HealthManagement
Promoting Management and Leadership

Insiders cause most data security breaches

The latest Protenus breach barometer shows this year's security trend remained true for October – i.e., at least one breach occurs in the healthcare sector each day. That month a total of 37 breaches were reported, based on data Protenus gathered from the U.S. Department of Health and Human Services' Office of Civil Rights, as well as research from the site DataBreaches.net.

Insider error continues to be a problem area for the industry. Although insiders accounted for 29 percent of all breaches in October, Protenus researchers note that insider errors impacted an even greater amount of patient records. For instance, of the three insider breaches for which Protenus had data, user error caused the breach of about 157,000 patient records that month. This represents a drastic increase from other months, September breached just 24,958 records and August affected 26,831.

Notably, one of those insider errors involved a flyer sent to HIV patients, asking them to participate in an HIV research project. The trouble was that the healthcare organisation used envelopes with a clear front that revealed the HIV status. This was the second breach of this kind this year.

Another insider incident involved another troubling trend this year: an improperly secured Amazon S3 bucket. That incident breached the records of about 150,000 patients.

"These incidents serve as a reminder for healthcare organizations to conduct routine training for employees on how to properly handle and distribute information to patients, without breaching their privacy," the report authors write.

"This is especially the case when working with vulnerable populations, as patients with diagnoses like HIV have a lot more at stake if their information is made public -- much more sensitive than their credit card information, such a breach be catastrophic to their entire way of life," they add.

According to the report, hacking is still the healthcare industry's other leading culprit, accounting for about 35 percent of incidents and the breach of over 56,000 patient records. Two of the 13 incidents in October specifically mentioned ransomware, while two were caused by phishing and three mentioned extortion attempts. Data revealed that notorious hacker TheDarkOverLord was responsible for all the extortion attempts. Further, not all of the affected organisations have reported these breaches.

Another finding that may be a cause of concern: the industry continues to struggle with discovering breaches. It took an average of 448 days for an organisation to find a breach. In fact, one incident took 1,157 days or more than three years to discover a breach.

"Both external and internal actors continue to threaten patient information and these breaches have often gone undetected for years, affecting thousands of patients," the report authors write. "Our hope is that healthcare will begin to have conversations on how the industry can better protect the privacy of all patients and specifically devote attention to vulnerable populations."

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Sun, 3 Dec 2017