Health Information Compliance Alert

HIPAA Compliance: Know the Definition of a Business Associate to Avoid Hassles and Fines

Look at the risks before you implement a BAA versus confidentiality agreement.

Once trust is lost, it's hard to get it back. And that's why it's critical to have business associate agreements in place that protect you and your livelihood should a violation occur. But before you go to the trouble of outlining another third-party BAA, make sure you needit.

In the news: Last month, the HHS-OCR required the Center for Children's Digestive Health (CCDH), a small provider specializing in pediatric issues and operating from seven Illinois locations, to fork over $31,000 in fines for a "potential violation" of HIPAA due to a missing business associate agreement (BAA) with Filefax, a third-party vendor, dating back as far as 2003, an April 20, 2017 release said. Read the HHS-OCR release at: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ccdh/index.html.

The corrective action guidance suggests the lack of a BAA was discovered by the feds during a "compliance review" in 2015. "CCDH impermissibly disclosed the PHI of at least 10,728 individuals to Filefax when CCDH transferred the PHI to Filefax without obtaining Filefax's satisfactory assurances, in the form of a written business associate agreement," the resolution agreement stated. The CCDH's situation was avoidable, but the firm failed to ensure its patients' safety by following up with the vendor's execution of a BAA.

Nuts and bolts: Business associates and their subcontractors maintain PHI and ePHI just as your practice does. The level of their interaction with your practice depends on the complexity of the service they provide. A business associate (BA) is someone who performs one of these five services for a covered entity, suggested **Ryan Boggs**, **CISA, CRISC, HCISPP, CCSFP,** manager at IT advisory at BHG in Charlotte, N.C. during a session at HIMSS17 titled "Managing Risk As a Business Associate:"

- Legal work
- Accounting
- Billing
- Transcription
- Claims processing

Review: When you have identified an entity as a BA, you "must execute written contracts ... to make sure they safeguard PHI according to HIPAA standards," explains **Jo-Anne Sheehan, CPC, CPC-I, CPPM,** senior instructor with Certification Coaching Org., LLC, in Oceanville, N.J. "Business associates must do the same with any of their subcontractors who can be considered business associates."

Tip: When you've got a signed business associate agreement (BAA) on file, it binds the entity to HIPAA so make sure you get them signed, if law allows, before sharing PHI. "Business associates are subject to most of the same privacy and data security standards that apply to covered entities, and may be subject to HHS audits and penalties," Sheehan says.

Consider this: But how broad is the "business associate" label? Does it expand to your office's cleaning service? "Business associate agreements include organizations that may create, receive, maintain or transmit health information," notes HIPAA expert **Jim Sheldon-Dean**, founder and director of compliance services at Lewis Creek Systems LLC in Charlotte, Vt. Because your cleaning staff is not accessing health information in any way, they won't typically be considered "business associates."

An implemented BAA protects you and your partners if a breach occurs. Moreover, due to the costs, both financial and

personal, that arise from a violation, the complexity of a BAA to enforce HIPAA compliance make it particularly complicated. That's why it is important to know the difference between a BAA and confidentiality agreement.

Reasoning: "The cleaning staff should be under a confidentiality agreement but not necessarily a business associate agreement," Sheldon-Dean advises. "If you start asking your cleaning staff to look in the waste baskets and bring you any pieces of paper that have health information as kind of a compliance check, then they are doing something with PHI on your behalf and they'd be a business associate."

Warning: 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."

Reminder: A BAA protects you and your practice up to a point, which is why it's important to thoroughly vet your BAs and analyze and manage the risk from the get-go. "Essentially, it's your brand. If something happens at a third party, it's your news," reminded **Rodney Murray, CISA, CRISC**, principal at IT Advisory at BHG in Charlotte, NC at HIMSS17 in the "Managing Risk As a Business Associate" session.

Best bet: Protect your practice from any missteps a BA makes by getting a signed BAA on file. Look at the HHS-OCR guidance on constructing BAAs at: www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.