Published on *The National Law Review* https://natlawreview.com

Lessons To Be Learned From The Breach Of Nearly 500,000 Individual Health Records Reported In September 2017

Article By:

Michael R. Bertoncini

A recent report indicates that nearly 500,000 individual health records were breached in September 2017. This figure is taken from the 39 healthcare data breaches involving more than 500 records that were reported to the Department of Health and Human Services' Office for Civil Rights in September 2017. Healthcare providers suffered the most breaches with 27 reported incidents, followed by health plans with 10 breaches, and 2 breaches reported by business associates of covered entities. This demonstrates the need for security measures by both HIPAA Covered Entities and Business Associates.

The way the health records were accessed is notable. The biggest cause of the breaches was unauthorized access/disclosures (18 breaches), closely followed by hacking and IT incidents (17 breaches). This data about breaches reported in September shows the importance of taking proactive steps to ensure data security. With unauthorized access and disclosure continuing to be a leading cause of data breaches, organizations should consider focusing on potential sources of such unauthorized access and disclosure as they conduct the risk assessments required by HIPAA.

The report also notes that email was involved in many of the breaches reported to HHS in September, finding that there were 13 email-related breaches, including a healthcare employee who emailed PHI to a relative to receive assistance with a work-related action. While that case apparently involved intentional misconduct by a healthcare employee, it raises questions that are instructive for organizations across all industries dealing with sensitive data:

- Does the organization have clear policies regarding appropriate access to and disclosure of protected information?
- Does the organization provide training for new employees on information security?
- Does the organization provide refresher training for employees on information security?
- Does the organization's email policy address information security?
- Has the organization reviewed its email system as part of its risk assessment?

- Does the organization coordinate enforcement of its information security policies with its corrective action policies?

Another important lesson from these September data breach reports is that hacking continues to be a very real risk. Six of the top ten breaches in September were the result of hacking/IT incidents resulting in the exposure of 363,364 records – 76.81% of the records exposed in all reported breaches in September. The continuing risk from cyberattacks highlights the need for ongoing security audits, employee training, and table top exercises.

National Law Review, Volumess VII, Number 320