Part B Insider (Multispecialty) Coding Alert

Compliance: 3 Common HIPAA Breaches -And How to Avoid Them

As the OCR's Audit Phase 2 looms large, watch your practice's loopholes for these common HIPAA blunders.

Privacy and security are major players in the health care industry today, and many practices keep coming up short. HIPAA violations are rampant, and when protected health information (PHI) breaches occur, it can be disastrous for everyone involved.

Background: According to the Health Information Technology for Economic and Clinical Health Act (HITECH) final ruling, a HIPAA breach occurs when an individual's privacy and security are at risk because his or her PHI has been "accessed, acquired, used, or disclosed." After a breach has been identified, the U.S. Department of Health and Human Services (HHS) requires individuals to be notified under HIPAA.

The HHS mandates under HITECH that "HIPAA covered entities and their business associates provide notification following a breach of unsecured protected health information (HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414)."

If you are worried about a breach, you might want to consider these four questions based on the HIPAA criteria used in enforcing the 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?

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 access the PHI.
- Authorized workers might unwittingly transfer PHI 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.

Prevention Is Key

Oftentimes, the data lost is pivotal to the livelihood of your practice and is on a grand scale, particularly if the nature and breadth of the HIPAA breach involves over 500 patients in your state.

In massive cases like these, your practice must alert the patients, the media, and the HHS Secretary. If this happens, the OCR posts your error on its breach portal, there is usually a fine, and the press can report your HIPAA infractions to the public and once it's out there, it never goes away.

Primary causes of compromised PHI are theft, unauthorized access or disclosure, and hacking or IT incident. Deterring these types of issues can be daunting, especially with complicated regulations to follow, but prevention is critical to practice compliance as the new OCR Audit Phase 2 program ramps up.

Fortunately, there are many things that providers can do to address these breaches such as performing a risk evaluation, focusing on compliance shortcomings, and putting measures into place with the data gleaned from the analysis. The HHS even offers a risk assessment tool, but many physicians don't utilize it.

"Many physicians don't understand that this [risk analysis tool] is the first element in HIPAA security," says **Abby Pendleton, Esq.** of The Health Law Partners, P.C., in their Southfield, Michigan office. "This type of risk analysis is the starting point to find potential vulnerabilities and then put into place the appropriate safeguards. It is the stepping stone to implement HIPAA but not enough practitioners do it."

3 Major Breaches and How to Fix Them

Consider the following three common breaches along with expert tips on how to avoid them.

1. Theft. PHI is commonly adulterated when practice or partner technology, information, or paperwork is stolen. This could mean hardware plundered by thieves, including laptops, desktops, tablets, or mobile phones, but it also refers to the paper route□lifted paperwork, hard files, discs and film (x-rays or photography). Sadly, employees can steal PHI as well, 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 one of the easiest HIPAA breaches 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.

Performing a comprehensive background check on all your employees and business associates before hiring needs to be mandatory for added security. Your practice should impose strict disciplinary guidelines for both staff and business associates should you uncover this type of theft of materials or information.

2. Unauthorized Access or Disclosure. 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 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 PHI 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 can officially go is the focus of this breach.

Constantly re-educating staff about your privacy practices and ensuring that they understand that this is a big deal in regard to patient security and safety is essential. Another crucial detail is having an ironclad business associate agreement that protects you against partners who aren't always reliable. Lastly, 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," says Pendleton.

3. Hacking or IT Incident. Unfortunately, more often than not, practices think they are prepared but are actually technically vulnerable. This is where the risk assessment tool comes in handy to show you where hackers are most likely to strike.

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

Five key steps to take to ward off hackers are as follows:

- Assess your HIPAA risk annually either with the HHS online tool or using a reputable firm or program.
- "Hire a good IT firm who is well versed in the up-to-date HIPAA regulations and security issues. The expenditure is recommended because health care security is complex," suggests Mikel.
- Test your software often for vulnerabilities and keep it updated.
- Ensure that your tech people are monitoring the firewall security.
- Look for antivirus products that protect against threats common to health care hacking.

Resources: For more information about breaches and the HIPAA Breach Notification Rule, visit www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

For a quick link to the HHS risk assessment tool, visit www.healthit.gov/providers-professionals/security-risk-assessment.