Codify
BY AAPC

Health Information Compliance Alert

HIPAA Compliance: Heads Up: Your Contracts With BAs Are Under the Microscope

Why your BAA is now more important than ever before.

The "HIPAA police" aren't fooling around in response to emerging breaches, the feds are increasing penalties. And the fines aren't just rising for providers; they're also increasing for your business associates (BAs). All the more reason to take a second look at your BA agreements (BAAs) to make sure you're covering all the bases.

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 story on page 18).

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, notes attorney **Wayne J. Miller,** with the **Compliance Law Group**. "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: The updated requirements for breach notifications are effective on March 23. 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.