

Health Information Compliance Alert

Reader Question: Don't Sweep Your Compliance Concerns Under the Rug

Question: A provider in our area has established policies and procedures that allow PHI to be released inappropriately, such as calling out patients' information in waiting areas and not setting up unique IDs for its employees. This provider is not our business associate or trading partner, but we do often refer patients to them for care. Does HIPAA require that we report our concerns?

Tennessee subscriber

Answer: "No, there is nothing in the regulation that states you must report suspected or known violations by another entity where there is no formal business relationship," says **Rick Ensenbach**, senior security consultant with Shavlik Technologies in Roseville, MN.

But that doesn't mean you can't act on your suspicions. First step: Contact the compliance staff of the organization to discuss your concerns, Ensenbach suggests. If the entity resists making changes to its privacy or security practices, you should stop referring your patients to them, he advises.

While there is no requirement to report an unaffiliated provider's suspect behavior, filing an official complaint with the Office for Civil Rights or the Centers for Medicare & Medicaid Services could save you from a "guilty by association" label if the office's poor practices lead to a privacy or security breach.

The Bottom Line: You can choose to ignore your peers' noncompliant practices. However, you could find your reputation in the wringer if you continue to knowingly share patients' information with providers who fail to safeguard it, Ensenbach warns.