Health Information Compliance Alert

HIPAA Security: Keep Track of Your IT Assets

Tip: Know the who, where, and why on practice mobile devices.

Technology is a necessary tool to run a successful healthcare organization today, but it must be maintained and evaluated daily. Increasingly, large-scale HIPAA breaches highlight the importance of keeping tabs on health IT while the penalties show the damage mismanagement can inflict.

Understand These HIPAA Security Rule Facts

Keeping electronic protected health information (ePHI) safe is central to the theme of the HIPAA Security Rule, but security violations continue to be a thorn for both small and big covered entities (CEs). Part of the problem revolves around failures to implement better risk management after issues arise or are uncovered in risk analysis - a requirement under the Administrative Safeguards section of the Rule.

"The HIPAA Security Rule requires that organizations implement 'reasonable and appropriate' security controls based on their assessment of risk," explains **Adam Kehler, CISSP,** principal consultant and healthcare practice lead with **Online Business Systems**. Unfortunately, many organizations lack the health IT staff, know-how, or funds to fully comply with the mandates - and that's when violations crop up.

"Conducting a risk analysis, which is an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI held by an organization, is not only a Security Rule requirement, but also is fundamental to identifying and implementing safeguards that comply with and carry out the Security Rule standards and implementation specifications," reminds the **HHS Office for Civil Rights** (OCR) in the summer 2020 edition of the Cybersecurity Newsletter.

According to OCR, another issue CEs suffer from is not knowing where their IT assets are; thus, they often aren't aware when things go awry. "Despite this long-standing HIPAA requirement, OCR investigations frequently find that organizations lack sufficient understanding of where all of the ePHI entrusted to their care is located," the agency says.

Reminder: A proper HIPAA security risk analysis should include the following, according to Kehler:

- An inventory of ePHI throughout the organization
- A consideration of threats and vulnerabilities
- An evaluation of administrative, physical, and technical security controls
- A calculation of residual risk to ePHI

Identify Your IT Assets

You may be wondering what the feds consider an IT asset. OCR suggests that CEs and their business associates (BAs) should first identify and separate their IT assets into three groups: hardware, software, and data. Here is a breakdown of the three categories with examples:

1. Hardware assets: This refers to all the gadgets and IT hardware around your office, including mobile devices, desktop computers and workstations, servers, firewalls, routers, and other electronic media or tools such as medical devices that might be used to access ePHI.

2. Software assets: This covers every type of software utilized in a healthcare environment like device applications,

email and messaging, EHRs and EMRs, operating systems, and anti-virus programs. "Though lesser known, there are other programs important to IT operations and security such as backup solutions, virtual machine managers/hypervisors, and other administrative tools that should be included in an organization's inventory," notes the OCR Cybersecurity Newsletter.

3. Data assets: The ePHI that you create, transmit, receive, collate, or simply maintain is considered a data asset - and safeguarding it is the focus of the Security Rule.

Add These Inventory Tips to Your Risk Management

After you've identified your IT assets, an enterprise-wide risk assessment is not only necessary but expected under HIPAA. Once you've figured out the best course to protect ePHI from being usurped, you can better manage your organization's risks. It's also critical to remind BAs that they're required to implement policies and procedures to thwart the loss of IT assets, too.

Inventorying IT assets can be a very complicated job, particularly for larger healthcare organizations with hundreds of devices, software products, and staff; however, it can truly help alleviate any security gaps. Consider these first steps as you start the process of evaluating your technical tools and managing your risks:

- Understand what you have in the way of software programs and physical hardware.
- Create a hardware log and locate any stray devices.
- Make a running list of all applications, software programs, and vendors.
- Review data assets, ePHI activities, and past data security incidents.
- Outline comprehensive access and configuration controls.
- Perform patch management, software updates, and hardware upgrades accordingly.
- Know who and what's been going on in your networks and systems.
- Audit and review regularly, particularly when operations change and staff leave.

Warning: CEs must also keep on top of other Internet of Things (IoT) machines, too, cautions OCR. "Assets within an organization that do not directly store or process ePHI may still present a method for intrusion into the IT system that could lead to risks to the confidentiality, integrity, and availability of an organization's ePHI," OCR says.

IoT devices like HVAC systems or security alarms may have "weak or unchanged default passwords installed in a network without firewalls, network segmentation, or other techniques," leaving the door wide open for intruders, OCR suggests. By adding these IT assets to your inventory, you treat them like any other risk that needs to be managed and decrease your chances of intrusion.

Resource: Review the Cybersecurity Newsletter at: www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-summer-2020/index.html.