COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 1. January 31, 2019 2018 Closes With Spike in Loss of PHI From Ransomware, Phishing Breaches

By Theresa Defino

Breaches of protected health information (PHI) from phishing and ransomware continued to rack up as 2018 drew to a close, with covered entities (CEs) and business associates (BAs) in Georgia, Illinois, Michigan, California and New York reporting attacks.

In fact, Beazley Breach Response Services, which works with companies insured by the Beazley Group that suffer breaches, said in a recent report that attacks using a variety of ransomware variants spiked in the third quarter of 2018 across all industries.

Among breaches of PHI reported in late 2018, many involved ransomware and phishing. They included:

- Mind and Motion Developmental Centers of Georgia, based in Suwanee, said that up to 16,000 patient records had been exposed following a ransomware attack discovered Sept. 30. Forensic investigators also discovered an inactive keylogger and spam emailer on the system following the breach, which involved names, addresses, Social Security numbers and medical records, the company said.

- The Center for Vitreo-Retinal Diseases in Des Plaines, Illinois, said its servers were hit by a ransomware attack on Sept. 18, potentially affecting 20,371 patients. There was no indication the hacker downloaded information, but the center said unauthorized third parties could have viewed or accessed patient records.

- New York Oncology Hematology (NYOH) in Albany reported that an unauthorized user might have gained access to up to 14 employee email accounts through a series of targeted phishing attacks, resulting in the possible breach of protected information for more than 128,400 patients and employees. “The phishing emails sent were sophisticated in that they appeared as a legitimate email login page, which convinced the NYOH personnel to enter their user names and passwords,” the cancer center reported.

- Redwood Eye Center, based in Vallejo, California, said that IT Lighthouse, the third-party vendor that hosts and stores its electronic medical records, experienced a ransomware attack that locked its patient records, potentially exposing data from some 16,000 patients. There’s no evidence that the information was accessed, however.