Codify
BY AAPC

Psychiatry Coding & Reimbursement Alert

Compliance: Avoid Possible Penalties for PHI Violations Using This Expert Advice

Feds expect you to notify everyone affected by every HIPAA breach.

When you're faced with a potential privacy or security breach under the Health Insurance Portability and Accountability Act (HIPAA), the government requires you to file notifications to all parties the breach affects. If you don't, there could be dire consequences.

Potential penalties: Fines for HIPAA violations can range from $100 to $1,500,000. Spot potential HIPAA violations with this expert advice, and stay out in front of any penalties your practice could face for compromising an individual's protected health information (PHI).

Look for Compromised PHI to ID Breaches

Quite simply, "a [HIPAA] breach is an improper or unauthorized use, disclosure, or access of protected health information (PHI)," explains **Cyndee Weston, CPC, CMC, CMRS**, executive director of the American Medical Billing Association (AMBA) in Davis, Ok.

Official definition: In the HIPAA Breach Notification Rule (45 CFR §§ 164.400-414), the U.S. Department of Health & Human Services (HHS) defines a breach as "an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the ... [PHI]."

HHS presumes all impermissible uses or disclosure of PHI to be breaches "unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment."

Example: You are sending a fax to a neurologist's office containing a patient's PHI. You mistakenly misdial the fax number, sending the patient's PHI to the wrong fax number.

According to **Jim Sheldon-Dean**, principal and director of compliance services for Lewis Creek Systems, LLC, in Charlotte, Vt., other common HIPAA breaches include, but are not limited to:

- mailing the wrong PHI to a patient or business entity
- losing an unencrypted laptop or memory stick containing PHI
- using unsecure digital communications for professional purposes involving PHI over the Internet.

Bad news: In addition to these typical HIPAA violations, hackers are starting to assault medical practice's records in an effort to obtain PHI and other personal information, Sheldon-Dean warns.

HIPAA Breaches Aren't All Business-Related

Though most breaches occur within the realm of a medical practice's business operations, some PHI violations bleed into providers' personal, and in some cases political, worlds.

According to Weston, when a physician discusses a patient's medical history with a friend or family member that the patient has not authorized to access his medical records or information, it might be a breach. This will depend entirely on the situation, but everyone in the practice should mind what they say about patients' PHI outside of the office just to be safe.

Weston has also been on the receiving end of a HIPAA violation, which shows just how prevalent and unexpected these breaches can be.

"My local dentist sent out a political letter asking patients to vote for a specific candidate running for state office," Weston says. "He used his patient list to send the letters out. He violated HIPAA, because he misused my address, which is an identifier of PHI to send me information unrelated to my treatment and care."

Resource: Wondering what information constitutes PHI? Check out the list of 18 HIPAA identifiers at http://cphs.berkeley.edu/hipaa/hipaa18.html .

Best bet: Be on the lookout for PHI compromises everywhere. The better you get at spotting PHI vulnerabilities, the better you'll be at preventing HIPAA violations.

Notify 'Individuals,' Secretary of Breaches

When your practice commits a HIPAA breach, HHS wants you to provide notifications to three entities: any affected individuals; the HHS Secretary; and, in certain circumstances, the media.

Here's what HHS expects you to do for each of these entities should a breach occur:

- **Individuals:** You must immediately (i.e., no later than 60 days following the discovery of the breach) notify any patient, business associate, employee, etc., that the breach affects.These individual notifications must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what you are doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for your practice (or business associate, as applicable).
- **Secretary:** You must notify the HHS Secretary of any breaches by completing a breach report form, which you can find online at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html . If a breach affects 500 or more individuals, you must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, you may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.
- **Media:** If you experience a breach that affects more than 500 residents of a state or jurisdiction, you must notify the affected individuals and "provide notice to prominent media outlets serving the state or jurisdiction," HHS reports.

"According to HHS, you must notify individuals in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically," says **Kent Moore**, senior strategist for physician payment at the American Academy of Family Physicians. "If you have insufficient or out-of-date contact information for 10 or more individuals, you must provide substitute individual notice by either posting the notice on the home page of your web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. If you have insufficient or out-of-date contact information for fewer than 10 individuals, you may provide substitute notice by an alternative form of written notice, by telephone, or other means. In any case, you must also include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach," Moore adds.

"With respect to a breach at or by a business associate, you are ultimately responsible for ensuring individuals are notified, according to HHS," Moore says. "However, you may delegate the responsibility of providing individual notices to the business associate. You and your business associates should consider which of you is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the business associate performs on your behalf and which of you has the relationship with the individual."

Expert input: According to Weston, you can expect the following fines for the following types of HIPAA violations:

Advice: Take all your potential HIPAA violations seriously. Even if your practice avoids heavy fines for HIPAA violations,

you could suffer a dent in your integrity among patients if they discover even a single violation that your practice doesn't responsibly address.