Breached Patient Records Tripled in 2018 vs 2017, as Health Data Security Challenges Worsen

Proprietary data shows 51% of violations were repeat offenses; one employee regularly violated patient privacy for 15 years before detection

BALTIMORE -- 15,085,302 patient records were breached in 2018, according to new data released today in the Protenus Breach Barometer. Published by Protenus, an AI-powered healthcare compliance analytics platform that protects patient data for the nation's leading health systems, the Breach Barometer is the industry's definitive source for health data breach reporting.

There was a slight increase in the number of breaches, from 477 in 2017 compared to 503 in 2018. Alarmingly, the number of affected patient records almost tripled from 5.5M in 2017 to 15M in 2018. As first reported in 2016, a trend of at least one health data breach per day remained in 2018.

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

https://www.protenus.com/2019-breach-barometer

The single largest breach reported in 2018 was the result of hacking a Business Associate (BA). It involved a North Carolina-based health system vendor that had its patient information accessed by an unauthorized party. Hackers gained access to patient data over the course of a week, affecting 2.65M patient records. Looking across all incidents in 2018, hacking was the cause of 44% of the total number of breaches throughout the year.

In another breach, while millions of records weren't exposed, we were reminded of the dangers of insider threats. In this insider-wrongdoing incident, a medical assistant stole patient data by printing patient profiles and giving that sensitive information to others who used them to commit federal crimes. The medical assistant fraudulently collected more than

$33,000 in unemployment benefits. This entity may now face substantial post-breach costs, estimated to be close to $10M per breach.

Looking at the big picture, proprietary Protenus data found that family member snooping is the most common insider-related breach (67.38% of violations). The data also shows that 51% of violations are repeat offenses, indicating health systems accumulate risk that compounds over time if proper reporting, educations, and discipline do not occur.

Business associates and third-parties remain a major source of health data breaches, as the cases above demonstrate. 49 of the reported incidents, totaling 5,328,525 records breached, were disclosed by business associates with at least 102 incidents disclosed by other entities involving a BA or third-party.

Protenus, which publishes the Breach Barometer, was recently named the 2019 KLAS Category Leader in Patient Privacy Monitoring. Founded in 2014, the company helps health systems ensure health data is safe and being used appropriately.

About Protenus

The Protenus healthcare compliance analytics platform uses artificial intelligence to audit every access to patient records for the nation's leading health systems. Providing healthcare leaders full insight into how health data is being used, and alerting privacy, security and compliance teams to inappropriate activity. Protenus helps our partner hospitals make decisions about how to better protect their data, their patients, and their institutions. This year, Protenus was named the 2019 KLAS Category Leader in Patient Privacy Monitoring. In 2018 was named one of The Best Places to Work in Healthcare by Modern Healthcare and one of the Best Places to Work in Baltimore by the Baltimore Business Journal. Learn more at Protenus.com and follow us on Twitter @Protenus.

Contact

Kira Caban

Director, Public Relations

kira@protenus.com