Codify
BY AAPC

Optometry Coding & Billing Alert

HIPAA How-To: Review Your Business Associate Agreements Before the Feds Come Knocking

You have until September to get a handle on the recent changes.

Now that the omnibus rule is finalized, you need to review your all your practice's business relationship and ensure that all your BA agreements (BAAs) spell out the new breach notification responsibilities, the restrictions on personal health information (PHI) use, and more all before September rolls around. Here's what you need to know.

Background: The final rule brought together a slew of outstanding interim and proposed rules relating to HIPAA privacy, security and enforcement, most of which go into effect in September. Although the omnibus rule technically took effect on March 26, you'll have until Sept. 23 to come into compliance with most of its provisions, according to the law firm **Epstein Becker & Green** in a white paper.

Get to Know the Recent Changes

The omnibus rule makes significant changes to the definition of a business associate (BA), according to Epstein Becker & Green. The definition now includes the following types of entities as BAs:

- Health information organizations, e-prescribing gateways, and entities that provide data transmission services for protected health information (PHI) to a covered entity (CE) and that require access to PHI on a routine basis.
- Entities that offer personal health records to individuals on behalf of a CE; and
- Subcontractors that create, receive, maintain, or transmit PHI on behalf of another BA.

Traditionally, your BA's obligations were to comply with the BA agreement (BAA), which would dictate the requirements for using PHI with the CE, explains attorney **Wayne J. Miller, Esq.,** founding partner of the Compliance Law Group in Los Angeles.

New: But now that's changed. Not only does your BA need to comply with the BAA, but it will also be held liable under the law itself, Miller says. Another key change is a "trickle-down" effect that not only holds the BA directly liable for HIPAA violations, but also any subcontractors of the BA.

So even though the contractor or subcontractor with the CE is not actually a healthcare provider, they are now subject to direct enforcement actions and penalties if they're responsible for a HIPAA violation like a breach.

"Whatever obligations that this business associate takes on, they have to comply to the same extent ... of the law that the covered entity would," Miller states. The law also mandates that BAs provide PHI to the Centers for Medicare & Medicaid Services (CMS), patients and/or the CE, on request and pursuant to the law.

BAs also must participate in the breach notification process. If your BA has a breach on its side, the BA must notify you the CE properly and immediately. Additionally, BAs must now comply with the entire security rule, starting with the risk assessment, Miller says.

According to the final rule, the CE is responsible for reporting breaches on the BA or subcontractor level the BA isn't necessarily obligated to report directly to patients or the government when a breach occurs. But the BA is responsible for reporting the breach to the CE, and this is where your BAA comes in.

You have 60 days maximum to report a breach to the government, and the clock starts ticking when you first discover the issue. You must build into your BA contract a far shorter timeframe for the BA to report any breaches to you so you can in turn report them to HHS and the affected patients.

Your responsibility: So along with these changes, CEs have more oversight responsibilities to ensure that their contractors are complying with all these new rules. You won't be directly responsible for the BA's compliance process, but you need to make sure that your BA is making appropriate strides to comply.

You also need to review your business relationships to ensure that you have BAAs in place including for those relationships with entities that now qualify as BAs under the new definition, states Epstein Becker & Green. And look over your current BAAs to ensure that they comply with the omnibus rule's requirements.

Bottom line: One thing that the final rule makes clear is that if the BA is really an agent of the CE, then the CE is responsible for the acts of the BA, Miller stresses. So you need the ability to oversee and audit the BA. And you may want indemnification provisions and warranties in your BA contract.

Why Your BA is Still Your Responsibility

Thanks to the Health Information Technology for Economic and Clinical Health (HITECH) Act, your BA now has a "direct liability" in certain respects, and not just a contract obligation, Miller notes. "It's not just the covered entity who has liability, but the business associate does, too."

"Even though you're saying, 'Well, now, it's their responsibility,' it still isn't because you have to make sure an agreement is in place," Miller explains "And you have to at least oversee and monitor that your business associate is fulfilling the requirements that they have to meet."

Not only should you ensure that your BAs adhere to certain HIPAA Privacy Rule areas such as providing "reasonable safeguards" you also need to crack down on your BA's compliance with all the Security Rule requirements. "Certainly with respect to security requirements, [BAs] have just about all of the same requirements as a covered entity," Miller notes.

Crucial: And most of all, your BAA should reflect all these updated and enhanced BA responsibilities, Miller stresses.

Protect Yourself: Tighten Up Your BAA Now

Strengthening regulations are mandating more and more provisions that you need to include in your BAA. Although not all of these are technically mandated under HIPAA rules, **Jim Sheldon-Dean,** director of compliance services for Lewis Creek Systems, advises that you include the following elements in your BAA:

- Minimum Necessary Be sure to also include specific provisions on using the limited data set.
- Disclosure Restrictions Require the BA not to use or disclose PHI other than as allowed under the BAA or by law.
- Use Restrictions Establish the permitted and required uses of PHI. Include the restrictions on marketing, fundraising and sale of PHI.
- Safeguards Include language requiring the BA to use appropriate safeguards and comply with the applicable HIPAA privacy and security rules. Require the BA to comply with any HIPAA privacy rules applicable to the BA-CE relationship.
- Accounting of Disclosures The BA must account all disclosures of PHI and must comply with the individual's right of access to ePHI. Require the BA to report to you (the CE) any unauthorized uses or disclosures of PHI, including breaches of unsecured PHI.
- Breach Notification Include all the details of breach notification requirements, including timing, harm evaluation and the reporting process.

Beware: Your BAA should outline your BA's responsibility in notifying you of any breaches "without unreasonable delay" (within 60 days), informing you of who the breach affected and contact information. You must ensure that you as the CE and your BA:

- Notify individuals of any and all breaches within 60 days;
- Report to HHS and the media within 60 days of discovery any breaches affecting 500 or more individuals; and
- Report all prior year's breaches to HHS by March 1 every year.

Expert advice: Anytime you create or update your BAA, you should have it vetted by your legal counsel, Sheldon-Dean advises. And in this increasingly contentious HIPAA climate, you need your BAA to be as legally airtight as possible.

More information: In light of recent HIPAA breaches involving covered entities' (CEs') BAs, the U.S. Department of Health & Human Services (HHS) Office for Civil Rights is issuing further guidance and information on what your BAA should look like. See the article "Ensure 10 Essential Elements Appear in Your BAAs" below for more details.