Health Information Compliance Alert

Risk Management: There's More Than Just Lost PHI at Stake with a Data Breach

Tip: Encryption remains a critical deterrent to hackers.

Try as you might to prevent them, HIPAA breaches occur anyway. With the breach comes the loss of data security, which can overwhelm a practice, both financially and professionally. And with the cost of a breach on the rise, it's crucial to plan ahead for a cyber attack.

Background: If the past three months are any indication of hackers' impact on HIPAA security in 2018, covered entities (CEs) are in for a banner year. In June, July, and August alone, 90 breaches impacting 500 or more people rocked healthcare with a substantial loss of protected health information (PHI) and electronic PHI (ePHI), affecting the records of 3,210,932 individuals, outlines the HHS Office for Civil Rights (OCR) breach portal. Across the board, providers suffered the biggest brunt of the data outages, but health plans and business associates (BA) were hit hard, too, according to the OCR information.

Don't Ignore the Costs of a HIPAA Violation

What happens in the aftermath of a major data breach like the ones highlighted in the OCR breach portal this summer can make or break a CE. The costs to locate and stop the issue can be extreme, and oftentimes mean a complete shutdown of day-to-day operations until the problem is fixed.

And for HIPAA violations involving 500 or more individuals, the notification process brings both physical and fiscal challenges as well. Staff must alert the feds, state officials, the media, business associates, and patients as soon as possible.

Even if that all goes smoothly, HHS and others will have questions about the why and how of the data breach. During this part of the investigation, "the OCR will say, 'shoot us your policies and procedures," cautions **Brand Barney, CISSP, HCISPP, QSA,** security analyst with **Security Metrics** in Orem, Utah. "And they are going to go in with the assumption that you've done nothing, especially if you have no documentation."

That's when audits of administrative and technical safeguards usually ensue. As the dust settles, repercussions may include Civil Monetary Penalties (CMPs) from the government and required corrective action on the part of the CE. And as the costs related to new health IT products, staff training, risk planning, and outside legal/IT assistance pile up, patients may worry that your practice cannot secure their health and personal data and find other avenues of clinical care.

Cut Data Breach Costs with HIT-Savvy Protocols

That's why a strong course of action is essential to combat issues before they happen - protecting both your patients and your practice, suggests **IBM** and the **Ponemon Institute** in the collaborative study, "The 2018 Cost of a Data Breach: Global Overview," published in July. According to the research, organizations can expect a cost of around $148 per lost record, the report shows. For large-scale breaches, where thousands of individuals' PHI or ePHI is compromised, that could amount to millions of dollars.

Interesting: The IBM/Ponemon Institute research uncovers a rise in hacking in line with the 2018 data breach results found on the OCR breach portal. "Forty-eight percent of all breaches in this year's study were caused by malicious or criminal attacks," the report notes. However, two factors that greatly reduced costs and the probability of a data breach were the use of device encryption and incident response, explains the IBM/Ponemon Institute study.

"In this year's research, an incident response (IR) team reduced the cost by as much as $14 per compromised record," the report stresses. "Hence, companies with a strong IR capability could anticipate an adjusted cost of $134, down from $148 per record."

The study also indicates that "the extensive use of encryption reduced cost by $13 per capita, for an adjusted average cost of $135, down from $148 per record."

Put a Plan into Action Now

Risk analysis and management usually include the construction of a comprehensive incident response plan, which includes the steps to follow in case of a data breach. "Being prepared on an organizational level can mitigate the risk of both extensive data loss and negative press," says **Diana Maier**, an employment and privacy law attorney of the **Law Offices of Diana Maier** based in San Francisco.

"Before a breach takes place, a response team should be formed with key personnel, such as executives and privacy, legal, IT, and public relations staff," Maier advises. "This team should inform the organization on the protocol to expect following a breach. When a breach does happen, the team should be responsible for implementing the response plan."

Also, keep in mind that you may need to have more than one plan, depending on the kind of data involved in the incident, Maier notes.

Device management: Don't forget about the second part of IBM/Ponemon Institute's advice - encrypting devices. Penalties are avoidable with strong encryption, maintains attorney **John E. Morrone**, a partner at **Frier Levitt Attorneys at Law** in New York City. For instance, "merely losing an unencrypted device constitutes a data breach under HIPAA, so encryption is truly the best method to avoid a HIPAA breach."

A security incident is bad enough, and you need to know when not to panic versus when you need to launch a response. But if you drop the ball on your duties following a data breach, the risks for bad press and costly penalties are higher than ever before. Make sure you have a solid incident response plan in place to make a bad situation much more bearable.

Resource: To review the IBM/Ponemon Institute report, visit www.ibm.com/security/data-breach.