5.6M Patient Records Breached in 2017, as Healthcare Struggles to Proactively Protect Health Data

Insider-wrongdoing is the cause of the largest health data breach in 2017

BALTIMORE -- 5,579,438 patient records were breached in 2017, according to new data released today in the Protenus Breach Barometer. Published by Protenus, an artificial intelligence platform used by top health systems and academic medical centers to analyze every single action inside a medical record system, the Breach Barometer is the industry's definitive source for health data breach reporting.

Compared to 2016, healthcare experienced a slight increase in the number of breaches reported, from 450 in 2016 compared to 477 in 2017. In either year, this represents an average of more than one health data breach per day. In 2016, 27,314,647 records were affected by health data breaches, over five times greater than the number of records affected in 2017, as the result of several large hacking incidents in mid-2016.

To download the full report, or for more information, please visit:

https://www.protenus.com/2017-breach-barometer-annual-report

The single largest breach reported in 2017 was the result of insider-wrongdoing. This breach was the result of a Kentucky hospital employee inappropriately accessing the billing information of 697,800 patients over multiple incidents. Looking across all incidents in 2017, insiders were responsible for 37% of the total number of breaches this year.

In one particularly egregious incident of insider-wrongdoing, a hospital employee snooped on patient information for 14 years before the breach was discovered. The breach affected 1,100 patient records, and is an unfortunate example of how detrimental insider threats can be for a healthcare

organization. While hacking incidents are often quickly discovered because of the immediate disruption they have on an organization's day-to-day operations, insider threats can remain undiscovered for long periods of time. On average, it took 308 days for an organization to discover it had suffered a breach in 2017.

This long time to discovery of breaches remains a terrifying challenge for health systems everywhere. In fact, the prevalence of such a wide array of hard-to-detect insider threats is the main reason proactive monitoring of all accesses to patient data is rapidly gaining as a standard best practice in health systems across the country.

Business associates and third-parties remain a major source of health data breaches, as well. 53 of the reported incidents, totaling 647,198 records breached, were the result of business associate or other third party access to health data.

Protenus, which publishes the Breach Barometer, yesterday announced an $11M Series B investment in its comprehensive health data auditing and privacy monitoring platform. Founded in 2014, the company helps health systems ensure health data is safe and being used appropriately

About Protenus

Protenus protects patient privacy in the electronic health record (EHR) for top-ranked hospitals, using the latest big data techniques and Protenus-led advances in data science, machine learning, visualization, and software engineering. The Protenus platform uniquely understands the clinical behavior and context of each person accessing patient data to determine the appropriateness of each action, elevating only true threats to patient privacy. Protenus and its partner hospitals are fundamentally improving the way hospitals protect their patient data—further ensuring trust in healthcare. Learn more at Protenus.com and follow us on Twitter @Protenus.

Contact

Kira Caban
Director of Public Relations
kira@protenus.com
410-913-0274