OCR announces second-largest HIPAA breach settlement

September 28, 2020

On September 25, 2020, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) announced that it reached a settlement with Premera Blue Cross (PBC), a health plan operating in Washington and Alaska, related to a cyber attack on its information technology system. PBC agreed to pay $6.85 million, the second-largest payment to resolve a HIPAA investigation in OCR history.

OCR became aware of the incident when PBC filed a breach report on March 17, 2015. The report indicated that hackers had used a phishing email to install malware that gave them access to PBC's IT system in May 2014. The unauthorized access went undetected until January 2015. This attack, which is also known as an "advanced persistent threat," resulted in the disclosure 10.4 million individuals' protected health information. The information disclosed included names, addresses, dates of birth, email addresses, Social Security numbers, clinical information and bank account information.

Upon receipt of the breach report, OCR launched an investigation which uncovered "systemic noncompliance with the HIPAA Rules." This included failures to conduct enterprise-wide risk analyses, to implement risk management, and to utilize audit controls. OCR Director Roger Severino stated, "[i]f large health insurance entities don't invest the time and effort to identify their security vulnerabilities, be they technical or human, hackers surely will. This case vividly demonstrates the damage that results when hackers are allowed to roam undetected in a computer system for nearly nine months."

In addition to the monetary settlement, PBC agreed to adopt a corrective action plan with two years of monitoring by OCR. Last year, PBC settled a $10 million lawsuit with 30 states related to the breach and settled a class action brought by affected customers for $74 million. Anthem's $16 million OCR settlement announced in 2015 remains the largest on record.

There are at least two important takeaways from this settlement for all HIPAA covered entities. First, the settlement should serve as a reminder of the importance of risk analysis and management. Had PBC conducted a risk analysis and taken steps to manage identified risks, it might have prevented the attack or discovered it sooner. Second, covered entities need to be aware that, once they report a breach and OCR launches an investigation, all aspects of their HIPAA compliance program will be under the microscope. The large settlement amount reflects not only the seriousness of the breach itself but also the "systemic noncompliance" that OCR uncovered through its investigation. Covered entities should regularly audit their compliance programs – whether they do so themselves or engage a third party – to ensure that they are in compliance with all aspects of the rules.

Authors