Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History

This is a HIPAA Settlement Announcement

Final

Issued by: Office for Civil Rights (OCR)

Issue Date: July 10, 1905

Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History

Anthem, Inc. has agreed to pay $16 million to the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) and take substantial corrective action to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules after a series of cyberattacks led to the largest U.S. health data breach in history and exposed the electronic protected health information of almost 79 million people.

The $16 million settlement eclipses the previous high of $5.55 million paid to OCR in 2016.

Anthem is an independent licensee of the Blue Cross and Blue Shield Association operating throughout the United States and is one of the nation's largest health benefits companies, providing medical care coverage to one in eight Americans through its affiliated health plans. This breach affected electronic protected health information (ePHI) that Anthem, Inc. maintained for its affiliated health plans and any other covered entity health plans.

On March 13, 2015, Anthem filed a breach report with the HHS Office for Civil Rights detailing that, on January 29, 2015, they discovered cyber-attackers had gained access to their IT system via an undetected continuous and targeted cyberattack for the apparent purpose of extracting data, otherwise known as an advanced persistent threat attack. After filing their breach report, Anthem discovered cyber-attackers had infiltrated their system through spear phishing emails sent to an Anthem subsidiary after at least one employee responded to the malicious email and opened the door to further attacks. OCR's investigation revealed that between December 2, 2014 and January 27, 2015, the cyber-attackers stole the ePHI of almost 79 million individuals, including names, social security numbers, medical identification numbers, addresses, dates of birth, email addresses, and employment information.

"The largest health data breach in U.S. history fully merits the largest HIPAA settlement in history," said OCR Director Roger Severino. "Unfortunately, Anthem failed to implement appropriate measures for detecting hackers who had gained access to their system to harvest passwords and steal people's private information." Director Severino continued, "We know that large health care entities are attractive targets for hackers, which is why they are expected to have strong password policies and to monitor and respond to security incidents in a timely fashion or risk enforcement by OCR."

In addition to the impermissible disclosure of ePHI, OCR's investigation revealed that Anthem failed to conduct an enterprise-wide risk analysis, had insufficient procedures to regularly review information system activity, failed to identify and respond to suspected or known security incidents, and failed to implement adequate minimum access controls to prevent the cyber-attackers from accessing sensitive ePHI, beginning as early as February 18, 2014.

In addition to the $16 million settlement, Anthem will undertake a robust corrective action plan to comply with the HIPAA Rules. The resolution agreement and corrective action plan may be found on the OCR website at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/anthem/index.html.

HHS is committed to making its websites and documents accessible to the widest possible audience, including individuals with disabilities. We are in the process of retroactively making some documents accessible. If you need assistance accessing an accessible version of this document, please reach out to the guidance@hhs.gov.

Topic(s)

Health Care

Unique ID:
HHS-0945-1905-F-7395

Date Published: 6/8/2020

Return to top

Português

Italiano

فارسی

English