COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 10. October 08, 2020 Failure to Plug Security Gaps Leads to Large OCR Settlements for Premera, CHSPSC

By Jane Anderson

A large covered entity and a CE-affiliated business associate (BA) each paid multimillion-dollar settlements and agreed to two-year corrective action plans following prolonged cyberattacks that resulted in huge breaches.

The payments—$6.85 million from insurer Premera Blue Cross over a 2015 data breach[1] and $2.3 million from CHSPSC LLC,[2] an affiliate of Community Health Systems Inc., over a 2014 data breach—came as part of a flurry of breach settlements from the HHS Office for Civil Rights (OCR) in September.

At the same time as the OCR settlements, Anthem Inc. reached a $39.5 million settlement with 43 state attorneys general over a 2014 data breach, in which it also agreed to implement comprehensive security measures.[3]

In both the Premera case and the CHSPSC case, OCR found what it termed systemic longstanding issues of noncompliance with the HIPAA security rule. In Premera's case, the insurer had been warned about security issues but failed to take action, OCR said, while in CHSPSC's case, the company had received a warning from the FBI about a potential hack, but failed to step in quickly to stop it.

Premera's OCR Pact Follows States, Class Action

The Premera Blue Cross settlement, signed by both parties in March but only released in September, represents the second-largest payment to resolve a HIPAA investigation in OCR history.[4] Premera, which operates in Washington and Alaska, is the largest health insurer in the Pacific Northwest.

Premera filed a breach report in March 2015 stating that cyberattackers had gained unauthorized access to its information technology (IT) system. The hackers used a phishing email to install malware that gave them access to Premera's system in May 2014, and the breach went undetected for nearly nine months, until January 2015.

As a result, the hacker was able to access sensitive personal information, including private health information, Social Security numbers, bank account information, names, addresses, phone numbers, dates of birth, member identification numbers and email addresses.

OCR's investigation found "systemic noncompliance with the HIPAA rules including failure to conduct an enterprise-wide risk analysis, and failures to implement risk management, and audit controls," according to the settlement announcement.

"This case vividly demonstrates the damage that results when hackers are allowed to roam undetected in a computer system for nearly nine months," OCR Director Roger Severino said in a statement.

According to an investigation by Washington State Attorney General Bob Ferguson that concluded in mid-2019, the hacker "took advantage of multiple known weaknesses in Premera's data security. For years prior to the breach, cybersecurity experts and the company's own auditors repeatedly warned Premera of its inadequate security program, yet the company accepted many of the risks without fixing its practices."[5]

After the breach became public, Premera's call center agents told consumers that there was "no reason to believe that any of your information was accessed or misused." Call center agents also told consumers that "there were already significant security measures in place to protect your information," despite the internal warnings from IT experts, the Washington attorney general's office found.