Health Information Compliance Alert

EHR Compliance: Don't Forget to Assess, Analyze, and Manage EHR Risk, Too

Tip: Make a list of who's allowed EHR access - to avoid problems later.

Since the HITECH Act defined the importance of the implementation of electronic health records (EHR) to improve healthcare - first with Meaningful Use and now with MACRA's Advancing Care Information - health IT has been a major player supporting cliniciansto give their patients the most efficient and informed care.

However, EHRs aren't perfect, and a system that is perfect for a large, city hospital isn't going to fit the needs of a smaller, suburban specialist. That's why it's essential to audit your EHR systems, keep abreast of updates and applications, and check in with your vendorregularly, assessing risks and fixing problems before they start.

To perform a thorough risk analysis, you must look at target areas to reveal all the potential ways something can go wrong. Because when it comes down to it, there's nothing more important than securing the confidentiality, integrity, and availability of your patients' electronic protected health information (ePHI).

Of course, your main concern when working with EHRs is protecting data from unauthorized access, breaches, and leaks. When performing your risk analysis, the HHS Office of the National Coordinator for Health Information Technology (ONC) recommends that you evaluate the following questions:

- What new ePHI have EHRs introduced into my practice? Where will that ePHI reside?
- Who in my office will have access to EHRs?
- Should all employees have the same level of access to EHRs?
- Will I allow employees to have EHRs or ePHI on their mobile computing/storage devices? If so, how can we keep the data secure on those devices?
- How will I know if ePHI has been accidentally or maliciously disclosed to an unauthorized person?
- When we upgrade our electronic storage equipment (e.g., internal/external hard drives), how will we ensure that ePHI is properly erased from the old storage equipment before disposing of it?
- How will I ensure that backup facilities (e.g., tapes, hard drives, etc.) are secure?
- Will we share EHRs, or the ePHI contained in them, with other healthcare entities through a Health Information Organization (HIO)? If so, what security policies do I need to be aware of?
- What security requirements exist to protect my patients' health information if my EHR system is capable of providing patients with a way to access their health record/information via the Internet, such as a portal?
- Will I communicate with my patients electronically (e.g., through a portal or email)? Are those communications secured? How will I know that I'm communicating with the right patient?

Another element of your EHR privacy and security is how to ensure that the data contained in the records is accurate and remains unadulterated by unauthorized users. To assess your integrity risks, the ONC recommends that you consider these questions:

- Who in my office will be allowed to create or modify an EHR or the ePHI contained in it?
- How will I know if someone has altered or deleted data in an EHR?
- If I participate in an HIO, how will I know whether the health information I exchange is altered in an unauthorized manner?
- If my EHR system allows patients to access their health record/information online, will I allow patients to modify any of the health information in their EHRs? If so, what information?

Important: Staff EHR training can eradicate many issues from accidental disclosures of ePHI to more serious HIPAA violations. "Implementation is a critical step in EHR adoption," **Richard Loomis, MD**, chief medical officer and vice president of Practice Fusion says. "The ability to implement quickly and get your staff up to speed is vital to ensuring a smooth transition for your practice." He adds, "Any EHR you choose has to be easy to use to make training your staff quick and efficient. Get a clear understanding from the vendor on the implementation process and timeline."