Codify
BY AAPC

Health Information Compliance Alert

Case Study: Patient Data Breaches Skyrocket in First Half of 2019

More than 32 million patients have had their data compromised.

If you thought 2018 was a busy year for healthcare hackers, think again. If current data breach trends continue, 2019 will be one for the ages.

Background: Breach statistics suggest that healthcare is taking a beating so far in 2019. The healthcare data analytics giant, **Protenus Inc**, tracks data breach reporting using artificial intelligence (AI) and recently released a report in coordination with databreaches.net titled The 2019 Mid-Year Breach Barometer - and the numbers aren't pretty. From January to June 2019, there were 285 incidents; moreover, the 240 that were disclosed impacted 31,611,235 individuals' protected health information (PHI), according to Protenus.

Important: The 2019 healthcare breachfest is shocking for two reasons. First, data security incidents are on the rise, highlighting how vulnerable the industry is to cyber attack. Second, the huge number of affected patients' records just in the first half of this year is "more than double what the industry experienced throughout the entire year of 2018," notes the report.

Consider the Breach Stats

Hacking ranks as the overarching cause of the spike in lost electronic PHI (ePHI). In fact, 88 percent of the incidents were due to hacking in the first half of 2019 and included 168 breaches of the overall total, indicates Protenus. The additional 12 percent of breaches impacted paper records.

Who: The report shows that healthcare providers are the most endangered entities and took the biggest hit, accounting for 72 percent of the data outages. Business associates (BAs) were attributed with 9 percent while health plans added 11 percent to the incident log. Another 8 percent of breaches weren't categorized by entity type.

What: Insider threats due to human error and wrongdoing as well as the general theft of records factored in the numbers, Protenus notes. But cyber crime caused the majority of the breaches, and the hacks covered the spectrum of attacks from ransomware or malware attack to phishing and even extortion, relates the brief.

Here's Why Network Servers Are So Vulnerable

If you've scoped out the last six months of data breaches listed on the **HHS Office for Civil Rights** (OCR) breach portal, then you know that a majority of the biggest security incidents list "hacking/IT incident - network server" as the reason for the breach.

"The reason we're seeing 'network server' next to so many breaches is because that's where large amounts of PHI data is stored - on a server that is located within the organization's network, in a database or fileshare," advises **Jen Stone, MSCIS, CISSP, QSA**, a security analyst with **Security Metrics** in Orem, Utah.

Stone breaks down how the server works in a traditional setup:

- The server is the physical hardware;
- a fileshare is the logical partition on that server being used by individuals to store files;
- and a database is a structured set of data - again, residing on a server.

Because so much of an organization's information is stored on its network servers, they are a liability and ripe for cyber attacks. "Network servers are great targets for hackers because they can count on stealing a lot of information at one

time from a server, while there might only be a subset of that information on a laptop, and only be a few records in an email," explains Stone.

This kind of entry into a practice's records allows cyber thugs to wreak all kinds of havoc. "If a hacker can gain access to an organization's network, they can make their way to a network server and export the data stored there - or a copy of the data - to a server outside the organization's network, and under the hacker's control," Stone warns.

Over 20 Million Impacted in Biggest Breach of 2019… So Far

In an unusual turn of events, a breach lingered between August 2018 and March 2019 on the payments' page of the **American Medical Collection Agency** (AMCA), but the organization never realized the security incident - until patients' data showed up for sale on the dark web.

The third-party biller's breach has impacted more than 20 million individuals at 21 different companies so far, including **LabCorp** and **Quest Diagnostics**. According to breach alerts, patients' personal data was exposed in the security incident.

"Multiple class action lawsuits have been filed against Quest and LabCorp," says attorney **Christina Seda-Acosta**, with New York firm **Patterson Belknap Webb & Tyler LLP** in the Data Security Law Blog.

Seda-Acosta writes, "A number of the suits contend that defendants failed to safeguard patient information" as required under HIPAA, "exposing customers to fraud and identity theft."

AMCA filed for bankruptcy in June. No word is out on whether any of the agency's associates will follow suit.

Health Information Compliance Alert will continue to update on this story in future issues.

Tip: Though healthcare remains a focus point for hackers, practices can use their risk assessments to look at network server issues. There are perennial problems to look for, Stone suggests. "Network vulnerabilities I see regularly include unpatched systems, shared account credentials, remote access to ePHI that only requires a username and password (no multi-factor authentication), and insufficient malware protection."