Eli's Rehab Report

Compliance: Know When You Need a BAA

Hint: State agencies may get a pass.

Maintaining the privacy of your patient's medical records is essential to every provider's success. But there are times when you must share protected health information (PHI) with others. How do you know when you need to ask for a signed BAA?

Good news: Most of the entities that access medical records are considered business associates (BAs), and thus subject to the Health Insurance Portability and Accountability Act (HIPAA) when handling PHI.

Bad news: "A lot of companies and people aren't required to comply with HIPAA, and there are many times when health information may be available to these people and companies," says **Jo-Anne Sheehan, CPC, CPC-I, CPPM**, senior instructor with **Certification Coaching Org., LLC**, in Oceanville, N.J.

As a covered entity (CE), you will be able to share your patient's PHI by obtaining a signed business associate agreement (BAA) from certain entities. With others, however, you cannot legally bind them to HIPAA. Check out this who's who of entities that might access PHI.

Be Aware: BAs Come Bearing Many Services

If a provider is considered a BA, you must get a BAA contract signed in order to safeguard by PHI and HIPAA standards, says Sheehan.

Remember: Many BAs perform services that don't involve patient interaction, Sheehan says. So make sure you're on the lookout for BAs of all shapes and sizes.

According to Sheehan, "BAs can perform many different services for a covered entity," including (but not limited to):

- legal
- actuarial
- accounting
- consulting
- data aggregation
- management
- administrative accreditation
- processing or administering claims

- data analysis
- data transmission
- utilization review
- quality assurance
- certain patient safety activities
- billing
- benefit management
- practice management
- re-pricing

BAs Bound By Associate Agreement

When you have identified an entity as a BA, you "must execute written contracts ... to make sure they safeguard PHI according to HIPAA standards. Business associates must do the same with any of their subcontractors who can be considered business associates," Sheehan explains.

When you've got a signed 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 [Health and Human Services] audits and penalties," Sheehan says.

Best bet: Protect your practice from any missteps a BA makes by getting a signed BAA on file. For more information on constructing BAAs, see http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

HIPAA Doesn't Apply to Gyms, Marketers

Obviously, you'll want to get a signed BAA from any entity that you can consider a BA. Don't go chasing waterfalls, though. Some entities aren't bound by HIPAA and a BAA might not do much good.

Sheehan offers these examples of entities that aren't covered under HIPAA but may handle health information:

- life and long-term insurance companies
- workers' compensation insurers, administrative agencies, or employers (unless they are otherwise considered covered entities)
- agencies that deliver Social Security and welfare benefits
- automobile insurance plans that include health benefits
- search engines and websites that provide health or medical information and are not operated by a covered entity
- marketers
- gyms and fitness clubs
- direct to consumer (DTC) genetic testing companies
- many mobile applications (apps) used for health and fitness purposes
- those who conduct screenings at pharmacies, shopping centers, health fairs, or other public places for blood pressure, cholesterol, spinal alignment, and other conditions
- certain alternative medicine practitioners

- most schools and school districts
- researchers who obtain health data directly from health care providers
- most law enforcement agencies
- many state agencies, like child protective services
- courts, where health information is material to a case.

Best bet: Consider each request carefully, and consult with an attorney if you have any questions about disclosing PHI. Handling patient information is situational, and will largely depend "on whom the provider has a BAA with," Sheehan says.

For more information on BAs, see: www.hhs.gov/hipaa/for-professionals/faq/business-associates.