Health Information Compliance Alert

Cybersecurity: Master the Fundamentals of Forensic Investigations

Tip: Ransomware attacks usually warrant a forensic team.

Cyber criminals don't take a break - even in the midst of a pandemic. And with many providers busy fighting COVID-19 on the front lines, data security may be falling to the wayside, leaving the door open for hackers.

Problem: With their abundance of sensitive patient data ripe for the taking, hospitals and other healthcare facilities remain vulnerable targets, especially during these trying times. Many providers are operating in crisis mode, strapped for cash, and pushing IT issues to the back burner.

In addition, **HHS Office of Inspector General** (OIG), the **Federal Bureau of Investigation** (FBI), and others have reported increased cyber activity, including coronavirus phishing, COVID-19 texting scams, and malware infiltrations. Experts warn that healthcare could see an influx of ransomware attacks in the coming months, too.

Reminder: Covered entities (CEs), their business associates (BAs), and their patients are particularly vulnerable to "targeted" ransomware attacks, the **HHS Office for Civil Rights** (OCR) stresses in its Cybersecurity Newsletter. "In such incidents, ransomware can be customized and deployed based on the size and sophistication of a potential victim," explains OCR. "The ransom demands for this type of attack are often set according to the victim's perceived ability to pay," the agency adds.

First, Prevent and Mitigate Risks

CEs are required to analyze and manage their risks as part of the HIPAA Security Rule. Not only do they need to follow through on these steps because it is required under the law, but CEs and their partners should do this to protect their patients' electronic protected health information (ePHI) - and essentially their bottom lines.

Breach prevention starts with a thorough assessment of your organization's IT practices, software, hardware, training, and more. Next, the information gleaned from the audit is analyzed. This analysis is used to make a compliance plan with the goal of mitigating data security risks and decreasing the chances of HIPAA violations. Finally, your IT staff or vendor implements measures to maintain and manage risks (i.e. password controls, logging and monitoring, patch updates, etc.).

Unfortunately, there's no end to the nefariousness of cyber attackers, and even the savviest tech departments experience data security issues. The key is sifting through the clues that led to the outage - and ensuring it doesn't happen again.

"If you're attacked, get the best information security experts you can afford to see if there is a way out and to keep from damaging any evidence you may need to preserve," recommends HIPAA expert **Jim Sheldon-Dean,** founder and director of compliance services at **Lewis Creek Systems LLC** in Charlotte, Vermont.

Understand the Reasoning Behind a Forensic Investigation

If you find yourself on the wrong side of a data security breach, the best way to get answers is with an in-depth forensic investigation of your systems. Neither OCR nor the HIPAA Security Rule mandate this kind of check-up, but their findings often reveal things that your IT personnel may have overlooked.

"Forensic investigators provide an independent set of investigative eyes," advises **Jen Stone, MSCIS, CISSP, QSA,** a security analyst with **Security Metrics** in Orem, Utah. "A forensic team is typically engaged if you believe your systems have been compromised but don't know the extent of the breach, or whether it is a reportable breach under HIPAA rules.”

These specially trained teams find answers and uncover the security vulnerabilities that led to the breach in the first place, Stone suggests. "Even when IT groups believe that they've discovered the source of the compromise, forensic investigators routinely find evidence that was missed and the security weaknesses that will, when corrected, prevent the hackers from succeeding the next time,” she explains.

Breach Determines Level of Inquiry

Not every incident deserves a forensic-level examination, but every cyber attack should be investigated, admits **Adam Kehler, CISSP,** principal consultant and healthcare practice lead with **Online Business Systems**.

Why? A closer inspection of the breach will expose the factors that led to the incident. Plus, it will help determine whether a more extensive forensic investigation is necessary, Kehler adds.

He suggests that a probe of the case will reveal the answers to these important questions:

- How did the breach occur?
- What was its impact on the organization?
- If it's malware, what did it do and did it exfiltrate data?
- What systems were impacted?
- Can it be determined whether the attackers or malware were completely removed?
- What steps are necessary to fix the issue and stop it from happening again?
- Will new technical controls, procedures' updates, or additional staff training assist with recovery?

Important: "Forensic investigations help you see what went wrong, which vulnerabilities were exploited in the breach, and what you need to do to harden your systems so that it won't happen again,” Stone says.