

GURBIR S. GREWAL  
ATTORNEY GENERAL OF NEW JERSEY  
Division of Law  
124 Halsey Street - 5<sup>th</sup> Floor  
P.O. Box 45029  
Newark, New Jersey 07101  
Attorney for Plaintiffs

By: Elliott M. Siebers (033582012)  
Deputy Attorney General

SUPERIOR COURT OF NEW JERSEY  
CHANCERY DIVISION,  
MERCER COUNTY  
DOCKET NO.: MER-C-\_\_\_\_\_ -19

GURBIR S. GREWAL, Attorney General of  
the State of New Jersey, and PAUL R.  
RODRÍGUEZ, Acting Director of the New  
Jersey Division of Consumer Affairs,

Plaintiffs,

v.

Premera Blue Cross Blue Shield

Defendants.

**FINAL CONSENT JUDGMENT**

**I. BACKGROUND**

1.1 Plaintiffs Gurbir S. Grewal, Attorney General of the State of New Jersey (“Attorney General”) and Paul R. Rodríguez, Acting Director of the New Jersey Division of Consumer Affairs (“Director”) (collectively, “Plaintiffs”) on behalf of the State of New Jersey (“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,

1 45 C.F.R. §§ 160 et seq. (“HIPAA”), and the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1  
2 et seq.

3 1.2 Defendant Premera Blue Cross as defined in Paragraph 3.14 (“PREMERA”),  
4 appears by and through its attorneys, Theodore Kobus, III and Patrick Haggerty.

5 1.3 Plaintiffs and PREMERA stipulate to the entry of this Final Consent Judgment by  
6 the Court without the taking of proof and without trial or adjudication of any fact or law.

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

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

13 1.6 PREMERA recognizes and states that this Final Consent Judgment is entered into  
14 voluntarily and that no promises or threats have been made by Plaintiffs of any member, officer,  
15 agent or representative of Plaintiffs’ Offices, to induce it to enter into this Final Consent Judgment.

16 1.7 PREMERA waives any right they may have to appeal from this Final Consent  
17 Judgment.

18 1.8 PREMERA further agrees that it will not oppose the entry of this Final Consent  
19 Judgment on the grounds the Final Consent Judgment fails to comply with R. 4:52-4, and hereby  
20 waives any objections based thereon.

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

24 The Court has reviewed the terms of this Final Consent Judgment and based upon the Parties’  
25 agreement and for good cause shown:

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

1  
2 **II. PARTIES AND JURISDICTION**

3 2.1 Plaintiffs Gurbir S. Grewal, Attorney General of the State of New Jersey (“Attorney  
4 General”) and Paul R. Rodríguez, Acting Director of the New Jersey Division of Consumer Affairs  
5 (“Director”) (collectively, “Plaintiffs”) are the Plaintiffs in this action.

6 2.2 The Attorney General is charged with the responsibility of enforcing the New Jersey  
7 Consumer Fraud Act, N.J.S.A. 56:8-1 et seq. (“CFA”), and the Director is charged with  
8 administering the CFA on behalf of the Attorney General.

9 2.3 Premera Blue Cross is a Washington non-profit corporation with its principal  
10 office located at 7001 220th St. SW, Building 1, Mountlake Terrace, Washington 98043.

11 2.4 The Parties admit jurisdiction of this Court over the subject matter and over the  
12 Parties for purpose of this Final Consent Judgment. The Court retains jurisdiction for the  
13 purposes of enabling the Parties to apply for such further orders and relief as may be necessary  
14 for the construction, modification, enforcement, execution or satisfaction of this Final Consent  
15 Judgment.

16 2.5 Venue is proper pursuant to N.J.S.A. 56:8-8 and PREMERA consents to the filing  
17 of this Final Consent Judgment in a county where the Attorney General maintains an office for  
18 the limited purpose of resolving the claims at issue.

19 2.6 Jurisdiction is proper because PREMERA has engaged in conduct impacting New  
20 Jersey or its residents at all times relevant to the claims at issue.

21 2.7 This Final Consent Judgment is entered pursuant to and subject to N.J.S.A. 56:8-  
22 8 and N.J.S.A. 56:8-13.

23 **III. DEFINITIONS**

24 3.1 “COVERED SYSTEMS” shall mean all components, including but not limited  
25 to, assets, technology, and software, within the PREMERA NETWORK that are used to collect,  
26

1 | process, transmit, and/or store PERSONAL INFORMATION or PROTECTED HEALTH  
2 | INFORMATION.

3 |         3.2     “CONSUMER PROTECTION LAWS” shall mean the New Jersey Consumer  
4 | Fraud Act, N.J.S.A. 56:8-1 et seq.

5 |         3.3     “DESIGNATED PRIVACY OFFICIAL” shall mean the individual designated  
6 | by PREMERA who is responsible for the development and implementation of the policies and  
7 | procedures as required by 45 C.F.R. § 164.530(a).

8 |         3.4     “DESIGNATED SECURITY OFFICIAL” shall mean the individual designated  
9 | by PREMERA who is responsible for the development and implementation of the policies and  
10 | procedures as required by 45 C.F.R. § 164.308(a)(2).

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

12 |         3.6     “ENCRYPTED” shall refer to the existing industry standard to encode or obscure  
13 | data at rest or in transit. As of the EFFECTIVE DATE, the existing industry standard shall be  
14 | AES 256-bit encryption or Transport Layer Security (TLS) 1.2, or their equivalents.

15 |         3.7     “GLBA” shall mean the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113  
16 | Stat. 1338.

17 |         3.8     “HIPAA” shall mean the Health Insurance Portability and Accountability Act of  
18 | 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology  
19 | for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the  
20 | Department of Health and Human Services (“HHS”) Regulations, 45 C.F.R. §§ 160 et seq.

21 |         3.9     “HIPAA SECURITY RULE” shall mean the Security Standards for the  
22 | Protection of Electronic Protected Health Information, 45 C.F.R. Part 160 and Part 164, Subparts  
23 | A and E.

24 |         3.10    “HIPAA PRIVACY RULE” shall mean the Standards for Privacy of Individually  
25 | Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and E.  
26 |

1           3.11 “MULTI-FACTOR AUTHENTICATION” means authentication through  
2 verification of at least two of the following authentication factors: (i) Knowledge factors, such  
3 as a password; or (ii) Possession factors, such a token or text message on a mobile phone; or (iii)  
4 Inherence factors, such as a biometric characteristic.

5           3.12 “MULTISTATE EXECUTIVE COMMITTEE” shall mean the Attorneys  
6 General of the States of Washington, Oregon, and California.

7           3.13 “PERSONAL INFORMATION” shall have the same meaning as listed in the  
8 SECURITY BREACH NOTIFICATION ACT.

9           3.14 “PREMERA” shall mean Premera Blue Cross, its parent and its directly or  
10 indirectly wholly-owned or controlled affiliates, subsidiaries and divisions, successors and  
11 assigns.<sup>1</sup>

12           3.15 “PREMERA NETWORK” shall mean all networking equipment, databases or  
13 data stores, applications, servers, and endpoints that are capable of using and sharing software,  
14 data, and hardware resources, and that are owned, operated, and/or controlled by PREMERA.

15           3.16 “PROTECTED HEALTH INFORMATION” shall mean “individually  
16 identifiable health information” as defined by the Health Insurance Portability and  
17 Accountability Act (HIPAA), as amended by the Health Information Technology and Clinical  
18 Act (HITECH) and 45 C.F.R. § 160.103.

19           3.17 “SECURITY BREACH NOTIFICATION ACT” shall mean the New Jersey  
20 Identity Theft Prevention Act, N.J.S.A. 56:8-161 to -166.

21           3.18 “SECURITY INCIDENT” shall mean any compromise to the confidentiality,  
22 integrity, or availability of a PREMERA information asset that includes PERSONAL  
23 INFORMATION or PROTECTED HEALTH INFORMATION.

24 \_\_\_\_\_  
25 <sup>1</sup> For purposes of this definition, “control” means the possession, directly or indirectly, of the power to  
26 direct or cause the direction of the management and policies of an entity through majority ownership or voting  
power.

1 **IV. INJUNCTIVE RELIEF**

2 4.1 Application of Injunctions. The injunctive provisions of this Final Consent  
3 Judgment shall apply to PREMERA and its officers, directors, and employees.

4 4.2 Injunctions. PREMERA shall engage in or refrain from engaging in the practices  
5 as identified in this Final Consent Judgment.

6 4.3 **COMPLIANCE WITH STATE AND FEDERAL LAW:**

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

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

10 c. PREMERA shall comply with HIPAA in connection with its collection,  
11 maintenance, and safeguarding of PROTECTED HEALTH INFORMATION.

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

16 4.4 **COMPLIANCE PROGRAM:**

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

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

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

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

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

10 f. PREMERA shall ensure that its Compliance Program continues to receive the  
11 resources and support necessary to ensure that the Compliance Program functions as required and  
12 intended by this Final Consent Judgment.

13 g. PREMERA may satisfy the implementation and maintenance of the Compliance  
14 Program and the safeguards required by this Final Consent Judgment through review, maintenance,  
15 and, if necessary, updating of an existing compliance program or existing safeguards, provided that  
16 such existing compliance program and existing safeguards meet the requirements set forth in this  
17 Final Consent Judgment.

18 **4.5 INFORMATION SECURITY PROGRAM:**

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

24 b. PREMERA shall implement, maintain, regularly review and revise, and comply  
25 with a comprehensive information security program ("Information Security Program") that is  
26 reasonably designed to protect the security, integrity, availability, and confidentiality of the

1 PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION that PREMERA  
2 collects, stores, transmits, and/or maintains.

3 c. PREMERA's Information Security Program shall document the administrative,  
4 technical, and physical safeguards appropriate to:

5 (i). The size and complexity of PREMERA's operations;

6 (ii). The nature and scope of PREMERA's activities; and

7 (iii). The sensitivity of the PERSONAL INFORMATION or PROTECTED  
8 HEALTH INFORMATION that PREMERA collects, stores, transmits, and/or maintains.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

24 i. PREMERA shall ensure that the Chief Information Security Officer and  
25 Information Security Program receive the resources and support necessary to ensure that the  
26 Information Security Program functions as intended by this Final Consent Judgment.

1 j. PREMERA shall ensure that employees who are responsible for implementing,  
2 maintaining, or monitoring the Information Security Program, including but not limited to the  
3 Chief Information Officer and Chief Information Security Officer, have sufficient knowledge of  
4 the requirements of the Final Consent Judgment.

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

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

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

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

- 21 (i). Preparation;
- 22 (ii). Investigation, Detection and Analysis;
- 23 (iii). Containment;
- 24 (iv). Notification and Coordination with Law Enforcement;
- 25 (v). Eradication;
- 26 (vi). Recovery;

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

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

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

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

14 **4.6 PERSONAL INFORMATION AND PROTECTED HEALTH**  
15 **INFORMATION SAFEGUARDS AND CONTROLS:**

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

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

25 **4.7 SPECIFIC TECHNICAL SAFEGUARDS AND CONTROLS:**

26 a. Asset Inventory and Managing Critical Assets:

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

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

18 b. Mapping and Encryption of Sensitive Data:

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

25 (ii). PREMERA shall ensure that electronic PERSONAL INFORMATION or  
26 PROTECTED HEALTH INFORMATION that is stored at rest or is in transmission is

1 ENCRYPTED except where PREMERA determines that ENCRYPTION is not reasonable and  
2 appropriate and it documents the rationale for this decision.

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

10 d. Penetration Testing: PREMERA shall engage a third-party vendor to perform an  
11 annual penetration test to the PREMERA NETWORK, and shall ensure any risks or  
12 vulnerabilities identified are risk assessed, prioritized, and addressed under PREMERA's  
13 Information Security Program. The parties understand and agree that addressing a risk may  
14 include remediation or alternate risk mitigation efforts based on the risk assessment in Paragraph  
15 4.7(e).

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

1 safeguarding or security of any PERSONAL INFORMATION or PROTECTED HEALTH  
2 INFORMATION maintained on the PREMERA NETWORK.

3 (i). The risk assessment shall include an accurate and thorough assessment of  
4 the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic  
5 protected health information held as required by HIPAA Security Rule, 45 C.F.R. §  
6 164.308(a)(1)(ii)(A).

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

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

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

25 (i). PREMERA shall, within nine (9) months of the EFFECTIVE DATE,  
26 implement and maintain appropriate controls to manage access to, and use of, all administrator,

1 service, and vendor accounts with access to PERSONAL INFORMATION or PROTECTED  
2 HEALTH INFORMATION. Such controls shall include, without limitation, (1) strong passwords,  
3 (2) password confidentiality policies, (3) password-rotation policies, (4) MULTI-FACTOR  
4 AUTHENTICATION or any other equal or greater authentication protocol for identity  
5 management, and (5) appropriate safeguards for administrative level passwords.

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

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

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

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

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

24 (vii). PREMERA shall regularly inventory the users who have access to the  
25 PREMERA NETWORK in order to review and determine whether or not such access remains  
26 necessary or appropriate. PREMERA shall regularly compare employee termination lists to user

1 accounts to ensure access privileges have been appropriately terminated. At a minimum, such  
2 review shall be performed on a quarterly basis. When the privileges, including for any disabled  
3 accounts, are determined to be no longer necessary for any business function, PREMERA shall  
4 terminate access privileges for those accounts.

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

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

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

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

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

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

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

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

## 16 V. ASSESSMENT AND REPORTING REQUIREMENTS TO THE ATTORNEY

### 17 GENERAL

#### 18 5.1 Information Security Assessment:

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

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

1 (ii). Explain the extent to which such safeguards are appropriate in light of  
2 PREMERA's size and complexity, the nature and scope of PREMERA's activities, and the  
3 sensitivity of the PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION  
4 maintained by PREMERA;

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

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

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

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

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

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

25 c. Each Third-Party Assessment must be completed within sixty (60) days after the  
26 end of the reporting period to which the Third-Party Assessment applies. PREMERA shall provide

1 a copy of the Third-Party Assessor's Report on the Third Party Assessment to the Washington  
2 Attorney General's Office within thirty (30) days of the completion of the report.

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

6 e. The Washington Attorney General's Office may provide a copy of the Third-Party  
7 Assessor's Report received from PREMERA to another Attorney General's Office upon request,  
8 and to the extent the New Jersey Office of the Attorney General receives a copy of said report, it  
9 shall, to the extent permitted by the laws of New Jersey, treat such Third-Party Assessor's Report  
10 as exempt from disclosure under the relevant public records laws.

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

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

19 b. The Compliance Program Assessor shall:

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

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

23 (iii). Identify any potential conflicts-of-interest that may hinder PREMERA's  
24 obligation to comply with state and federal laws related to data security and privacy; and  
25  
26

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 Office  
3 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  
12 Compliance Program Assessor's Report received from PREMERA to another Attorney  
13 General's Office upon request, and that Attorney General shall, to the extent permitted by the  
14 laws of New Jersey, treat such Compliance Program Assessor's Report as exempt from  
15 disclosure under 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 Consent Judgment for a period of no less than three (3)  
21 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 New Jersey Office of the Attorney General in an  
26

1 amount to be designated by and in the sole discretion of the MULTISTATE EXECUTIVE  
2 COMMITTEE. The distribution to New Jersey shall be \$72,168.10 in the form of a wire transfer  
3 within thirty (30) days of the EFFECTIVE DATE of this Final Consent Judgment. Said payment  
4 shall be used by the New Jersey Attorney General and/or New Jersey Division of Consumer  
5 Affairs for attorneys' fees and other costs of investigation and litigation; or to be placed in, or  
6 applied to, consumer protection enforcement funds, including future consumer protection  
7 enforcement, consumer education, litigation or local consumer aid fund or revolving fund, used  
8 to defray the costs of the inquiry leading hereto, or for any lawful purpose, at the sole discretion  
9 of the New Jersey Office of the Attorney General and the New Jersey Division of Consumer  
10 Affairs.  
11

### 12 13 **VIII. RELEASE**

14 8.1 Following full payment of the amount due under this Final Consent Judgment, the  
15 Plaintiffs shall release and discharge PREMERA from all civil claims that the Attorney General  
16 has or could have brought under New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 et seq., the  
17 New Jersey Identity Theft Prevention Act, N.J.S.A. 56:8-161 to -166, and the Health Insurance  
18 Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by  
19 the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5,  
20 123 Stat. 226, as well as the Department of Health and Human Services ("HHS") Regulations,  
21 45 C.F.R. §§ 160 et seq. arising out of PREMERA's conduct and the Attorney General's  
22 investigation of the data security incident first publicly announced March 17, 2015. Nothing  
23 contained in this paragraph shall be construed to limit the ability of the Plaintiffs to enforce the  
24 obligations that PREMERA has under this Final Consent Judgment. Further, nothing in this Final  
25 Consent Judgment shall be construed to create, waive, or limit any private right of action or any  
26 action brought by any state agency other than the Attorney General.



1 requiring immediate action, the Attorney General will notify PREMERA in writing of such  
2 failure to comply and PREMERA shall have thirty (30) days from receipt of such written notice  
3 to provide a good faith written response to that Attorney General, including either a statement  
4 that PREMERA believes it is in full compliance or otherwise a statement explaining how the  
5 violation occurred, how it has been addressed or when it will be addressed, and what PREMERA  
6 will do to make sure the violation does not happen again. The Attorney General may agree to  
7 provide PREMERA more than thirty (30) days to respond.

8 9.2 Nothing herein shall be construed to exonerate any failure to comply with any  
9 provision of this Final Consent Judgment, or limit the right and authority of an Attorney General  
10 to initiate a proceeding for any failure to comply with this Final Consent Judgment after receiving  
11 the response from PREMERA described in Paragraph 9.1, if the Attorney General determines  
12 that an enforcement action is in the public interest.

#### 13 X. ENFORCEMENT

14 10.1 Violation of any of the injunctions contained in this Final Consent Judgment, as  
15 determined by the Court, shall constitute a violation of an injunction for which civil penalties  
16 may be sought by the Attorney General pursuant to N.J.S.A. 56:8-14.

17 10.2 This Final Consent Judgment is entered pursuant to N.J.S.A. 56:8-8 and N.J.S.A.  
18 56:8-13. Jurisdiction is retained for the purpose of enabling any party to this Final Consent  
19 Judgment with or without the prior consent of the other party to apply to the Court at any time  
20 for enforcement of compliance with this Final Consent Judgment, to punish violations thereof, or  
21 to modify or clarify this Final Consent Judgment.

22 10.3 Under no circumstances shall this Final Consent Judgment or the name of the State  
23 of New Jersey, the Office of the Attorney General, Consumer Protection Division, or any of their  
24 employees or representatives be used by PREMERA in connection with any selling, advertising,  
25 or promotion of products or services, or as an endorsement or approval of PREMERA's acts,  
26 practices or conduct of business.

1           10.4 Nothing in this Final Consent Judgment shall be construed to limit the authority  
2 or ability of the New Jersey Office of the Attorney General to protect the interests of New Jersey  
3 or the people of New Jersey. This Final Consent Judgment shall not bar the New Jersey Attorney  
4 General, the New Jersey Division of Consumer Affairs or any other governmental entity from  
5 enforcing laws, regulations, or rules against PREMERA for conduct subsequent to or otherwise  
6 not covered by this Final Consent Judgment. Further, nothing in this Final Consent Judgment shall  
7 be construed to limit the ability of the Plaintiffs to enforce the obligations that PREMERA has  
8 under this Final Consent Judgment.

9           10.5 Nothing in this Final Consent Judgment shall be construed as relieving  
10 PREMERA of the obligation to comply with all state and federal laws, regulations, and rules,  
11 nor shall any of the provisions of this Final Consent Judgment be deemed to be permission to  
12 engage in any acts or practices prohibited by such laws, regulations, and rules.

13           10.6 PREMERA shall deliver a copy of this Final Consent Judgment to, and otherwise  
14 fully apprise, its Chief Executive Officer, Chief Information Officer, Chief Information Security  
15 Officer, Compliance Officer, DESIGNATED PRIVACY OFFICIAL, DESIGNATED  
16 SECURITY OFFICIAL, Chief Legal Officer, and its Board of Directors within (30) days of the  
17 EFFECTIVE DATE. If PREMERA hires or replaces any of the above listed officers, counsel  
18 or Directors, PREMERA shall deliver a copy of this Final Consent Judgment to their  
19 replacements within thirty (30) days from the date on which such person assumes his/her position  
20 with PREMERA.

21           10.7 PREMERA shall not participate in any activity or form a separate entity or  
22 corporation for the purpose of engaging in acts or practices in whole or in part that are prohibited  
23 by this Final Consent Judgment or for any other purpose that would otherwise circumvent any  
24 term of this Final Consent Judgment. PREMERA shall not knowingly cause, permit, or  
25 encourage any other persons or entities acting on its behalf, to engage in practices prohibited by  
26 this Final Consent Judgment.

1           10.8   PREMERA agrees that this Final Consent Judgment does not entitle it to seek or  
2 to obtain attorneys' fees as a prevailing party under any statute, regulation, or rule, and  
3 PREMERA further waives any right to attorneys' fees that may arise under such statute,  
4 regulation, or rule.

5           10.9   This Final Consent Judgment shall not be construed to waive any claims of  
6 sovereign immunity New Jersey may have in any action or proceeding.

7           10.10 If any portion of this Final Consent Judgment is held invalid by operation of law,  
8 the remaining terms of this Final Consent Judgment shall not be affected and shall remain in full  
9 force and effect.

10          10.11 Whenever PREMERA shall provide reports to the Washington Attorney  
11 General under Section V of this Final Consent Judgment, those requirements shall be satisfied by  
12 sending the report to: ATTN: Tiffany Lee and Andrea Alegrett, Assistant Attorney General,  
13 Consumer Protection Division, Office of the Attorney General, 800 Fifth Avenue #2000, Seattle,  
14 WA 98104.

15          10.12 Any notice or report provided by the Attorney General to PREMERA under  
16 Section IX of this Final Consent Judgment shall be satisfied by sending notice to: Chief Legal  
17 Officer, Premera Blue Cross, 7001 220th St., SW, MS 316, Mountlake Terrace, WA 98043.

18          10.13 All documents to be provided under this Final Consent Judgment shall be sent by  
19 United States mail, certified mail return receipt requested, or other nationally recognized courier  
20 service that provides for tracking services and identification of the person signing for the notice  
21 or document, and shall have been deemed to be sent upon mailing. The parties may update their  
22 designee or address by sending written notice to the other party informing it of the change.

23          10.14 Jurisdiction is retained by the Court for the purpose of enabling any party to the  
24 Final Consent Judgment to apply to the Court at any time for such further orders and directions  
25 as may be necessary or appropriate for the construction or the carrying out of this Final Consent  
26 Judgment, for the modification of any of the injunctive provisions hereof, for enforcement of

1 compliance herewith, and for the punishment of violations hereof, if any.

2 10.15 The clerk is ordered to enter this Final Consent Judgment forthwith.

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

4 11.1 Upon entry of this Final Consent Judgment, all claims in this matter, not otherwise  
5 addressed by this Final Consent Judgment are dismissed.

6  
7 **IT IS ON THE \_\_\_\_\_ DAY OF \_\_\_\_\_, 2019 SO ORDERED, ADJUDGED,**  
8 **AND DECREED.**

9  
10 \_\_\_\_\_  
11 HON. PAUL INNES, P.J. Ch.

12 JOINTLY APPROVED AND SUBMITTED  
13 FOR ENTRY:

14 FOR PLAINTIFFS:

15 GURBIR S. GREWAL  
16 ATTORNEY GENERAL OF NEW JERSEY

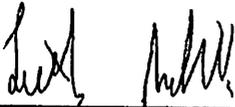
17 By: Elliott M. Siebers

17 Dated: July 11, 2019

18 Elliott M. Siebers  
19 Deputy Attorney General  
20 State of New Jersey  
21 124 Halsey Street  
22 P.O. Box 45029  
23 Newark, NJ 07101  
24 (973)648-4846  
25 elliot.siebers@law.njoag.gov  
26 Atty. ID #033582012

1 FOR DEFENDANT, PREMIERA BLUE CROSS:

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

By:  \_\_\_\_\_ Dated: 7/10/19, 2019  
Tim McMichael  
Assistant General Counsel – Director of Litigation / SI  
Premera Blue Cross

COUNSEL FOR DEFENDANT, PREMIERA BLUE CROSS

By:  \_\_\_\_\_ Dated: 7/10/2019  
THEODORE J. KOBUS III  
Baker & Hostetler LLP  
45 Rockefeller Plaza  
New York, NY 10111-0100  
  
PATRICK H. HAGGERTY  
Baker & Hostetler LLP  
312 Walnut St., Suite 3200  
Cincinnati, OH 45202