Statistically, What’s the Chance of a Breach?

Save to myBoK

By Lou Ann Wiedemann, MS, RHIA, CHDA, CDIP, FAHIMA

According to the Department of Health and Human Services Office for Civil Rights (OCR), from January 2016 to November 2016 approximately 169,013,996 people were affected by 1,737 healthcare breaches. The Ponemon Institute estimates that data breaches could cost the healthcare industry as much as $6.2 billion annually.

New technologies, revised workflow processes, and changes to business practices commanded much of 2016. Information governance, Big Data, healthcare hacking, ransomware, and the Internet of Things impacted business models and organizational cultures across the US. As a result, privacy and security functions often struggled to keep up in this fast paced world of change. Given all the data, statistically, what is the chance an organization will have a breach in 2017?

Better Safe than Sorry

Healthcare privacy and security are fundamental concepts in the industry today. When adding in the focus on information governance (IG), organizations and providers alike are examining ways to enhance their safeguards. Now is the time for privacy and security officers to begin actively looking into more ways to protect patient portals, electronic health records, medical apps, data entry points, and all of the other information resources the organization relies upon.

The Ponemon Institute data on breaches offers a stark warning that the threat is real for all healthcare organizations:[1]

- 50 percent of breaches are the result of a criminal attack
- 56 percent of organizations do not think their incident response process is adequately funded
- 38 percent of all breaches relate to medical identify theft in some fashion
- Only 19 percent of organizations have a process in place to correct health records after a breach has been identified
- 69 percent of organizations report employee negligence as a primary concern

With no obvious end to data breaches in sight, statistics such as these are likely to continue. Healthcare hacking is at an all-time high, producing breaches of network servers that affect thousands of patients at one time. Portable workstations such as laptops are easy targets for theft. And don’t forget paper records. Many organizations continue to maintain paper records—most likely in offsite storage units where safeguarding information becomes more difficult than when records are kept onsite. Although it is difficult to walk out of a storage facility with thousands of records, the data within the record continues to meet a need for crafty criminals.

Value of Healthcare Data Rising

Cyber attacks involving hacking, phishing, and viruses continue to reach further into the healthcare sector as the value of healthcare data increases. Health records are extremely attractive to cyber criminals given the amount of sensitive data contained in each record. Data such as insurance information, Social Security numbers, phone numbers, date of birth, and zip codes are sometimes all a criminal needs to profit off the information. Cybersecurity vulnerabilities shook up the industry in 2016 and organizations want to ensure that current policies and procedures reflect appropriate safeguards.

Once health information is obtained medical identity theft becomes a scary truth. Using someone else’s health insurance creates a cascading of events that can end in a patient care nightmare. Gaining access to healthcare treatment in the victim’s name, the thief begins to contaminate health information including allergies, past history, and medication lists. These inaccuracies threaten effective treatment and could result in incorrect blood transfusions, medication dosages, or medicines. Thieves could potentially begin receiving prescription medications, leaving a patient without life-saving medications.

Breaches a Matter of ‘When,’ Not ‘If’

The healthcare industry is beginning to see that privacy and security is not always a technology issue; it has become a business issue. Those who understand the risks, invest in mature information governance activities, and invest in privacy and security activities will be able to mitigate risks proactively.

So what does it all mean? It comes down to this—the risk of a healthcare facility suffering a data breach has never been higher. According to an article in *Security Intelligence* analyzing data breach figures, the total number of data breaches in the healthcare industry increased from 81 in 2015 to 283 in 2016.[2] This represents a 249 percent increase in just one year. And of the 91 HIPAA-covered entities and 84 business associates included in Ponemon’s 2016 study on the privacy and security of health data, 90 percent suffered a data breach in the past two years.[3] Given this statistic many healthcare experts agree that it is not a matter of “if,” but “when” a breach will occur at a healthcare organization.

Notes

1. Ponemon Institute. “Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data.” May 2016.
2. Brink, Derek. “Health Care Security in 2016: End-of-Year Checkup on Security Trends.” *Security Intelligence*. December 23, 2016.
3. Ponemon Institute. “Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data.”

References

Kam, Rick. “Top Predictions for 2016: Privacy and Security.” *Healthcare IT News*. January 07, 2016.

Olavsrud, Thor. “Top 4 Security Trends of 2016.” CIO. December 20, 2016.

Lou Ann Wiedemann (lou-ann.wiedemann@ahima.org) is vice president of HIM Practice Excellence at AHIMA.

Article citation:
Wiedemann, Lou Ann. "Statistically, What’s the Chance of a Breach?" *Journal of AHIMA* 88, no.3 (March 2017): 26-27.