# Point of Contract

## Use Business Associate Agreements to Protect Patient Information

By Pamela M. Schumacher, MS, CCMP

Providing health care in the United States relies on partnerships, contracts, and supply chains to meet operational needs. When a practice uses outside vendors to handle some of its operations, establishing comprehensive business associate agreements (BAAs) can help ensure the security and privacy of patient information.

### Getting Down to Business

Every health care provider who electronically transmits health information in connection with certain transactions is considered a covered entity under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 Privacy Rule. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which the U.S. Department of Health and Human Services has established standards under HIPAA.[1]

"Health care providers, health plans, and clearinghouses that engage in standard electronic transactions are considered covered entities under the HIPAA Privacy Rule," says Richelle Marting, JD, MHSA, RHIA, CPC, CEMC, CPMA, CPC-I, a health care reimbursement attorney in Olathe, Kansas. "However, not all health care providers are subject to HIPAA. Using electronic technology, such as email, does not mean a health care provider is a covered entity. The transmission must be in connection with a covered transaction, but if they bill electronic claims to health plans, they are probably a HIPAA-covered entity."

When a covered entity—such as a medical practice—outsources functions, activities, or services to a third party that is not a member of their workforce and the outsourced function involves a disclosure of protected health information (PHI), the third party is known as a business associate. To note, PHI is "all 'individually identifiable health information' held or transmitted by a covered entity or its business associate in any form or media, whether electronic, paper, or oral."[1] Covered entities enter BAAs to establish a legally binding relationship with business associates to ensure the protection of PHI.[1]

### In Good Company

"A [BAA] should always be based on the type of business, scope, purpose, data being shared, timeframe, and an agreement of return of data or destruction of information when it's no longer required," says Lisa J. McKeen, CMA (AAMA), who has been in the health information field since 2005 and is a privacy and security officer at General Dynamics Information Technology in New York. "The number of agreements varies and will depend on the practice."

Marting adds that the number of BAAs needed depends on the practice, its structure and specialty, and vendor types. "Some practices outsource more services than others," he explains. "Those that fulfill most of their work in-house may have substantially fewer [BAAs] than practices that outsource many services. Regardless, many software-as-a-service arrangements warrant [BAAs], and it's not uncommon to have tens or hundreds of [BAAs], even in smaller practices."

Common third parties with whom practices have BAAs include the following:

- Billing companies
- Medical record vendors

## Work in Progress

Failing to have BAAs when required is one of the most common and riskiest mistakes a practice can make, says Richelle Marting, JD, MHSA, RHIA, CPC, CEMC, CPMA, CPC-I. Follow these steps to ensure your practice is covered:

- **Develop a contracting process.** Decide how to assess whether a BAA is needed—based on the specific scope of work requested—and who reviews those requests. Identify how individuals throughout the practice can request a BAA for new vendors (e.g., for a new shredding company or a new after-hours call service provider).
- **Do the hardest work once.** Develop a standard BAA template you are comfortable with, and always ask vendors to sign the standard document first.
- **Have a checklist of required provisions for your practice** and a list of important provisions such as limitation on liability, governing law, and timeframes for reporting breaches in case a vendor will not use a provider's agreement.
- **Save BAAs on file** along with their related fully executed agreements and maintain a list of those companies with which you have BAAs. The Office for Civil Rights typically begins audits with a request for such a list, so it saves time to always have one on hand.

- Legal counsel
- Cloud service providers
- Consultants
- Pharmacy benefit managers
- Collection agencies
- Peer review companies
- Risk management vendors
- E-prescribing gateways
- PHI data destruction services
- Information technology support
- Password management vendors
- Medical answering services

### Safe Keeping

"To understand what is required, start by going to HHS.gov. Using the search button, you can pull up the criteria for a BAA and an example," says McKeen. "You can also check HealthIT.gov. These sites will give you the federal regulations. You don't necessarily need a lawyer to draft these agreements."

In addition to describing the permitted and required uses of PHI by the business associate, a BAA must do the following at a minimum:

- Stipulate that the business associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law.
- Require the business associate to use appropriate safeguards to prevent the use or disclosure of the PHI.

…

- Require the business associate to ensure that any subcontractors with access to PHI agree to the same restrictions and conditions that apply to the business associate.
- Authorize the termination of the contract by the covered entity if the business associate violates any term of the agreement (and vice versa).[2]

Marting cautions practices against relying solely on boilerplate agreements. "[BAAs] need to be carefully reviewed, understood, and negotiated, because they can create liability for the practice if not handled appropriately. Some things to watch out for include any limitations on liability. Look for a heading titled, 'Limitation on Liability.' Business associates may try to include language stating they do not have any liability to the covered entity or their liability is limited to some amount, such as a month's worth of services. These limits are often woefully inadequate to compensate the covered entity for the potential damages if the business associate causes a data breach."

Another area she highlights to be aware of is the timeframe in which the business associate must report potential breaches. "Covered entities have strict deadlines if an event becomes a breach and need sufficient time from when the business associate reports an event to investigate and make appropriate reports, if necessary. The covered entity's deadline begins when its business associate knows of the event, not when they report it to the covered entity.

"Also, look at whether business associates reserve the right to sell the covered entity's data. Selling PHI requires certain specific consent from patients. Business associates may attempt to avoid that disclosure and consent step by indicating they may de-identify data to make it no longer protected under HIPAA. Still, practices may have concerns with their business associates profiting from the practice's data and may wish to address or prohibit any sale of the data, whether or not it is identifiable," says Marting.

When it comes to PHI, McKeen recommends having a written policy prohibiting its sale: "That way, the third party or business associate must comply with your policy and procedures pertaining to PHI, and you'll be better protected if there's a breach.

"I always stress the importance of understanding the HIPAA privacy, confidentiality, and security requirements to medical office staff," adds McKeen. "Medical assistants should know the terms of the [BAAs] and what is and is not allowed. Sometimes, staff will unintentionally overshare patient information; in other instances, they may accidentally obstruct care by not disclosing enough patient information." ✦

**References**


1. Summary of the HIPAA Privacy Rule. US Department of Health and Human Services. Reviewed October 19, 2022. Accessed August 15, 2024. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
2. HIPAA Business Associate Agreement. The HIPAA Journal. Accessed August 15, 2024. https://www.hipaajournal.com/hipaa-business-associate-agreement/