Codify
BY AAPC

Health Information Compliance Alert

Toolkit: Close Up Your Practice Loopholes with These Authentication Tips

With cyberattacks on the rise, make safeguarding data an end-of-year priority.

Hacking—it's everywhere. It's commonplace now to wake up to weird emails from nefarious sources, receive calls from outlandish numbers, and get ominous text messages from folks you thought previously blocked from your account. Due to workplace necessity, our livelihoods are closely linked with our personal and business technology and mobility, and unfortunately, there's just no way to avoid every cyberattack.

Healthcare has become a frequent victim to intimidation from digital criminals, and though completely breach-proofing your practice is not possible, you can greatly cut down on the likelihood of an infraction. Putting a plan in place to verify users on the devices in your healthcare practice is a good place to start.

What is Authentication?

According to the OCR, "authentication is a process used to verify whether someone or something is who or what it purports to be in the electronic context, while keeping unauthorized people or programs from gaining access to information," an OCR report from Oct. 2016 suggests (see the full report here: http://www.hhs.gov/sites/default/files/november-2016-cyber-newsletter.pdf.)

History and context. As HIPAA violations continue to pile up, wreaking havoc on the healthcare industry, it's never been more critical to verify staff, set up passwords, and put plans into place. In fact, the HIPAA Security rule requires that "reasonable and appropriate authentication procedures" be initiated to protect the ePHI of patients, and if for one reason or another, your practice is privy to a breach, you'll be held accountable for your lack of authentication guidelines.

Risk analysis. Assessing your practice risk and where data is lost, is the initial step toward eradicating ePHI loss. For starters, a quarterly, in-house audit of all devices and software helps stave off digital mayhem. It is wise to engage the services of a certified health IT firm or law group to do a risk analysis of your systems, too.

"Hackers are a step ahead of private practices, and they [physicians] easily fall victim to them," says **Clinton Mikel, Esq.** of The Health Law Partners, in their Southfield, Michigan office. "If the OCR investigates and finds over 500 individuals were affected, the first thing they will look for is the security risk analysis."

Know These Two Types of Verification

Single-factor and multi-factor authentication are two types of password control, the OCR suggests. Once a risk analysis is done, the potential for cyberattack is easily assessed and you can go about organizing a plan for passwords and access.

Single-factor authentication refers to the requirement of only one set of credentials for access—like a password associated with something in the office — to a device, network, or system. This type of verification is considered weaker than multi-factor authentication, which requires two or more things to allow a covered entity access. For example, staff might need a keycard to enter the office, fingerprint verification to turn devices on, and a password to log into the system.

When putting together your HIPAA-compliance plan, consider these authentication ideas to increase ePHI security:

- Password
- PIN numbers

- Fingerprint requirement
- Passcode
- Voice activation
- Log-in attempt logouts

Tip: Before setting up a plan or even hiring a certified health IT expert, take a look at the ONC's helpful Security Risk Assessment Tool. The tool gives advice, breaks down HIPAA compliance for novices, and offers information on how to audit your practice safety and security measures.

For more information on the ONC's Security Risk Assessment Tool, visit https://www.healthit.gov/providers-professionals/security-risk-assessment-tool.