Health Information Compliance Alert

HIPAA Security: Foil Infiltrators With Beefed-Up HIPAA Compliance

Tip: Hammer out a security management process ASAP.

According to recent evidence from the feds, you're right to be worried about your IT systems. Moreover, securing patients' electronic protected health information (ePHI) has become more perilous during the pandemic with hackers ratcheting up their attacks. In fact, the healthcare industry is under greater threat than ever before.

Background: In a joint advisory issued on Oct. 28, the **Cybersecurity and Infrastructure Security Agency** (CISA), the **Federal Bureau of Investigation** (FBI), and the **Department of Health and Human Services** (HHS) announced that cyber criminals are ramping up their efforts to take down healthcare systems worldwide with more sophisticated malware and ransomware attacks. The three agencies point to the utilization of an amalgam of programs that build on each other - seizing systems, encrypting data, and essentially blocking providers from doing their jobs. Eventually, hackers demand providers and hospitals pay up if they want to access their data and help patients. The costs both professionally and financially can be astronomical (see story p.1).

Concern over these latest ransomware threats is justified, but HIPAA compliance can play a role in thwarting cyber attacks for covered entities (CEs) and their business associates (BAs), suggests HHS in its recent fact sheet "Ransomware and HIPAA.” A combination of a security management process, identifying and remedying risks, and training staff on spotting malicious activity are all factors that decrease providers' chances of a data security incident, the brief indicates.

Caution: There's another major reason you might want to do your best to avoid a ransomware attack other than the typical worries and hassles. If you choose to pay off the hackers to get your data back, you could now find yourself bogged down with federal fines.

"Unfortunately for healthcare providers, the **Department of Treasury** recently announced that any entity that pays a ransom to get their data returned will be in violation of the International Emergency Economic Powers Act and will thus be subject to paying steep civil monetary penalties, not to exceed $250,000,” warns **Wachler & Associates** in its Health Law Blog.

See the Intersection of a Ransomware Attack and a HIPAA Breach

According to HHS, the presence of ransomware on your computer isn't necessarily a violation. The facts of the case, subsequent investigations, and risk analyses determine whether or not a breach has happened.

Definition: If you're confused about what constitutes a breach under HIPAA, you're not alone. "According to the Privacy Rule, a breach is any acquisition, access, use, or disclosure in violation of the Privacy Rule - and that covers a lot,” explains **Jim Sheldon-Dean,** founder and director of compliance services at **Lewis Creek Systems, LLC** in Charlotte, Vermont.

In addition, if evidence gleaned from the risk assessment shows that there was a "low probability” that PHI was compromised, then the incident might not be a breach, indicates **HHS Office for Civil Rights** (OCR) breach guidance. And to make this determination, HIPAA (45 C.F.R. 164.402(2)) requires you to perform a risk assessment on at least these four factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;

- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

Tip: A comprehensive risk analysis using these four factors can help you uncover not only the specifics but also whether there was a low probability of compromise of the PHI. For example, the investigation may identify the type of virus in your system, how it got there, what the malware is doing, and whether ePHI has been impacted.

Add These Mitigation Steps to Your HIPAA To-Do List

Even though cyber crime is increasing during COVID-19, that doesn't mean that there aren't things you can do to circumvent a ransomware attack. Initial steps should always include staff training and security management.

Why? It's also critical that all personnel understand that it can happen to any organization no matter the size or scope; these types of hackers don't discriminate. "End users are targeted," exhorts the advisory.

It is essential that you "make employees and stakeholders aware of the threats - such as ransomware and phishing scams - and how they are delivered. Additionally, provide users training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities," the brief continues.

Important: "Ransomware can affect practices through both targeted and non-targeted attacks," advises **Jen Stone, MSCIS, CISSP, QSA,** a security analyst with **Security Metrics** in Orem, Utah. "A lot of my customers think they're too small to be targets, and maybe that's true, but the non-targeted attacks are still out there," she adds.

Though your physical and financial resources may determine your mitigation strategies, there are many little things that your organization can do to cut down the likelihood of an attack. Consider adding these HIPAA-friendly tips and tactics to your compliance checklist:

- Keep on top of patch management and password controls - especially with remote workers during the pandemic.
- Monitor remote access and audit accounts to ensure both compliance and legitimacy.
- Identify and secure IT assets, including mobile and medical devices.
- Install antivirus software on all computers. Configure it "to update automatically, perform both real-time and regularly scheduled scans, and not be able to be uninstalled except by administrators," Stone stresses.
- Back up your data and maintain offline copies. "If your data gets locked up, you have something to work from and can perhaps avoid paying the ransom," Sheldon-Dean says. "If you don't, you don't really have a chance."
- Devise a contingency plan that both ensures patients' safety and aligns with pandemic protocols and restrictions.
- Outline an incident response plan with a chain of command, including phone numbers and emails for IT management and others who need to be alerted.
- "Test incident response plans immediately. Assess whether changes need to be made to address any changes to the organization as a result of COVID-19," advises attorney **Elizabeth F. Hodge** with **Akerman LLP** in a blog post.

End point: The feds recommend that all providers consider worst-case scenarios. "Plan for the possibility of critical information systems being inaccessible for an extended period of time," urges the advisory. Organizations should figure out ahead of time how they will communicate and maintain records while caring for patients during the pandemic. Additionally, they may want to practice paper-based methods regularly and train staff accordingly.

Resource: See HHS insight on ransomware and HIPAA at: www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.