COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 8. August 07, 2019 In Sign of Growing State Might, Premera Pays $10M to 30 AGs, $74M to Resolve Class Action

By Theresa Defino

July was one hot month for Premera Blue Cross, and not because of the weather. The plan, which has two million members in Alaska and Washington State, offered the privacy and security compliance community yet another example of the threat of enforcement for HIPAA violations that can come from state officials, as well as demonstrating the financial pain of settling now-routine class action suits.

Premera now ranks near the top in quantifiable costs associated with a privacy or security breach, after Anthem, which resolved its class actions suit by committing to $115 million in payments and expenditures, followed by a $16 million settlement with the HHS Office for Civil Rights (OCR). Although Anthem also entered into an agreement with a group of states, corrective actions were required but no payment was made ("OCR Exacts Its Pound of Flesh From Anthem With $16 Million Settlement, Corrective Actions," *RPP* 18, no. 11).

Premera may not be quite out of the woods yet in terms of enforcement actions. The third of the triple threat to covered entities and business associates—fines imposed by OCR—has yet to emerge for Premera.

Plan officials did not answer *RPP*'s question as to whether enforcement action was expected by OCR; the agency has a policy of not commenting on whether it is or is not conducting a compliance investigation. But if the Anthem example holds, OCR may yet collect fines and require corrective actions even if the states and class action attorneys have already done the same.

Led by Washington, the other states in the settlement are Alabama, Alaska, Arizona, Arkansas, California, Connecticut, Florida, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiana, Massachusetts, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Jersey, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Rhode Island, Utah and Vermont.

Washington state will receive more than half of the 10 million settlement—$5.4 million to be exact—while the other states will receive the balance. Washington will use its funds for the "continued enforcement of state data security and privacy laws."

Corrective Actions Run the Gamut

As announced by Washington State AG Bob Ferguson, the settlement calls for Premera to do the following:

- "Ensure its data security program protects personal health information as required by law
- Regularly assess and update its security measures
- Map where HIPAA-protected information, including personal health information, is located on the

Premera network

- Provide data security reports, completed by a third-party security expert approved by the multistate coalition, to the Washington State Attorney General's Office
- Hire a chief information security officer, a separate position from the chief information officer. The information security officer must be experienced in data security and HIPAA compliance and will be responsible for implementing, maintaining and monitoring the company's security program.
- Hold regular meetings between the chief information security officer and Premera's executive management. The information security officer must meet with Premera's CEO every two months and inform the CEO of any unauthorized intrusion into the Premera network within 48 hours of discovery.
- Create a compliance program and hire a compliance officer with a background in HIPAA compliance
- Map where HIPAA-protected information, including personal health information, is located on the Premera network
- Provide security training to all employees who handle personal information and protected health information."

Dani Chung, Premera spokesperson, sent *RPP* the following statement in response to the state attorneys' settlement.

> "We are pleased to have reached an agreement with state attorneys general to resolve legal inquiries into the 2014 cyberattack on our data network. The commitments we have agreed to are consistent with our ongoing focus on protecting personal customer information.
>
> Premera takes the security of its data and the personal information of its customers seriously and has worked closely with state attorneys general, regulators and their information security experts, since the attack was made public in 2015. It is important to note that independent investigators have made no determination that any customer information was removed from Premera's systems.
>
> Premera continues to enhance its cybersecurity programs and practices, achieving an industry-leading HITRUST certification in 2018. To achieve certification, Premera demonstrated its ability to identify risks, protect assets, detect attacks, and respond and restore capabilities should the need arise."

Two More Years of Credit Monitoring

Ferguson's announcement of the attorneys general settlement noted that the class action agreement "provides for additional relief for affected individuals."

The class action attorneys and Premera jointly issued a statement after resolving the suit, which pointed out that it calls for Premera to pay "$32 million to resolve the litigation. Those funds will pay for an additional two years of premium credit monitoring, and identity protection services, out-of-pocket losses, and cash payments to all class members who make a claim. The fund also will pay for administrative and notice costs related to the settlement, including attorneys' fees. The benefits will not be available until the settlement has been finally

approved by the Court and any appeals have been concluded."

Like the $115 million Anthem class action settlement, Premera's agreement requires it to spend millions on corrective actions, as part of "comprehensive remedial measures and injunctive relief in the form of business practice changes and future commitments related to Premera's IT security practices." Unlike Anthem's list, nothing appears to be redacted from Premera's requirements, which span a three-year settlement period ("Six Lessons From Anthem's Pricey, Record-Setting Breach Settlements," *RPP* 19, no. 6).

In each of the three years of the class action settlement, Premera is to spend "at least" $14 million a year "on core cybersecurity operations, investments, and initiatives whose primary purpose is to improve or maintain information protection." The settlement doesn't say how much of an increase, if any, the $14 million is over what Premera currently spends.

Data Segmentation Among the Requirements

The settlement includes four pages of 14 numbered actions, some of them multipart, that Premera has agreed to undertake, such as "data protection steps" and encryption and remediation of vulnerabilities. Documents related to the settlement are posted at http://bit.ly/2LZ9yvF.

The following are highlights of the actions Premera must take during the three-year settlement period of the class action settlement.

- "Place data that have not been accessed for three-to-five years in a separate, secured, logically air-gapped environment. Accessing claims data stored this way will require "levels of management and, as appropriate, legal approval."
- "Conduct adversarial simulations at least once per year [for three years] to include simulation of compromised privileged credentials for both the network and database systems."
- "Collect and maintain logs of covered information systems in real-time, allowing for processing and aggregation of logs in the security device chain as follows: Premera will maintain logs for a period of one (1) year in an active state; and Premera will maintain logs in a cold state for years two (2) and three (3). Premera will document and account for any periods of outage. Covered information systems include all servers and infrastructure involved in the protection of PII and PHI, including Intrusion Detection Systems, database activity monitoring systems, authentication systems, firewalls, and other end user access control systems. Premera will enlist a third-party assessor to ascertain compliance with this requirement."

In response to the class action settlement, Mark Gregory, Premera's executive vice president and chief information officer, indicated the plan was eager to move forward from the 2015 breach.

"We are pleased to be putting this litigation behind us, and to be providing additional substantial benefits to individuals whose data was potentially accessed during the cyberattack," he said in a statement. "Premera takes the security of its data and the personal information of its customers seriously and has worked closely with state and federal regulators and their information security experts.''