People. Trust. Results.
Since 1960

The Latest Report from Verizon: 58% of PHI Breaches in the Healthcare Sector Stem from Inside Users

In the new *Verizon Protected Health Information Data Breach Report* (PHIDBR), Verizon security experts studied nearly 1,400 PHI data security incidents across 27 countries to create a detailed analysis of the everyday threats healthcare organizations face today. The study of the incidents occurring in 2016 and 2017 revealed that both paper and electronic medical records remain the focus of hackers who target patients' identities, health histories, and treatment plans.

Healthcare is rapidly becoming digitally-driven. "The ability to access information quickly to allow a team of care providers to make point-of-care decisions is vital," said the report. One interesting take-away from the study, however, is that digital security has simply not kept up with the growth, leaving the information a veritable sitting duck for ongoing breaches and attacks. It is worth noting that 75% of the incidents contained in this study occurred in the United States.

According to the analysis, 58% of the security breach attempts involved insiders, of which human error was found to have contributed to half of the incidents. However, those attempts that were 'intentional' were primarily carried out by abusing privileged access credentials or stealing them from fellow employees to gain unauthorized access. Not surprisingly, a chunk of these insider breaches were found to have been driven by curiosity - as in the case of viewing a celebrity's health records. However, a concerning amount – 48% - reflected financial motives such as using patient data to commit credit fraud and file bogus tax returns.

While external users represented a smaller volume of the breaches studied, financial gain was identified as the motive in the vast majority of these particular incidents. From phishing and ransomware to stolen access credentials to theft of laptops and other mobile devices, hackers maintain a growing arsenal of tools to gain unauthorized access to PHI and other sensitive data.

To help combat the most common threat actions highlighted in the report, Verizon recommends:

- Full disk encryption
- Routine monitoring of record access
- Prevention of malware and mitigation of impact

Also in consideration of the analysis results showing that half of the insider breaches were due to human error, ongoing workforce education on privacy and security guidelines is essential. Combined with effective workplace policies, employee awareness can greatly reduce the risk of breaches occurring from simple employee mistakes and omissions.

Verizon's full report can be obtained here.