Codify
BY AAPC

Optometry Coding & Billing Alert

Compliance: Get Ahead of Notification Curve for PHI Breach

Avoid stiff penalties that could hurt your practice.

With fines ranging from $100 to $1,500,000, you can't afford to make mistakes with notifications for protected health information (PHI) breaches under the Health Insurance Portability and Accountability Act (HIPAA).

Help is here: Spot potential HIPAA violations with this expert advice. We'll help you stay out in front of any penalties your practice could face for compromising an individual's 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: 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 patient's primary care provider containing PHI about your cataract treatment. 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

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 populations should a breach occur:

- Individuals: You must immediately notify any patient, business associate, employee, etc., that the breach affects.
- 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.
- 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.