

STATE OF CONNECTICUT

DOCKET NO. HHD-CV-19-6114113-S

STATE OF CONNECTICUT, <i>Plaintiff,</i>	:	SUPERIOR COURT
	:	
	:	JUDICIAL DISTRICT OF HARTFORD
v.	:	
	:	AT HARTFORD
PREMERA BLUE CROSS <i>Defendant.</i>	:	JULY 11, 2019

STIPULATED JUDGMENT

1.1 Plaintiff State of Connecticut (“the State”) conducted an investigation and commenced this action pursuant to the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the Department of Health and Human Services (“HHS”) Regulations, 45 C.F.R. §§ 160 *et seq.* (“HIPAA”), Connecticut Unfair Trade Practices Act (“CUTPA”), General Statutes § 42-110b *et seq.*, and Connecticut's Safeguards Law, General Statutes § 42-471.

1.2 Plaintiff appears by and through William Tong, Connecticut Attorney General and Premera Blue Cross as defined in Paragraph 3.14 (“PREMERA”), appears by and through their attorneys, Martin T. Booher, Theodore Kobus, III, and Patrick H. Haggerty.

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

1 General Statutes § 42-110b *et seq.*, and the Safeguards Law, General Statutes § 42-471. The
2 Attorney General is also authorized to enforce violations of the Data Breach Notification Law,
3 General Statutes § 36a-701b *et seq.*

4 2.2 Premera Blue Cross is a Washington non-profit corporation with its principal
5 office located at 7001 220th St. SW, Building 1, Mountlake Terrace, Washington 98043.

6 2.3 This Court has jurisdiction of the subject matter of this action, jurisdiction over
7 the parties to this action, and venue is proper in this Court.

8 2.4 PREMERA consents to the filing of this Stipulated Judgment in the Superior
9 Court of the Judicial District of Hartford, which is the proper venue to enforce this Stipulated
10 Judgment pursuant to CUTPA.

11 2.5 Jurisdiction is proper because PREMERA has engaged in conduct impacting
12 Connecticut or its residents at all times relevant to the claims at issue. For the purposes of this
13 Stipulated Judgment, or any action to enforce this Stipulated Judgment, PREMERA consents
14 to the Court's jurisdiction over this Stipulated Judgment and consents to venue in this judicial
15 district.

16 2.6 This Stipulated Judgment is entered pursuant to CUTPA, and more specifically,
17 General Statutes § 42-110m.

18 **III. DEFINITIONS**

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

23 3.2 "CONSUMER PROTECTION LAWS" shall mean the Connecticut Unfair
24 Trade Practices Act ("CUTPA"), General Statutes § 42-110b *et seq.*, and Connecticut's
25 Safeguards Law, General Statutes § 42-471.

1 3.3 “DESIGNATED PRIVACY OFFICIAL” shall mean the individual designated
2 by PREMERA who is responsible for the development and implementation of the policies and
3 procedures as required by 45 C.F.R. § 164.530(a).

4 3.4 “DESIGNATED SECURITY OFFICIAL” shall mean the individual designated
5 by PREMERA who is responsible for the development and implementation of the policies and
6 procedures as required by 45 C.F.R. § 164.308(a)(2).

7 3.5 “EFFECTIVE DATE” shall be July 11, 2019.

8 3.6 “ENCRYPTED” shall refer to the existing industry standard to encode or
9 obscure data at rest or in transit. As of the EFFECTIVE DATE, the existing industry standard
10 shall be AES 256-bit encryption or Transport Layer Security (TLS) 1.2, or their equivalents.

11 3.7 “GLBA” shall mean the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113
12 Stat. 1338.

13 3.8 “HIPAA” shall mean the Health Insurance Portability and Accountability Act of
14 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology
15 for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the
16 Department of Health and Human Services (“HHS”) Regulations, 45 C.F.R. §§ 160 *et seq.*

17 3.9 “HIPAA SECURITY RULE” shall mean the Security Standards for the
18 Protection of Electronic Protected Health Information, 45 C.F.R. Part 160 and Part 164,
19 Subparts A and E.

20 3.10 “HIPAA PRIVACY RULE” shall mean the Standards for Privacy of
21 Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and
22 E.

23 3.11 “MULTI-FACTOR AUTHENTICATION” means authentication through
24 verification of at least two of the following authentication factors: (i) Knowledge factors, such
25 as a password; or (ii) Possession factors, such a token or text message on a mobile phone; or
26 (iii) Inherence factors, such as a biometric characteristic.

1 4.2 Injunctions. PREMERA shall engage in or refrain from engaging in the practices
2 as identified in this Stipulated Judgment.

3 4.3 **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 compliance
13 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 Stipulated Judgment.

1 g. PREMERA may satisfy the implementation and maintenance of the Compliance
2 Program and the safeguards required by this Stipulated Judgment through review, maintenance,
3 and, if necessary, updating of an existing compliance program or existing safeguards, provided
4 that such existing compliance program and existing safeguards meet the requirements set forth in
5 this Stipulated Judgment.

6 4.4 **INFORMATION SECURITY PROGRAM:**

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

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

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

- 19 (i). The size and complexity of PREMERA’s operations;
20 (ii). The nature and scope of PREMERA’s activities; and
21 (iii). The sensitivity of the PERSONAL INFORMATION or PROTECTED
22 HEALTH INFORMATION that PREMERA collects, stores, 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
26

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

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

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

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

10 (i). Protect the security, integrity, availability, and confidentiality of
11 PERSONAL INFORMATION and PROTECTED HEALTH INFORMATION;

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

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

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

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

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

26

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

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

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

19 g. PREMERA shall employ an executive or officer who shall be responsible for
20 implementing, maintaining, and monitoring the Information Security Program (for ease,
21 hereinafter referred to as the "Chief Information Security Officer"). The Chief Information
22 Security Officer shall have the appropriate background or experience in information security
23 and HIPAA compliance. PREMERA shall ensure that the Chief Information Security Officer
24 is a separate position from the Chief Information Officer, and shall serve as PREMERA's
25 DESIGNATED SECURITY OFFICIAL. The Chief Information Security Officer shall have
26

1 direct access to the Chief Executive Officer and the Audit and Compliance Committee of the
2 Board of Directors.

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

17 i. PREMERA shall ensure that the Chief Information Security Officer and
18 Information Security Program receive the resources and support necessary to ensure that the
19 Information Security Program functions as intended by this Stipulated Judgment.

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

24 k. At least once each year, PREMERA shall provide training on safeguarding and
25 protecting consumer PERSONAL INFORMATION and PROTECTED HEALTH
26 INFORMATION to all employees who handle such information, and its employees responsible

1 for implementing, maintaining, or monitoring the Information Security Program.
2 PREMERA's Information Security Program shall be designed and implemented to ensure the
3 appropriate and timely identification, investigation of, and response to SECURITY
4 INCIDENTS.

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

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

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

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

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

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

8 **4.5 PERSONAL INFORMATION AND PROTECTED HEALTH**
9 **INFORMATION SAFEGUARDS AND CONTROLS:**

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

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

19 **4.6 SPECIFIC TECHNICAL SAFEGUARDS AND CONTROLS:**

20 a. Asset Inventory and Managing Critical Assets:

21 (i). PREMERA shall, within one hundred and eighty days (180) days of the
22 EFFECTIVE DATE of this Stipulated Judgment, implement and
23 maintain a configuration management database that contains an asset
24 inventory for all known Critical Assets that identifies: (a) the name of
25 the asset; (b) the version of the asset; (c) the owner of the asset; (d) the
26 asset's location within the PREMERA NETWORK; (e) whether the

1 asset is a Critical Asset; and (f) the date that each security update or
2 patch was applied. PREMERA shall apply the highest rating it uses for
3 any asset that either it uses to collect, store, transmit, or use PERSONAL
4 INFORMATION or PROTECTED HEALTH INFORMATION
5 (“Critical Assets”).

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

12 b. Mapping and Encryption of Sensitive Data:

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

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

23 c. Segmentation: PREMERA shall implement and maintain segmentation
24 protocols and related policies that are reasonably designed to properly segment the PREMERA
25 NETWORK, which shall, at a minimum, ensure system functionality and performance to meet
26 business needs while also mitigating exposure to the enterprise network in the event of an

1 attack or malicious intruder access. Additionally, PREMERA shall regularly evaluate, and as
2 appropriate, restrict and disable any unnecessary ports of service on the PREMERA
3 NETWORK.

4 d. Penetration Testing: PREMERA shall engage a third-party vendor to perform an
5 annual penetration test to the PREMERA NETWORK, and shall ensure any risks or
6 vulnerabilities identified are risk assessed, prioritized, and addressed under PREMERA'S
7 Information Security Program. The parties understand and agree that addressing a risk may
8 include remediation or alternate risk mitigation efforts based on the risk assessment in
9 Paragraph 4.6(e).

10 e. Risk Assessment: PREMERA shall conduct an accurate and thorough risk
11 assessment on any material risks and/or vulnerabilities identified by its internal auditors or
12 through penetration testing as required by Paragraph 4.6(d) within thirty (30) days of
13 identification of the risk or vulnerability to the PREMERA NETWORK and its COVERED
14 SYSTEMS. PREMERA shall rate each vulnerability on a risk-based rating scale developed by
15 PREMERA that takes into account cybersecurity best practices and risk to PERSONAL
16 INFORMATION and PROTECTED HEALTH INFORMATION. PREMERA shall ensure
17 that risks or vulnerabilities that threaten the safeguarding or security of any PERSONAL
18 INFORMATION or PROTECTED HEALTH INFORMATION maintained on the PREMERA
19 NETWORK shall be addressed and remediated as expeditiously as possible. PREMERA shall
20 document in writing any decision not to address a risk or vulnerability that threatens the
21 safeguarding or security of any PERSONAL INFORMATION or PROTECTED HEALTH
22 INFORMATION maintained on the PREMERA NETWORK.

23 (i). The risk assessment shall include an accurate and thorough assessment of
24 the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic
25 protected health information held as required by HIPAA Security Rule, 45 C.F.R. §
26 164.308(a)(1)(ii)(A).

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

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

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

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

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

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

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

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

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

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

26

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

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

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

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

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

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

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

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

14 V. ASSESSMENT AND REPORTING REQUIREMENTS TO THE ATTORNEY

15 GENERAL

16 5.1 Information Security Assessment:

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

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

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

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

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

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

8 (v). Specifically review and evaluate the reasonableness of any decision to not
9 encrypt PERSONAL INFORMATION and PERSONAL HEALTH INFORMATION, in
10 compliance with Paragraph 4.6(b).

11 (vi). Specifically review and evaluate PREMERA's response to SECURITY
12 INCIDENTS in the Security Incident Report (see Paragraph 4.4(o)); and

13 (vii). Specifically review and evaluate PREMERA's compliance with the
14 penetration testing requirements set forth in Paragraph 4.6(d); the risk assessment requirements
15 set forth in Paragraph 4.6(e); the logging and monitoring requirements set forth in Paragraph
16 4.7(j); the change control requirements set forth in Paragraph 4.6(k); and the updates/patch
17 management requirements set forth in Paragraph 4.6(l).

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

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

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

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

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

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

16 b. The Compliance Program Assessor shall:

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

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

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

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

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

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

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

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

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

13 **VI. DOCUMENT RETENTION**

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

17 **VII. PAYMENT TO THE STATES**

18 7.1 No later than thirty (30) days after the EFFECTIVE DATE, PREMERA shall pay
19 a total of Ten Million Dollars (\$10,000,000.00) to the Attorneys General, to be distributed as
20 designated by the MULTISTATE EXECUTIVE COMMITTEE. Out of this payment, Premera
21 shall pay to the State of Connecticut the amount of Fifty Three Thousand, Eight Hundred and
22 Fifty Dollars and Eighty Six Cents (\$53,850.86). Said payment shall be used by the Attorney
23 General for additional consumer relief; attorneys' fees and other costs of investigation and
24 litigation; or to be placed in, or applied to, consumer protection enforcement funds, including
25 future consumer protection enforcement, consumer education, litigation or local consumer aid
26 fund or revolving fund, used to defray the costs of the inquiry leading hereto, or for any lawful

1 purpose, at the sole discretion of the Attorney General.

2 **VIII. RELEASE**

3 8.1 Following full payment of the amount due under this Stipulated Judgment, the
4 Connecticut Attorney General shall release and discharge PREMERA from all civil claims that
5 the Attorney General has or could have brought under HIPAA, the CONSUMER
6 PROTECTION LAWS, AND SECURITY BREACH NOTIFICATION ACT arising out of
7 PREMERA's conduct related to, and the Attorney General's investigation of, the data security
8 incident first publicly announced March 17, 2015. Nothing contained in this paragraph shall be
9 construed to limit the ability of the Connecticut Attorney General to enforce the obligations
10 that PREMERA has under this Stipulated Judgment. Further, nothing in this Stipulated
11 Judgment shall be construed to create, waive, or limit any private right of action or any action
12 brought by any state agency other than the Attorney General.

13 8.2 The obligations and other provisions of this Stipulated Judgment set forth in
14 Sections 4.4 and 4.6 shall expire at the conclusion of the five (5) year period after the
15 EFFECTIVE DATE of this Stipulated Judgment, unless they have expired at an earlier date
16 pursuant to their specific terms. The obligations and other provisions of this Stipulated
17 Judgment set forth in Paragraphs 4.3 and 4.5 shall expire at the conclusion of the ten (10) year
18 period after the EFFECTIVE DATE of this Stipulated Judgment, unless they have expired at
19 an earlier date pursuant to their specific terms. Other sections and paragraph with specified
20 time periods shall expire as detailed in those sections and paragraphs. Nothing in this
21 paragraph should be construed or applied to excuse PREMERA from its obligation to comply
22 with all applicable state and federal laws, regulations and rules.

23 8.3 Notwithstanding any term of this Stipulated Judgment, any and all of the
24 following forms of liability are specifically reserved and excluded from the release as to any
25 entity or person, including PREMERA:

26 a. Any criminal liability that any person or entity, including PREMERA, has or

1 may have to the States.

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

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

8 **IX. MEET AND CONFER**

9 9.1 If any Attorney General determines that PREMERA has failed to comply with
10 any of Sections IV and V of this Stipulated Judgment, and if in the Attorney General’s sole
11 discretion the failure to comply with this Stipulated Judgment does not threaten the health or
12 safety of the citizens of the Attorney General’s State and/or does not create an emergency
13 requiring immediate action, the Attorney General will notify PREMERA in writing of such
14 failure to comply and PREMERA shall have thirty (30) days from receipt of such written
15 notice to provide a good faith written response to that Attorney General, including either a
16 statement that PREMERA believes it is in full compliance or otherwise a statement explaining
17 how the violation occurred, how it has been addressed or when it will be addressed, and what
18 PREMERA will do to make sure the violation does not happen again. The Attorney General
19 may agree to provide PREMERA more than thirty (30) days to respond.

20 9.2 Nothing herein shall be construed to exonerate any failure to comply with any
21 provision of this Stipulated Judgment, or limit the right and authority of an Attorney General to
22 initiate a proceeding for any failure to comply with this Stipulated Judgment after receiving the
23 response from PREMERA described in Paragraph 9.1, if the Attorney General determines that
24 an enforcement action is in the public interest.

25 **X. ENFORCEMENT**

26 10.1 Violation of any of the injunctions contained in this Stipulated Judgment, as

1 determined by the Court, shall constitute a violation of an injunction for which civil penalties
2 may be sought by the Attorney General pursuant to General Statutes § 42-110o.

3 10.2 This Stipulated Judgment is entered pursuant to CUTPA, and more specifically,
4 General Statutes § 42-110m. Jurisdiction is retained for the purpose of enabling any party to
5 this Stipulated Judgment with or without the prior consent of the other party to apply to the
6 Court at any time for enforcement of compliance with this Stipulated Judgment, to punish
7 violations thereof, or to modify or clarify this Stipulated Judgment.

8 10.3 Under no circumstances shall this Stipulated Judgment or the name of the State
9 of Connecticut, the Office of the Attorney General, Consumer Protection Division, or any of
10 their employees or representatives be used by PREMERA in connection with any selling,
11 advertising, or promotion of products or services, or as an endorsement or approval of
12 PREMERA's acts, practices or conduct of business.

13 10.4 Nothing in this Stipulated Judgment shall be construed to limit the authority or
14 ability of the Connecticut Attorney General to protect the interests of Connecticut or the people
15 of Connecticut. This Stipulated Judgment shall not bar the Connecticut Attorney General or
16 any other governmental entity from enforcing laws, regulations, or rules against PREMERA
17 for conduct subsequent to or otherwise not covered by this Stipulated Judgment. Further,
18 nothing in this Stipulated Judgment shall be construed to limit the ability of the Connecticut
19 Attorney General to enforce the obligations that PREMERA has under this Stipulated
20 Judgment.

21 10.5 Nothing in this Stipulated Judgment shall be construed as relieving PREMERA
22 of the obligation to comply with all state and federal laws, regulations, and rules, nor shall any
23 of the provisions of this Stipulated Judgment be deemed to be permission to engage in any acts
24 or practices prohibited by such laws, regulations, and rules.

25 10.6 PREMERA shall deliver a copy of this Stipulated Judgment to, and otherwise
26 fully apprise, its Chief Executive Officer, Chief Information Officer, Chief Information

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

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

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

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

20 10.10 This Stipulated Judgment shall not be construed to waive any claims of
21 sovereign immunity Connecticut may have in any action or proceeding.

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

25 10.12 Whenever PREMERA shall provide reports to the Washington Attorney
26 General under Section V of this Stipulated Judgment, those requirements shall be satisfied by

1 sending the report to: ATTN: Tiffany Lee and Andrea Alegrett, Assistant Attorney General,
2 Consumer Protection Division, Office of the Attorney General, 800 Fifth Avenue #2000,
3 Seattle, WA 98104.

4 10.13 Any notice or report provided by the Attorney General to PREMERA under
5 Section IX of this Stipulated Judgment shall be satisfied by sending notice to: Chief Legal
6 Officer, Premera Blue Cross, 7001 220th St., SW, MS 316, Mountlake Terrace, WA 98043.

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

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

18 10.16 The clerk is ordered to enter this Stipulated Judgment forthwith.

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

20 11.1 Upon entry of this Stipulated Judgment, all claims in this matter, not otherwise
21 addressed by this Stipulated Judgment are dismissed.

22 APPROVED:

23
24 PLAINTIFF, THE STATE OF CONNECTICUT

25 WILLIAM TONG,
26 Attorney General

1 APPROVED:

2 PLAINTIFF, THE STATE OF CONNECTICUT

3 WILLIAM TONG,
4 Attorney General

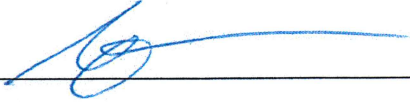
5 By: Michele Lucan

Date: 7/11/19

6 Michele Lucan
7 John Neumon
8 *Assistant Attorneys General*
9 Office of the Attorney General
10 110 Sherman Street
11 Hartford, Connecticut 06105
12 (860) 808-5440
13 Michele.lucan@ct.gov
14 John.neumon@ct.gov
15
16
17
18
19
20
21
22
23
24
25
26

1 APPROVED:

2 COUNSEL FOR DEFENDANT, PREMERA

3 By: 
4 _____

Date: 7/10/19

5 Martin T. Booher
6 Baker & Hostetler LLP
7 Key Tower
8 127 Public Square, Suite 2000
9 Cleveland, OH 44114
10 Telephone: (216) 861-7141
11 Email: mbooher@bakerlaw.com

12 Theodore J. Kobus III
13 Baker & Hostetler LLP
14 45 Rockefeller Plaza
15 New York, NY 10111
16 Telephone: (212) 271-1504
17 Email: tkobus@bakerlaw.com

18 Patrick H. Haggerty
19 Baker & Hostetler LLP
20 312 Walnut St., Suite 3200
21 Cincinnati, OH 45202
22 Telephone: (513) 929-3412
23 Email: phaggerty@bakerlaw.com

24 Entered:

25 _____
26 Judge

Date: _____