Codify
BY AAPC

Health Information Compliance Alert

Toolkit: Thwart Inside Threats With These Pointers

Tip: Implement multi-factor authentication on all your devices.

The news is always ripe with tales of phishing attacks and ransomware takedowns, but many health IT breaches are caused by insider threats. Whether employees seek to purposely harm your health IT or do so unintentionally, it's wise to protect yourself and your patients against an inside attack.

Definition: According to the United States Computer Emergency Readiness Team (US-CERT), there are two types of insider threats: malicious and unintentional. Employees, business associates (BAs), and vendors who work specifically to corrode, corrupt, or hack your system are considered malicious threats. On the other hand, vendors, BAs, and staff with access to your IT resources can hurt your practice accidentally, and they bring an unintentional threat to your business.

"Although there has been a lot of recent publicity about external threats to the information systems of healthcare providers, covered entities [CEs] need to also consider and proactively address threats from within their organization," remind attorneys **Elizabeth Hodge** and **Carolyn Metnick** with national law firm **Akerman LLP**.

Watch for These Unintended Risks

Many HIPAA issues and lost protected health information (PHI) are due to human error. US-CERT research suggests that there are four main causes of unintended threats. Those include the following:

- **Accidental disclosure:** An example of accidental disclosure would be when an employee posts something on social media or sends an email to the wrong patient.
- **Social engineering:** This problem is especially common. Phishing happens when a staff member clicks on an attachment and unleashes chaos on your system from the malware in the attachment.
- **Physical issues:** In these scenarios, physical records are not properly disposed of and get into nefarious hands.
- **Mobile devices:** Unencrypted lost or stolen mobile devices like cell phones, laptops, or tablets with patient information on them continue to wreak havoc on the healthcare industry and are a perennial cause of breaches.

Inadvertent hazards like these are best eradicated with a combination of risk assessment and management, security protocols like encryption and multi-factor passwords, logging and monitoring of devices, and most importantly, comprehensive staff education from the top down.

Tip: Make sure you train employees to keep their eyes open and report suspicious behavior of other employees that may pose a security threat, Hodge and Metnick say. "Start privacy training upon hiring (coordinate it with other training such as records management, code of conduct, etc.)."

Tackle Dangers Head On

There are usually signs that an insider threat is on the horizon, suggests US-CERT guidance. US-CERT indicates these actions may be the start of malicious activity by an employee or BA:

- Remotely accesses systems during off times or vacation.
- Works unusual hours when no one else is in the office.
- Copies classified materials.
- Shows "notable enthusiasm for overtime, weekend or unusual work schedules."
- Seems overly curious about business activities not related to his or her job.

The HHS Office for Civil Rights (OCR) Cybersecurity Newsletter offers great advice on insider threats and what to do after an employee is terminated. Pocket these OCR tips to set up your procedures:

- **Keep policies updated.** In your HIPAA compliance plan, outline clearly who is allowed to access PHI - and who isn't. This also means updating protocols after an employee leaves or is terminated.
- **Monitor, inventory, and log.** From your mobile devices to how many times access has been blocked because of too many password attempts, your IT staff must keep abreast of your practice devices, networks, and systems. Documentation allows management to see outlier behavior that may lead to threats down the line.
- **Address physical access.** Keep a log of who has a key to the office and access to hardware, and make sure the locks are changed when an employee is terminated. "Take back all devices and items permitting access to facilities (like laptops, smartphones, removable media, ID badges, keys)," reminds OCR.
- **Outline remote access.** Implement remote access procedures like remote purging and wiping to combat insider threats, loss, and hacks. Don't forget to "terminate access to remote applications, services, and websites such as accounts used to access third-party or cloud-based services" after an employee leaves, OCR advises.
- **Implement multi-factor authentication.** Strong passwords protect your practice - it's just that simple. Remember to change those often, never reuse the same password, and to update immediately when staff turnover.

Expert advice: Employees are often nervous to verify breaches or tell practice management about their hunches. "Train in incident management, top to bottom," advises **Jim Sheldon-Dean,** principal and director of compliance services for **Lewis Creek Systems, LLC,** in Charlotte, Vermont. "Staff need to feel like they are empowered to report their suspicions of information security incidents, the handling of incidents needs to be clearly defined, and top management needs to understand the impacts of incidents and the necessity to prevent them as reasonably practicable."

Resources: Find more US-CERT guidance at https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf.

Review the OCR Cybersecurity Newsletter on insider threats at www.hhs.gov/sites/default/files/november-cybersecurity-newsletter-11292017.pdf.