Codify
BY AAPC

Health Information Compliance Alert

Cybersecurity: Prevent Medical Mayhem with Better Patch Protocols

Tip: Check with your software vendor to ensure patches are appropriate.

When you delete or bypass software updates, you run the risk of being open for a cyber attack. Hackers scan for vulnerabilities day and night, and healthcare remains a favorite target. Managing bugs, glitches, and patches is crucial and keeps intruders out - safeguarding both your patients and your practice.

History: In January, HHS issued a report to all covered entities (CEs) about malware issues caused by Spectre and Meltdown, concerning "how computer chips handle data that have the potential to expose sensitive information, such as protected health information (PHI), being processed on the chip," says the agency release. The "design flaws" nicknamed Spectre and Meltdown were "present in nearly all processors produced in the last 10 years and affected millions of devices," follows up the HHS Office of Civil Rights (OCR) June 2018 Cybersecurity Newsletter on the topic.

Read the HHS release at https://content.govdelivery.com/attachments/USDHSCIKR/2018/01/17/file_attachments/944452/HCCIC-2018-001a-SpectreMeltdown.pdf.

Caveat: Sometimes installing software updates doesn't always fix the problem, which was the case with patches for vulnerabilities due to Spectre and Meltdown. "Vendors scrambled to release patches that addressed this problem," OCR notes. "However, testing indicated that a side effect of the patches" was a "decreased performance in certain computer uses."

These types of cybersecurity scenarios lead to the loss of data and promote the HIPAA Security Rule mandate for thorough risk analyses of systems and devices. Because as this case reveals, "testing and understanding the impact of patches can be critical to mitigating the risks patches are designed to address while avoiding or minimizing risks that patches may introduce," warns OCR.

Identify Threats and Fix Them

Malware attacks happen, but that doesn't mean they're inevitable. Challenges do arise when risk assessments occur, and the necessary changes are easy on paper but hard to implement in real time. And though it can be a pain for CEs and their business associates (BAs) to stop the daily grind and turn over technical processes to allow for software updates on hardware and devices, that health IT management is essential to protect ePHI.

"Cyber criminals prey upon the lax security practices, most breaches and attacks are preventable through a higher prioritization of operational security, including patch management and aggressive training programs," observes **Kurt J. Long**, founder and CEO of **Fair Warning, Inc.** in Clearwater, Florida.

Mechanics: Network and technical security oversight lead to breaches - it's just that simple. But you can protect your practice with HIT protocols. "Apply vendor recommendation patches aggressively, and watch for vendor updates vigilantly," suggests Long. "Not only should your IT team remain on top of such updates, but also, they should be driving a security-centric culture through your organization."

Long maintains that it should be a team effort and all staff must understand security compliance. "All team members should understand the importance of installing security updates and maintaining proper security protocols," he adds. "When everyone is on board, you can now plan and prevent for future attacks."

Pocket This Patch Management Advice

Every organization is different; therefore, you can't expect one HIT solution to fit across all healthcare landscapes. Patch arrangements and rules for large-scale clinics and hospitals are going to be completely different than those for small, rural providers.

"Each type of program will have its own unique set of vulnerabilities and challenges for patching," advises OCR. "But, the identification and mitigation of risks associated with unpatched software is important to ensure the protection of ePHI.

When putting together your patch management guide, consider implementing five "common steps," the Cybersecurity Newsletter stresses. The OCR's tips are as follows:

1. "Evaluation: Evaluate patches to determine if they apply to your software/systems.

2. "Patch Testing: When possible, test patches on an isolated system to determine if there are any unforeseen or unwanted side effects, such as applications not functioning properly or system instability.

3. "Approval: Once patches have been evaluated and tested, approve them for deployment.

4. "Deployment: Following approval, patches can be scheduled to be installed on live or production systems.

5. "Verification and Testing: After deploying the patches, continue to test and audit systems to ensure that the patches were applied correctly and that there are no unforeseen side effects."

Expert input: Shirking on software maintenance and ignoring your practice risks can lead you into trouble with hackers - and with the OCR should a breach occur.

"Even small healthcare companies get hacked," warned **Thomas Lewis, CISSP, CISA, QSA,** CEO of information security in a blog posting for **LBMC Information Security**. And if a hacking incident leads to a HIPAA breach, the size of your organization won't protect you from a government audit and potential sanctions, Lewis warns. The OCR will investigate organizations of any size when they suffer a data breach.

Reference: Read the June 2018 edition of the OCR Cybersecurity Newsletter at www.hhs.gov/sites/default/files/june-2018-newsletter-software-patches.pdf.