

Anthem Will Pay Record \$16 Million To Settle Health Care Data Breach

By James A. Hoover

October 2018

Reprinted with Permission from the [Birmingham Medical News](#)

Anthem, Inc., the country's second largest insurer has agreed to pay \$16 million to the U.S. Department of Health and Human Services, Office for Civil Rights ("OCR") and take corrective action to settle potential violations of the Health Insurance Portability and Accountability Act ("HIPAA") Privacy and Security Rules. The \$16 million settlement significantly surpasses the previous settlement high of \$5.55 million paid to OCR in 2016. "The largest health data breach in U.S. history fully merits the largest HIPAA settlement in history," OCR Director Roger Severino said.

The potential violations stemmed from 2015 cyberattacks that resulted in names, dates of birth and social security numbers being accessed by hackers. The hackers spear-phished a single employee and gained access to the company's system. The cyberattacks led to the largest U.S. health data breach in history and exposed the electronic protected health information ("ePHI") of almost 79 million people.

On March 13, 2015, Anthem filed a breach report with OCR disclosing that, on January 29, 2015, it discovered cyber-attackers had gained access to Anthem's IT system. 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 Office of Civil Rights also determined 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.

Anthem previously settled with consumers in June 2017 over the massive breach by paying \$115 million, a record deal for private civil claims from data breaches, paying the out-of-pocket expenses customers' incurred due to the breach and agreeing to provide two years of credit monitoring.

Anthem admitted no liability as a result of the settlement, which comes in lieu of fines HHS could have imposed.

The resolution agreement and corrective action plan may be found on the OCR website [here](#).

For more information, please contact:



James A. Hoover

Partner

Birmingham, AL

Phone (205) 458-5111

E-Mail jhoover@burr.com

Jim Hoover is a partner at Burr & Forman LLP and practices exclusively in the healthcare industry group.