Health Information Compliance Alert

Case Study: Beware: HIPAA Compliance Won't Always Ensure Protection From Breaches

Take 5 steps to go beyond Security Rule standards to protect your data.

The most recent massive HIPAA breach is teaching a hard-learned lesson: even top-notch HIPAA Security compliance practices won't protect you from a devastating breach of your patients' data. Here's what you need to know about this latest cyberattack breach.

What Happened in Yet Another 'Sophisticated Cyberattack'

Background: Insurer **Premera Blue Cross** recently announced a sophisticated cyberattack on its IT systems that affected 11 million individuals' financial and protected health information (PHI). The attackers gained unauthorized access to the personal information of members, employees and other individuals who do business with Premera.

Premera discovered the cyberattack on Jan. 29, 2015, although the initial attack occurred nearly one year ago on May 5, 2014. According to the insurer, the attack affected Premera, as well as its affiliates **Premera Blue Cross Blue Shield of Alaska, Vivacity** and **Connexion Insurance Solutions, Inc.**

Impact: The attackers may have accessed members' and applicants' names, birthdates, email addresses, postal addresses, telephone numbers, Social Security numbers, member identification numbers, bank account information, claims information, and clinical information. Premera insists that the investigation into the cyberattack has not revealed evidence that the attackers removed such data from its systems or used this data inappropriately. Affected claims date back to 2002.

Upon learning of the attack, Premera notified the **FBI** and began working with the cybersecurity firm **Mandiant**. Premera is providing affected individuals with two years of free credit monitoring and identity protection services. The company has also set up a special website with information and updates regarding the cyberattack at www.premeraupdate.com.

Why Recent Audit Didn't Raise Big Red Flags

Before the breach, the federal **Office of Personnel Management** (OPM) and the **HHS Office of Inspector General** (OIG) conducted an audit of Premera's operations, finding that the insurer had potential vulnerabilities in its IT security, according to a March 20 analysis by Seattle-based healthcare attorney **Casey Moriarty** for the law firm **Ogden Murphy Wallace Attorneys** (OMW). But the federal agencies did not in fact find any massive problems with Premera's HIPAA security compliance.

The audit report stated: "Nothing came to our attention that caused us to believe that Premera is not in compliance with the HIPAA security, privacy, and national provider identifier regulations."

Instead, the OPM and OIG found that Premera's IT system lacked more advanced features, such as "piggybacking prevention" and a better methodology for applying software patches, updates and server configurations, Moriarty noted.

"Upon review of the audit report, it appears that Premera did have fairly robust security safeguards," Moriarty said. So this seems to imply that you cannot assume that HIPAA compliance guarantees protection from data breaches.

What to Do When HIPAA Compliance Isn't Enough

But wait can you really just throw your hands up and lament that a "sophisticated cyberattack" caused a breach

despite your compliance with HIPAA?

Not so fast: "The reality is this environment should be considered the 'new normal,'" and these so-called sophisticated cyberattacks "are imminent and not the exception," warned partner-in-charge **Thomas Lewis** in a March 20 blog posting for **LBMC Security & Risk Services**. "The healthcare industry needs to accept that the onus is on them to anticipate these threats and to adequately prepare for them."

Strategy: And going above and beyond HIPAA regulations to secure your data is possible Lewis provided the following five action points:

1. Employ stronger authentication, particularly to reduce vulnerabilities in remote access. Use multi-factor authentication or even token-based authentication.

2. Use better encryption to safeguard data, and be sure to pair stronger encryption with careful key management for ultimate effectiveness. "The devil is in the details, and the execution of stringent key management is necessary or the encryption becomes useless," Lewis warned.

3. Improve your anti-phishing controls by better training your employees on how to spot phishing attempts. The most effective training method is utilizing programs set up internally to mimic phishing attacks. Beware that phishing "is the easiest entry point for thieves," Lewis cautioned.

4. Enact network segmentation as a method to silo more sensitive data behind more stringent security controls in conjunction with multi-factor authentication.

5. Add monitoring systems to more quickly detect and respond to attacks. "Faster MTTD (Mean Time to Detect) translates into faster MTTR (Mean Time to Respond) and allows you to isolate and minimize the damage," Lewis said.

Lesson learned: "The unfortunate takeaway from Premera's data breach is that HIPAA compliance may not be enough to ensure security from attacks carried out by sophisticated hackers," Moriarty warned. "Although a covered entity's security policies and procedures may technically comply with the HIPAA Security Rule, it is still critical to go further and address any known vulnerabilities that HIPAA may not even require to be addressed."