Briefings on HIPAA

HIPAA Q&A: Medical record requests, provider relationships, soundproofing, and accidental disclosures

by Mary D. Brandt, MBA, RHIA, CHE, CHPS

Q: Does the HIPAA Privacy Rule strictly prohibit the disclosure or request of an entire medical record? If not, does there need to be a case-by-case justification every time an entire record is disclosed?

A: The Privacy Rule does not prohibit the disclosure of an entire medical record, but it does apply the "minimum necessary" rule (see 45 *CFR* §164.514(d)). You may release the entire record if it is specifically justified as the amount reasonably necessary to accomplish the purpose of the request (for example, a valid subpoena that requests "any and all records" on an individual). You may also release a complete copy of the record if the patient provides written authorization to do so.

Q: Can a healthcare provider be a business associate (BA) of another provider? In other words, do providers need to have business associate agreements (BAA) between one another?

A: Yes, Provider 1 may be a BA of Provider 2, if it provides a service to Provider 2 that requires access to Provider 2's PHI. In this case, Provider 2 would need to have a BAA with Provider 1. Providers who exchange PHI in the course of providing treatment for shared patients do not need to have BAAs with each other.

Q: Does the HIPAA Privacy Rule require facilities to make structural changes like soundproofing or private rooms in order to prevent disclosures that could occur from overhearing conversations?

A: No, the Privacy Rule does not require facilities to make structural changes. It does, however, require reasonable safeguards and minimum necessary policies and procedures to protect an individual's privacy. Common safeguards include:

- Asking staff to speak quietly with family members in a waiting room or other public area
- Avoiding the use of patient names in public hallways and elevators
- Isolating or locking file cabinets and record storage areas
- Using password protection for computers that contain PHI

Q: If you discover that you have accidentally accessed a patient's information on your facility's computer system, what's the best course of action? Who should you notify first? Are you at risk of being in trouble if you looked at the information before realizing the error?

A: Immediately notify your facility's privacy official. If you don't need access to patient information, your computer access profile should not allow that access. If you do need access to patient information but accidentally accessed the record of a family member or colleague in the course of your work, let your privacy official know. If the access was accidental, you should not be disciplined.

Editor's note: Brandt is a healthcare consultant specializing in healthcare regulatory compliance and operations improvement. She is also an advisory board member for ***BOH****. This information does not constitute legal advice. Consult legal counsel for answers to specific privacy and security questions. Opinions expressed are those of the author and do not represent HCPro or ACDIS. Email your HIPAA questions to Editor Steven Andrews at sandrews@hcpro.com.*