Codify
BY AAPC

# Part B Insider (Multispecialty) Coding Alert

## HIPAA: Master 4 Contracts for Security and Privacy

**Tip: Factor cybersecurity into your BAAs.**

HIPAA compliance planning and training can help circumvent breaches, and adding risk assessment and analysis to that makes for comprehensive planning. Managing HIPAA, however, must include following through on the regulatory basics - and that includes having all your agreements and arrangements in line.

Read on for an overview of what you may need, depending on the work that you do, the partners you deal with, and the information you distribute.

**Know These 4 Major Agreements**

If patients' protected health information (PHI) is transmitted, transacted, or used at your organization, you are subject to following certain guidelines of HIPAA. However, covered entities (CEs) engage in all matters of business with various vendors, business associates (BAs), and other providers, and the degree and scope of PHI usage will determine both the level of data shared and the type of contract needed.

**1. Business Associate Agreement:** BAs "perform certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity," according to HHS Office for Civil Rights (OCR). Examples of BAs include health IT vendors, lawyers, accountants, billers, coders, transcribers, pharmacists, clinical labs, and more.

**Important:** To the extent that you provide a BA with access to PHI, you need to assess how much PHI the BA needs to perform its work, explains partner attorney **Laurie Cohen** of Nixon Peabody in Albany, New York. You should always limit the access to the minimum necessary.

After you've identified a partner as a BA, you "must execute written contracts … to make sure they safeguard PHI according to HIPAA standards," explains **Jo-Anne Sheehan**, senior instructor with Certification Coaching Org., in Oceanville, New Jersey. "Business associates must do the same with any of their subcontractors who can be considered business associates."

**Tip:** When you've got a signed BAA on file, it binds the entity to HIPAA - so make sure you get them signed, if time allows, before sharing PHI or electronic PHI (ePHI). "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.

Review an OCR-approved sample BAA at www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

**2. Data Use Agreement:** If you're a CE and plan on doing research or sharing limited data set (LDS) files for public health purposes, you'll need a data use agreement (DUA). In a nutshell, LDS files contain partially de-identified patient information and the DUA - a cousin of the BAA - authorizes CEs to use that data. Here are the specifics to know as outlined in the Privacy Rule:

- Use and disclose the information in the LDS only for the permitted purposes of research, public health, or healthcare operations;
- Report any breaches of those use and disclosure limits;
- Ensure that any agent or subcontractor permitted to access the LDS agrees to similar use and disclosure restrictions; and
- Prohibit the re-identification of the data or contact any individuals by using information from the LDS.

Find more details on DUAs and LDS files, including 21st Century Cures Act additions like setting research expiration dates and limitations, at www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html.

**Bonus:** "A data use agreement can be combined with a business associate agreement into a single agreement that meets the requirements of both provisions of the HIPAA Privacy Rule," advises OCR. For example, if you want a BA to use LDS files to do research for your practice, one agreement will do, the agency suggests.

**3. Organized Health Care Arrangement:** An OHCA facilitates care coordination by allowing different CEs in separate clinical settings to work together and share data under HIPAA. "The HIPAA Privacy Rule also permits providers that typically provide healthcare to a common set of patients to designate themselves as an OHCA for purposes of HIPAA," notes the American Health Information Management Association (AHIMA) in online guidance.

"By participating in an OHCA arrangement under HIPAA, legally separate covered entities without common ownership or control that are clinically or operationally integrated can more easily share appropriate and necessary information," counsels attorney **Kathleen D. Kenney** of Polsinelli LLP in Chicago.

**Reminder:** However, those involved need to remember that they still need to follow compliance standards. "The obligation, under HIPAA to ensure access and audit controls, is in place for any user that accesses a covered entity's system containing ePHI does not change because of an OHCA arrangement," Kenney points out.

**4. Confidentiality Agreement:** You likely employ workers who don't use, disclose, create, receive, maintain, or transmit PHI such as office cleaning companies or mail delivery providers. "They're not business associates," advises **Jim Sheldon-Dean**, founder and director of compliance services at Lewis Creek Systems, LLC in Charlotte, Vermont. "They should be under a confidentiality agreement, so that they know if they see anything or hear anything, they shouldn't repeat it."

**Reasoning:** "They're not doing anything with PHI on your behalf," Sheldon-Dean says, and therefore, they aren't considered your BAs. But "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," he cautions.

**Here's Why You Should Review Your Contracts Annually**

As part of your risk assessment, a thorough review of your business relationships will help you determine what agreements are necessary to align with HIPAA. It's critical to update BAs and BAAs, especially because OCR will go right to your risk management practices after a breach. And your practice could get the blame for any PHI mishaps by BAs, so make sure your agreements are watertight.

"It's not uncommon for healthcare organizations to go beyond HIPAA requirements in their BAAs, using the document as the basis for service level requirements, too. If your BAA is that comprehensive, check for language about how you want your partner to demonstrate compliance, as well as what cybersecurity requirements, if any, are specified," says **Grant Elliott**, CEO of Ostendio and co-founder and president of the Health Care Cloud Coalition (HC3).

**Tip:** So, even if you've covered your bases with an initial BAA, reevaluate your contracts.

"If you've had the same standard contract for a while, review it," Elliot says. Check to see whether you can audit the security program, whether there have been any amendments since the contract was drawn up and signed, and consider whether the contract needs any updates as cyberattacks become increasingly clever and frequent, he recommends.