Health Information Compliance Alert

Compliance: Cut Down Your Breach Factor with a Look at 3 Common Violations

Tip: Proof of a risk analysis and implemented plan help after a breach.

If you've avoided a HIPAA breach, it means you've dodged the proverbial compliance bullet. But it doesn't mean you're immune to future violations. Keep this quick compliance checklist in mind to ensure your slate remains clean.

Review: If you are worried about a breach, you might want to consider these four questions based on the HIPAA Breach Notification Rule:

1. What type of information was lost and how large an impact would it be?
2. Who obtained the PHI, and how and to whom was it leaked?
3. Did anyone actually receive and see the data?
4. What did your practice do to lessen the effect of the lost PHI?

Read the HIPAA Breach Notification Rule at: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

Take a Look at The Basics

Whether you're old hat at HIPAA or just getting started, consider these three common violations that are a concern for even the most compliance savvy practices.

Combat Theft with These Tactics

Protected Health Information (PHI) and electronic protected health information (ePHI) are commonly adulterated when provider and/or partner technology, information, or paperwork is stolen. This could mean anything from an office break-in, where actual hardware or physical files and property are taken, to lost or lifted portables that were snatched outside the practice then compromised.

Remember: Employees steal PHI and ePHI too, recording patient data for their own personal gain. When this kind of HIPAA breach happens, the records of patients are often exposed and sold for profit.

Theft is the easiest HIPAA violation to deal with and overcome. A good place to start is with the encryption of all your electronic devices, especially the phone you might dictate into or the tablet you carry around the office. These types of at-rest devices can be quickly pocketed by anyone that comes through your practice doors from patients to employees to the guy that delivers your lunch.

Scrutinize and educate: Performing a comprehensive background check on all your employees and business associates before hiring needs to be mandatory for added security. However, vetting processes aren't perfect and employees are tempted by the easy access to patient information and financial data for numerous nefarious reasons □ and in those cases, strict disciplinary guidelines should be imposed.

Avoid Unauthorized Access or Disclosure Snafus

This culprit is a frequent contributor to breaches and can easily be remedied with proper staff education. It often arises when providers and their employees let their policies slip when transferring PHI and ePHI to third parties like claims and collections companies, outside billers, and insurance carriers.

This could be a detailed phone message or fax about a patient to an unauthorized individual or business associate or emailing patient information to insurers for claims, but it also covers something as simple as displaying patient information without consent on the practice bulletin board in the waiting room. The combination of what can be related, who has access to it, and where the PHI/ePHI can officially go is the focus of this breach.

Train and retain: Constantly re-educating staff about your compliance practices and ensuring that they understand the importance of both practice and patient security is essential. Another crucial detail is having an ironclad business associate agreement that protects you against partners who aren't always reliable.

Tip: When you go about enlisting outside resources, look for "sophisticated vendors that have very advanced HIPAA programs because smaller firms don't know what the HIPAA rules are," advises **Abby Pendleton, Esq.** of The Health Law Partners, P.C., in the Southfield, Michigan office.

Don't Get Slack About Cyber Attacks

Unfortunately, more often than not, practices think they are prepared but are actually technically vulnerable. From social engineering schemes like phishing and spoofing to malicious attacks involving malware and spyware, healthcare's cybersecurity is on the top of everyone's watchlist. And that's why it's essential to follow the golden rule of HIPAA compliance: assess, analyze, and manage.

Federal help: This is where the Office of the National Coordinator for Health Information Technology (ONC) risk assessment tool comes in handy. The ONC site assists practices in the initial stages of HIPAA compliance planning and points you toward the best methods for addressing security.

Reminder: "Hackers are a step ahead of private practices, and they [physicians] easily fall victim to them," says attorney **Clinton Mikel, Esq.** of The Health Law Partners, P.C., in the 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."

Exceptions: Since most breaches are accidental and relatively benign, guidelines for exceptions to the rule are available for providers to follow if an infraction is suspected. Here are a few examples:

- An employee might "unintentionally" give the wrong patient data to a physician, but the doctor realizes the error and doesn't use or access the PHI or ePHI.
- Authorized workers might unwittingly transfer ePHI to another "covered entity," but that worker sees the mistake and deletes the information.
- Authorized personnel believe that the PHI could not be conveyed to another source for instance, patient data was mailed but is returned unopened due to a wrong address.

Resource: To access the ONC's risk assessment tool, visit https://www.healthit.gov/providers-professionals/security-risk-assessment-tool.