (1) have safeguards in place to protect
23 PERSONAL INFORMATION, PROTECTED HEALTH INFORMATION, or MEDICAL
24 INFORMATION and (2) notify PREMERA promptly after discovering any potential compromise
25 of the confidentiality, integrity, or availability of PERSONAL INFORMATION, PROTECTED
26 HEALTH INFORMATION, or MEDICAL INFORMATION that is held, stored or processed by
27 the service provider or vendor on behalf of PREMERA.
28

1 **4.6 PERSONAL INFORMATION, PROTECTED HEALTH INFORMATION,**
2 **AND MEDICAL INFORMATION SAFEGUARDS AND CONTROLS:**

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

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

13 **4.7 SPECIFIC TECHNICAL SAFEGUARDS AND CONTROLS:**

14 a. Asset Inventory and Managing Critical Assets:

15 (i). PREMERA shall, within one hundred and eighty days (180) days of the
16 EFFECTIVE DATE of this Final Judgment and Permanent Injunction, implement and maintain a
17 configuration management database that contains an asset inventory for all known Critical Assets
18 that identifies: (a) the name of the asset; (b) the version of the asset; (c) the owner of the asset;
19 (d) the asset's location within the PREMERA NETWORK; (e) whether the asset is a Critical
20 Asset; and (f) the date that each security update or patch was applied. PREMERA shall apply the
21 highest rating it uses for any asset that either it uses to collect, store, transmit, or use PERSONAL
22 INFORMATION, PROTECTED HEALTH INFORMATION, or MEDICAL INFORMATION
23 ("Critical Assets").

24 (ii). PREMERA shall, within one year of the EFFECTIVE DATE of this Final
25 Judgment and Permanent Injunction, implement and maintain an asset inventory for all assets that
26 identifies: (a) the name of the asset; (b) the version of the asset; (c) the owner of the asset; (d) the
27 asset's location within the PREMERA NETWORK; (e) whether the asset is a Critical Asset; and
28 (f) the date that each security update or patch was applied.

1 b. Mapping and Encryption of Sensitive Data:

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

8 (ii). PREMERA shall ensure that electronic PERSONAL INFORMATION,
9 PROTECTED HEALTH INFORMATION, or MEDICAL INFORMATION that is stored at rest
10 or is in transmission is ENCRYPTED except where PREMERA determines that ENCRYPTION
11 is not reasonable and appropriate and it documents the rationale for this decision.

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

18 d. Penetration Testing: PREMERA shall engage a third-party vendor to perform an
19 annual penetration test to the PREMERA NETWORK, and shall ensure any risks or
20 vulnerabilities identified are risk assessed, prioritized, and addressed under PREMERA'S
21 Information Security Program. The parties understand and agree that addressing a risk may
22 include remediation or alternate risk mitigation efforts based on the risk assessment in Paragraph
23 4.7(e).

24 e. Risk Assessment: PREMERA shall conduct an accurate and thorough risk
25 assessment on any material risks and/or vulnerabilities identified by its internal auditors or
26 through penetration testing as required by Paragraph 4.7(d) within thirty (30) days of
27 identification of the risk or vulnerability to the PREMERA NETWORK and its COVERED
28 SYSTEMS. PREMERA shall rate each vulnerability on a risk-based rating scale developed by

1 PREMERA that takes into account cybersecurity best practices and risk to PERSONAL
2 INFORMATION, PROTECTED HEALTH INFORMATION, and MEDICAL INFORMATION.
3 PREMERA shall ensure that risks or vulnerabilities that threaten the safeguarding or security of
4 any PERSONAL INFORMATION, PROTECTED HEALTH INFORMATION, or MEDICAL
5 INFORMATION maintained on the PREMERA NETWORK shall be addressed and remediated
6 as expeditiously as possible. PREMERA shall document in writing any decision not to address a
7 risk or vulnerability that threatens the safeguarding or security of any PERSONAL
8 INFORMATION, PROTECTED HEALTH INFORMATION, or MEDICAL INFORMATION
9 maintained on the PREMERA NETWORK.

10 (i). The risk assessment shall include an accurate and thorough assessment of
11 the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic
12 protected health information held as required by HIPAA Security Rule, 45 C.F.R.
13 § 164.308(a)(1)(ii)(A).

14 (ii). PREMERA shall implement and maintain a corresponding risk-assessment
15 program designed to identify and assess risks to the PREMERA NETWORK. In cases where
16 PREMERA deems quantitative risk to be acceptable, PREMERA shall generate and retain a
17 report demonstrating how such risks are to be managed in consideration of the risk to
18 PERSONAL INFORMATION, PROTECTED HEALTH INFORMATION, and MEDICAL
19 INFORMATION, and the cost or difficulty in implementing effective countermeasures. All
20 reports shall be maintained by the Chief Information Security Officer and be available for
21 inspection by its DESIGNATED PRIVACY OFFICIAL, and the Third-Party Assessor described
22 in Paragraph 5.1 of this Final Judgment and Permanent Injunction.

23 f. Secure Network Communications: PREMERA shall implement and maintain
24 controls that filter incoming emails for potential phishing attacks or other fraudulent emails and
25 that establish strong peer-to-peer communications between its employees and vendors. In
26 addition, PREMERA will secure external communications to limit the ability of an attacker or
27 malicious intruder to communicate from the PREMERA NETWORK to unknown IP addresses.
28

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

6 (i). PREMERA shall, within nine (9) months of the EFFECTIVE DATE,
7 implement and maintain appropriate controls to manage access to, and use of, all administrator,
8 service, and vendor accounts with access to PERSONAL INFORMATION, PROTECTED
9 HEALTH INFORMATION, or MEDICAL INFORMATION. Such controls shall include,
10 without limitation, (1) strong passwords, (2) password confidentiality policies, (3) password-
11 rotation policies, (4) MULTI-FACTOR AUTHENTICATION or any other equal or greater
12 authentication protocol for identity management, and (5) appropriate safeguards for
13 administrative level passwords.

14 (ii). PREMERA shall implement and maintain appropriate controls to manage
15 access to, and use of, all PREMERA employee user accounts with access to PERSONAL
16 INFORMATION, PROTECTED HEALTH INFORMATION, or MEDICAL INFORMATION.

17 (iii). PREMERA shall implement and maintain appropriate administrative
18 processes and procedures to store and monitor the account credentials and access privileges of
19 employees who have privileges to design, maintain, operate, and update the PREMERA
20 NETWORK.

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

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

28

1 (vi). PREMERA shall immediately disable access privileges for all persons
2 whose access to the PREMERA NETWORK is no longer required or appropriate. PREMERA
3 shall limit access to PERSONAL INFORMATION, PROTECTED HEALTH INFORMATION,
4 or MEDICAL INFORMATION by persons accessing the PREMERA NETWORK on a least-
5 privileged basis.

6 (vii). PREMERA shall regularly inventory the users who have access to the
7 PREMERA NETWORK in order to review and determine whether or not such access remains
8 necessary or appropriate. PREMERA shall regularly compare employee termination lists to user
9 accounts to ensure access privileges have been appropriately terminated. At a minimum, such
10 review shall be performed on a quarterly basis. When the privileges, including for any disabled
11 accounts, are determined to be no longer necessary for any business function, PREMERA shall
12 terminate access privileges for those accounts.

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

16 h. File Integrity and End-point Monitoring: PREMERA shall deploy and maintain
17 controls designed to provide near real-time and/or real-time notification of unauthorized access to
18 PERSONAL INFORMATION, PROTECTED HEALTH INFORMATION, or MEDICAL
19 INFORMATION. PREMERA shall, within six (6) months from the EFFECTIVE DATE of this
20 Final Judgment and Permanent Injunction, deploy and maintain controls designed to provide near
21 real-time or real-time notification of modifications to any applications or systems that either
22 contain or provide access to PERSONAL INFORMATION, PROTECTED HEALTH
23 INFORMATION, or MEDICAL INFORMATION.

24 i. Controlling Permissible Applications: For servers in the PREMERA NETWORK,
25 PREMERA shall deploy and maintain controls within one year of the EFFECTIVE DATE that
26 are designed to block and/or prevent the execution of unauthorized applications within the
27 PREMERA NETWORK, as prescribed in the implementation standards of the HITRUST
28 framework. For clients (e.g., desktops, laptops, tablets), PREMERA shall maintain the controls

1 prescribed in the implemented HITRUST framework designed to block and/or prevent the
2 execution of unauthorized applications within the PREMERA NETWORK. Additionally, the
3 controls will provide alerts when unauthorized applications attempt to execute on the PREMERA
4 NETWORK.

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

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

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

13 k. Change Control: PREMERA shall implement and maintain policies and
14 procedures reasonably designed to manage and document changes to the PREMERA
15 NETWORK.

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

23 **IV. ASSESSMENT AND REPORTING REQUIREMENTS TO THE ATTORNEY**

24 **GENERAL**

25 5.1 Information Security Assessment:

26 a. PREMERA shall, for a period of three years (3) after the EFFECTIVE DATE of
27 this Final Judgment and Permanent Injunction, obtain an annual information security assessment
28 and report from a third-party professional (“Third Party Assessor”) using procedures and

1 standards generally accepted in the profession (“Third party Assessment”), commencing within
2 one (1) year after the EFFECTIVE DATE of this Final Judgment and Permanent Injunction. The
3 Third Party Assessor’s report on the Third-Party Assessment shall:

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

6 (ii). Explain the extent to which such safeguards are appropriate in light of
7 PREMERA’s size and complexity, the nature and scope of PREMERA’s activities, and the
8 sensitivity of the PERSONAL INFORMATION, PROTECTED HEALTH INFORMATION, or
9 MEDICAL INFORMATION maintained by PREMERA;

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

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

15 (v). Specifically review and evaluate the reasonableness of any decision to not
16 encrypt PERSONAL INFORMATION, PERSONAL HEALTH INFORMATION, or MEDICAL
17 INFORMATION, in compliance with Paragraph 4.7(b);

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

20 (vii). Specifically review and evaluate PREMERA’s compliance with the
21 penetration testing requirements set forth in Paragraph 4.7(d); the risk assessment requirements
22 set forth in Paragraph 4.7(e); the logging and monitoring requirements set forth in Paragraph
23 4.7(j); the change control requirements set forth in Paragraph 4.7(k); and the updates/patch
24 management requirements set forth in Paragraph 4.7(l).

25 b. The Third-Party Assessor shall be a Certified Information Systems Security
26 Professional (“CISSP”) or a Certified Information Systems Auditor (“CISA”), or a similarly
27 qualified person or organization; have at least five (5) years of experience evaluating the
28

1 effectiveness of computer system security or information system security; and must be approved
2 by the MULTISTATE EXECUTIVE COMMITTEE.

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

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

10 e. The Washington Attorney General's Office may provide a copy of the Third-Party
11 Assessor's Report received from PREMERA to the California Attorney General's Office upon
12 request, and the California Attorney General shall, to the extent permitted by the laws of
13 California, treat such Third-Party Assessor's Report as exempt from disclosure under the relevant
14 public records laws.

15 5.2 Compliance Program Assessment: Within one-hundred-and-eighty (180) days of
16 the EFFECTIVE DATE of this Final Judgment and Permanent Injunction, PREMERA shall
17 conduct an assessment of the structure of and personnel responsible for PREMERA's Compliance
18 Program (the "Compliance Program Assessment"). The Compliance Program Assessment
19 required by this paragraph shall be conducted by a third-party professional (the "Compliance
20 Program Assessor").

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

23 b. The Compliance Program Assessor shall:

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

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

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

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

4 c. The findings of the Compliance Program Assessment shall be documented in a
5 report (the “Compliance Program Assessor’s Report”). PREMERA shall provide a copy of the
6 Compliance Program Assessor’s Report to the Washington Attorney General’s Office within
7 thirty (30) days of the completion of the Compliance Program Assessment.

8 d. The State of Washington shall, to the extent permitted by the laws of the State of
9 Washington, treat such Compliance Program Assessor’s Report as exempt from disclosure under
10 the relevant public records laws.

11 e. The Washington Attorney General’s Office may provide a copy of the Compliance
12 Program Assessor’s Report received from PREMERA to the California Attorney General’s Office
13 upon request, and the California Attorney General shall, to the extent permitted by the laws of
14 California, treat such Compliance Program Assessor’s Report as exempt from disclosure under
15 the relevant public records laws.

16 5.3 PREMERA will make reasonable good faith efforts to address any concerns and
17 implement recommendations made by the Third Party Assessor or the Compliance Assessor.

18 VI. DOCUMENT RETENTION

19 6.1 PREMERA shall retain and maintain the reports, records, information and other
20 documentation required by this Final Judgment and Permanent Injunction for a period of no less
21 than three (3) years after the document is finalized, last edited, or last used.

22 VII. PAYMENT TO THE STATES

23 7.1 No later than thirty (30) days after the EFFECTIVE DATE, PREMERA shall pay
24 a total of Ten Million Dollars (\$10,000,000.00) to the Attorneys General. This amount is to be
25 divided and paid by PREMERA directly to the California Attorney General in an amount to be
26 designated by and in the sole discretion of the MULTISTATE EXECUTIVE COMMITTEE.
27 Said payment may be used by the Attorney General for purposes that may include, but are not
28 limited to, additional consumer relief; attorneys’ fees and other costs of investigation and

1 litigation, or to be placed in, or applied to, consumer protection enforcement funds, including
2 future consumer protection enforcement, consumer education, litigation or local consumer aid
3 fund or revolving fund, used to defray the costs of the inquiry leading hereto, or for any lawful
4 purpose, at the sole discretion of the Attorney General.

5 7.2 Specifically pursuant to Business and Professions Code section 17206, PREMERA
6 shall pay the Attorney General the amount of \$1,002,813.77, which shall be allocated and used in
7 accordance with Business and Professions Code section 17206. Payment shall be made by wire
8 transfer to the California Attorney General's Office pursuant to instructions provided by the
9 California Attorney General's Office.

10 **VIII. RELEASE**

11 8.1 Following full payment of the amount due under this Final Judgment and
12 Permanent Injunction, the Attorney General shall release and discharge PREMERA from all civil
13 claims that the Attorney General has or could have brought under Civil Code sections 56.101(a),
14 56.10(a), 56.36(c), and 1798.82, Business and Professions Code sections 17200 et seq. and 17500
15 et seq., and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-
16 191, 110 Stat. 1938, as amended by the Health Information Technology for Economic and
17 Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the Department of Health and
18 Human Services ("HHS") Regulations, 45 C.F.R. §§ 160 et seq. arising out of PREMERA's
19 conduct related to, and the Attorney General's investigation of, the data security incident first
20 publicly announced March 17, 2015. Nothing contained in this paragraph shall be construed to
21 limit the ability of the Attorney General to enforce the obligations that PREMERA has under this
22 Final Judgment and Permanent Injunction. Further, nothing in this Final Judgment and
23 Permanent Injunction shall be construed to create, waive, or limit any private right of action or
24 any action brought by any state agency other than the Attorney General.

25 8.2 The obligations and other provisions of this Final Judgment and Permanent
26 Injunction set forth in Sections 4.5 and 4.7 shall expire at the conclusion of the five (5) year
27 period after the EFFECTIVE DATE of this Final Judgment and Permanent Injunction, unless
28 they have expired at an earlier date pursuant to their specific terms. The obligations and other

1 provisions of this Final Judgment and Permanent Injunction set forth in Paragraphs 4.4 and 4.6
2 shall expire at the conclusion of the ten (10) year period after the EFFECTIVE DATE of this
3 Final Judgment and Permanent Injunction, unless they have expired at an earlier date pursuant to
4 their specific terms. Other sections and paragraph with specified time periods shall expire as
5 detailed in those sections and paragraphs. Nothing in this paragraph should be construed or
6 applied to excuse PREMERA from its obligation to comply with all applicable state and federal
7 laws, regulations and rules.

8 8.3 Notwithstanding any term of this Final Judgment and Permanent Injunction, any
9 and all of the following forms of liability are specifically reserved and excluded from the release
10 as to any entity or person, including PREMERA:

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

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

16 (i). State or federal antitrust violations;

17 (ii). State or federal securities violations; or

18 (iii). State or federal tax claims.

19 **IX. MEET AND CONFER**

20 9.1 If the Attorney General determines that PREMERA has failed to comply with any
21 of Sections IV and V of this Final Judgment and Permanent Injunction, and if in the Attorney
22 General's sole discretion the failure to comply with this Final Judgment and Permanent Injunction
23 does not threaten the health or safety of the residents of the State of California and/or does not
24 create an emergency requiring immediate action, the Attorney General will notify PREMERA in
25 writing of such failure to comply and PREMERA shall have thirty (30) days from receipt of such
26 written notice to provide a good faith written response to the Attorney General, including either a
27 statement that PREMERA believes it is in full compliance or otherwise a statement explaining
28 how the violation occurred, how it has been addressed or when it will be addressed, and what

1 from the denial of PREMERA's most recent motion to terminate or at such earlier time as the
2 Court may allow.

3 10.4 Under no circumstances shall this Final Judgment and Permanent Injunction or the
4 name of the Office of the Attorney General or any of its employees or representatives be used by
5 PREMERA in connection with any selling, advertising, or promotion of products or services, or
6 as an endorsement or approval of PREMERA's acts, practices or conduct of business.

7 10.5 Nothing in this Final Judgment and Permanent Injunction shall be construed to
8 limit the authority or ability of the Attorney General to protect the interests of the State of
9 California or the people of the State of California. This Final Judgment and Permanent Injunction
10 shall not bar the Attorney General or any other governmental entity from enforcing laws,
11 regulations, or rules against PREMERA for conduct subsequent to or otherwise not covered by
12 this Final Judgment and Permanent Injunction. Further, nothing in this Final Judgment and
13 Permanent Injunction shall be construed to limit the ability of the Attorney General to enforce the
14 obligations that PREMERA has under this Final Judgment and Permanent Injunction.

15 10.6 Nothing in this Final Judgment and Permanent Injunction shall be construed as
16 relieving PREMERA of the obligation to comply with all state and federal laws, regulations, and
17 rules, nor shall any of the provisions of this Final Judgment and Permanent Injunction be deemed
18 to be permission to engage in any acts or practices prohibited by such laws, regulations, and rules.

19 10.7 PREMERA shall deliver a copy of this Final Judgment and Permanent Injunction
20 to, and otherwise fully apprise, its Chief Executive Officer, Chief Information Officer, Chief
21 Information Security Officer, Compliance Officer, DESIGNATED PRIVACY OFFICIAL,
22 DESIGNATED SECURITY OFFICIAL, Chief Legal Officer, and its Board of Directors within
23 (30) days of the EFFECTIVE DATE. To the extent PREMERA hires or replaces any of the above
24 listed officers, counsel or Directors, PREMERA shall deliver a copy of this Final Judgment and
25 Permanent Injunction to their replacements within thirty (30) days from the date on which such
26 person assumes his/her position with PREMERA.

27
28

1 10.8 No court costs, if any, shall be taxed upon the Attorney General. To the extent
2 there are any court costs associated with the filing of this Final Judgment and Permanent
3 Injunction, PREMERA shall pay all such court costs.

4 10.9 PREMERA shall not participate in any activity or form a separate entity or
5 corporation for the purpose of engaging in acts or practices in whole or in part that are prohibited
6 by this Final Judgment and Permanent Injunction or for any other purpose that would otherwise
7 circumvent any term of this Final Judgment and Permanent Injunction. PREMERA shall not
8 knowingly cause, permit, or encourage any other persons or entities acting on its behalf, to
9 engage in practices prohibited by this Final Judgment and Permanent Injunction.

10 10.10 PREMERA agrees that this Final Judgment and Permanent Injunction does not
11 entitle it to seek or to obtain attorneys' fees as a prevailing party under any statute, regulation, or
12 rule, and PREMERA further waives any right to attorneys' fees that may arise under such statute,
13 regulation, or rule.

14 10.11 This Final Judgment and Permanent Injunction shall not be construed to waive any
15 claims of sovereign immunity of the State of California may have in any action or proceeding.

16 10.12 If any portion of this Final Judgment and Permanent Injunction is held invalid by
17 operation of law, the remaining terms of this Final Judgment and Permanent Injunction shall not
18 be affected and shall remain in full force and effect.

19 10.13 Whenever PREMERA shall provide reports to the Washington Attorney General
20 under Section V of this Final Judgment and Permanent Injunction, those requirements shall be
21 satisfied by sending the report to: ATTN: Tiffany Lee and Andrea Alegrett, Assistant Attorney
22 General, Consumer Protection Division, Office of the Attorney General, 800 Fifth Avenue #2000,
23 Seattle, WA 98104.

24 10.14 Except as specified elsewhere in this Final Judgment and Permanent Injunction,
25 whenever PREMERA shall provide notice and documents to the Attorney General under this
26 Judgment, that requirement shall be satisfied by sending the notice and documents to: Yen P.
27 (TiTi) Nguyen, Deputy Attorney General, Consumer Law Section/Privacy Unit, 455 Golden Gate
28 Avenue, Suite 11000, San Francisco, CA 94102.

1 10.15 Any notice or report provided by the Attorney General to PREMERA under
2 Section IX of this Final Judgment and Permanent Injunction shall be satisfied by sending notice
3 to: Chief Legal Officer, Premera Blue Cross, 7001 220th St., SW, MS 316, Mountlake Terrace,
4 WA 98043.

5 10.16 All documents to be provided under this Final Judgment and Permanent Injunction
6 shall be sent by United States mail, certified mail return receipt requested, or other nationally
7 recognized courier service that provides for tracking services and identification of the person
8 signing for the notice or document, and shall have been deemed to be sent upon mailing. The
9 parties may update their designee or address by sending written notice to the other party
10 informing it of the change.

11 10.17 Jurisdiction is retained by the Court for the purpose of enabling any party to the
12 Final Judgment and Permanent Injunction to apply to the Court at any time for such further orders
13 and directions as may be necessary or appropriate for the construction or the carrying out of this
14 Final Judgment and Permanent Injunction, for the modification of any of the injunctive provisions
15 hereof, for enforcement of compliance herewith, and for the punishment of violations hereof, if
16 any.

17 10.18 The clerk is ordered to enter this Final Judgment and Permanent Injunction
18 forthwith.

19
20 Dated: _____, 2019

Judge of the Superior Court