COSMOS
Navigate the Compliance Universe

Compliance Today - October 2019
Incident response: Best practices in breach management

By Rita Bowen, MA, RHIA, CHPS, CHPC, SSGB, and Melissa Landry, RHIA

Rita Bowen (rbowen@mrocorp.com) is Vice President, Privacy, Compliance and HIM Policy, MRO in Norristown, PA.

Melissa Landry (melandry@ochsner.org) is Assistant Vice President, Health Information Management, Ochsner Health System in Jefferson Parish, LA.

In February 2019, the Health and Human Services (HHS) Office for Civil Rights (OCR) announced an all-time record year in Health Insurance Portability and Accountability Act (HIPAA) enforcement activity. In 2018, OCR settled ten cases and was granted summary judgment in a case before an administrative law judge, together totaling $28.7 million from enforcement actions. This total surpassed the previous record of $23.5 million from 2016 by 22%. In addition, OCR achieved the single largest individual HIPAA settlement in history of $16 million with Anthem Inc., representing a nearly three-fold increase over the previous record settlement of $5.5 million in 2016.[1]

The Anthem breach affected electronic protected health information (ePHI) that was maintained for affiliated health plans and any other covered entity health plans. The breach report filed with the OCR indicated that cyberattackers had gained access to the insurance company's IT system via an undetected, continuous, and targeted cyberattack for the apparent purpose of extracting data, otherwise known as an advanced persistent threat attack. It was later determined that cyberattackers had infiltrated the company's system through spear phishing emails sent to a subsidiary after at least one employee responded to the malicious email and opened the door to further attacks.

The OCR investigation revealed that between December 2, 2014 and January 27, 2015, the cyberattackers 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. Further, the investigation revealed the following risk factors that contributed to such a massive data breach:

- Failure to conduct an enterprise-wide risk analysis,
- Insufficient policies and procedures to regularly review information system activity,
- Failure to identify and respond to suspected or known security incidents, and
- Failure to implement adequate minimum access controls to prevent the cyberattackers from accessing sensitive ePHI.