MDS Alert

Reader Question: Implement Data Safety Plan Before Terminating Employees

Question: With so much turnover at our facility, I worry about residents' protected health information. What policies and practices should we implement to keep information safe despite having so many employees on staff?

New Mexico Subscriber

Answer: The U.S. Department of Health and Human Services 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 Health Information Portability and Accountability Act (HIPAA) compliance plan, outline clearly who is allowed to access protected health information (PHI) and electronic PHI (ePHI) - 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's 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)," the OCR says.
- 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, the OCR advises.
- Implement multifactor 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 turns over.

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."