Codify
BY AAPC

Health Information Compliance Alert

BAAs Aren't Always the Answer

Contracts differ according to the access and disclosure levels of PHI.

Many of the people who help to make a medical practice successful aren't necessarily involved in patient care, nor do they interact with patients directly. That's why it's wise to evaluate how protected health information (PHI) is accessed when you're figuring out who is or isn't a business associate, considering the myriad ways someone may come into contact with patients' data.

You do not need a business associate agreement (BAA) when there is no access, management, or "persistence of custody" of PHI, according to **Jim Sheldon-Dean**, founder and director of compliance services for Lewis Creek Systems, LLC in Charlotte, Vermont. You don't need a BAA with payers, other providers, and your own workforce members.

Those who would have no reason to use, disclose, create, receive, maintain, or transmit PHI on your behalf also fall into the no-BAA-needed category, Sheldon-Dean notes. This would include people like tradesmen (plumbers, electricians, etc.) and housekeeping or cleaning services.

"They're not business associates [BAs]," Sheldon-Dean states. "They should be under a confidentiality agreement so that they know if they see anything or hear anything, they shouldn't repeat it. But they're not business associates. They're not doing anything with PHI on your behalf."

Reminder: This type of contract protects you should an accident or theft happen, but it doesn't completely discharge you from liability. The language of the confidentiality agreement "puts the company on the hook if it should breach its obligations with respect to confidentiality," says attorney **Kathleen D. Kenney, Esq.**, of Polsinelli LLP in Chicago. "Most third parties with access to PHI will meet the definition of a business associate, but in the rare instances where they do not, having contractual protections in place puts a provider in a better position."

Kenney adds, "But this certainly does not absolve the provider from its own obligations to ensure safeguards as OCR will only look at the provider if an incident occurs and the third party does not meet the definition of a business associate."

Know What 'Conduit' Means in HIPAA

HIPAA regulations provide a narrow exception for "conduits" (FedEx, UPS, U.S. Postal Service, etc.) when the conduit or courier of information provides "simple delivery only," Sheldon-Dean says. These types of entities don't have any "persistence of custody" of PHI.

Persistence of custody means that the entity is storing or holding onto the PHI in some way. A common example is your regular email service provider.

Warning: What you send via your email provider "winds up being stored," Sheldon-Dean points out. "It may wind up being backed up in different email services." And so, your email service provider does "have persistent custody of messages."

"If somebody's providing email services for you and handling PHI, they are a business associate whether they like it or not," Sheldon-Dean cautions. And that's why cloud vendors are your business associates, too - "even if they're handling information that's encrypted, it's still information that's covered under the business associate rules," he continues.

Bottom line: "If the information [is] being held on to in some kind of persistent ways, there's some persistence of custody, then that's how you decide what the business associate relationship is in those situations," instructs Sheldon-Dean.

Resource: Find out more about the HIPAA conduit exceptions and BAs at: www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.