Pain Management Coding Alert

Reader Question: Employ Education to Cut PHI Breaches

Question: What can I do to make sure our practice stays current on best practices to avoid Health Information Portability and Accountability Act (HIPAA) breaches?

New Hampshire Subscriber

Answer: One of the best things you can do is incorporate an annual training. Since healthcare rules and regulations change every day, it's basically impossible (and definitely inadvisable) to think of HIPAA training, as required by the Department of Health and Human Services Office for Civil Rights (OCR) as a one-and-done seminar for employees. Make HIPAA training annual, at least, and don't forget to ensure that all staff members attend - including coders, billers, clinicians, any assistants, and the practice manger.

"The number one issue is lack of awareness that this can happen," says **Kurt J. Long**, founder and CEO of FairWarning Inc. in Clearwater, Florida. "Providers are worried about patients and focused on patient care and for whatever reason many practices of all sizes are remarkably unaware of the threats."

These five areas should be your focus for future trainings, according to HIPAA expert **Jim Sheldon-Dean**, principal and director of Compliance Services for Lewis Creek Systems LLC, in Charlotte, Vermont.

Cybersecurity: Avoiding ransomware attacks and phishing expeditions takes know-how. A thorough cybersecurity education is essential, maintains, Sheldon-Dean. "Don't open the attachment or click the link!"

Devices: Many of the high-profile HIPAA violations over the last year were directly related to the management (or lack thereof) of portable devices. Train employees on the proper use of portable devices and remote access, advises Sheldon-Dean. "Don't put PHI on your phone unless you are supposed to; don't start using new apps or devices without clearing them with IT; and don't access any email with any PHI unless you must for your job."

Upper management: Front desk employees often get minimal training, and that needs to change. But clinicians and upper management must also be on board and remain updated on HIPAA guidance, too. Upper management must be aware of "the importance of and processes in information security," explains Sheldon-Dean. "Good information security is a patient safety and corporate survival issue."

Risk awareness: Evaluating risk through assessment, analysis, and management is critical for practices, and it's required under the HIPAA Security Rule. An area in need of improvement is "training for managers to always be alert for risk issues," Sheldon-Dean says. "Local managers need to know how to watch for and act on things that may affect information security."

Incident management: HIPAA violations happen, but employees are often nervous to verify breaches or tell practice management about their hunches. Sheldon-Dean encourages, "Train in incident management, top to bottom." He adds, "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."