AssuredPartners

Brokers as Business Associates

February 2025

What Is a Business Associate?

In general, a business associate is any third-party that performs plan administration functions on behalf of a covered entity when those functions involve the use and/or disclosure of protected health information (PHI). Often, brokers will provide services to their clients such as health plan administration assistance; coordination with third-party administrators and/or carriers to resolve employee benefits and claims issues; data analytics; and other activities related to the creation, renewal, or replacement of a health insurance contract. Sometimes brokers will even provide software platforms to clients for their use in managing/administering their health plans and those platforms store PHI. When any of these services involve the use of PHI, the broker is almost certainly acting as a business associate on behalf of the client's health plan.

Under HIPAA's privacy requirements, employers (on behalf of their health plans) must enter into business associate agreements (BAAs) with any business associates before disclosing PHI to the business associate. A BAA essentially passes down the same privacy and security protections that apply to the health plan to the business associate. It is a way for employers to ensure that any PHI they entrust to third parties remains protected.

Who Is Responsible?

Technically, it is the employer's responsibility to ensure that any required BAAs are put in place on behalf of the health plans they sponsor for their employees. But employers may not realize that a BAA is necessary or understand when it is required. Therefore, a broker may want to consider proactively providing a BAA to its clients when it knows it is providing business associate services to that client. Adopting this practice may also help address the following potential issues:

1. An employer may misunderstand how much PHI they interact with or share with their vendors. Unless an employer is truly limiting the amount of information it shares with third parties to enrollment data and/or highly aggregated data ("summary health information"), a BAA will be necessary. As compliance advisors to their clients, brokers provide valuable protection to their clients by proactively providing a BAA. The Office for Civil Rights (OCR), which provides regulatory oversight of HIPAA's compliance requirements, has stated in its most recent HIPAA audit protocol that audits will include reviews of a covered entity's process for identifying and entering into BAAs with business associates. Therefore, ensuring that clients are covered from this perspective, at least with respect to their brokers, is a good idea.

2. The regulators have been clear that a business associate relationship exists even in the absence of a written contract. In other words, a vendor does not avoid business associate status by failing to execute a written agreement. If a broker is interacting with PHI on its client's behalf, then it is acting as a business associate (and a written agreement is required). Since business associates are directly liable for ensuring that they do not use or disclose PHI beyond what the terms of a BAA permits, having a BAA in place and abiding by its terms/limitations is crucial for compliance.
3. From a practical perspective, it is administratively easier for a broker to comply with a standard set of requirements in a single template BAA than trying to manage the different terms provided in a disparate set of BAAs provided by individual clients. Brokers that have a standard BAA template that they are familiar with and provide proactively to their clients will have a much easier time ensuring that they are abiding by the terms of the BAA.
4. Finally, sometimes vendors will ask brokers whether there is a BAA in place between the broker and their employer clients and may even refuse to provide a broker with data unless there is one in place, whether it was technically necessary or not. To avoid this, many brokers find it easiest to procure a BAA up front.

What About Clients with Fully Insured Plans?

Some brokers may wonder if a BAA is necessary in cases where a client only has fully-insured plans and has adopted a "hands-off" approach to administration – i.e., is truly limited to interacting with enrollment and/or summary health information (which is highly aggregated and by definition almost completely de-identified). While a BAA is technically not required in this instance, it may still be prudent to consider entering into a BAA. As noted above, employers may misunderstand the extent to which they are interacting with PHI. Or they may only think about certain health plans (e.g., a fully insured medical plan) and fail to consider other self-funded health plans such as health FSAs or HRAs, where additional HIPAA compliance obligations exist. In addition, plan designs change regularly, and if an employer switches to a funding mechanism/plan design that does entail additional access to PHI down the road, having a BAA already in place eases future administrative burdens. For these reasons, it is usually safest for brokers to put a compliant BAA in place with their employer clients regardless of plan funding. Doing so will protect the employer, as plan sponsor, if the employer were to inadvertently share information with its broker that goes beyond the allowable enrollment and/or summary health information. And remember to keep in mind that if employers do have more extensive PHI, they will also need to consider additional compliance obligations under HIPAA.

For assistance in drafting a compliant BAA, a link to the model HHS BAA may be found here: Model Business Associate Agreement (hhs.gov).

Caution: The Minimum Necessary Rule

There are many rules about appropriate use and disclosure of PHI, but one major requirement is known as the "Minimum Necessary Rule." The general idea behind this rule is that even when a use or disclosure of PHI is appropriate, a person should limit the type and amount of information being used/disclosed to the minimum necessary to accomplish the task at hand. While some exceptions apply, this rule should generally be applied whenever using or disclosing PHI for routine or non-routine purposes.

There are several ways the Minimum Necessary Rule can be violated. First, sometimes organizations allow too many people to access PHI, or allow access to more PHI than needed to carry out their responsibilities. Another common situation occurs when too many people are looped in on an issue. Even if technically it's permissible to share PHI with somebody (e.g., because there is a BAA in place), that doesn't mean every disclosure is necessary. It is important to think about who information is being shared with and consider whether that person really needs to see PHI to help resolve an issue.

Again, Who Is Responsible?

Plan sponsors must comply with the Minimum Necessary Rule by considering what type of PHI is appropriate for the various types of uses/disclosures it engages in. For example, an employer might routinely interact with its TPA for its self-funded plans. Or certain employees responsible for plan administration may routinely work with one another to resolve various types of benefits-related issues. These types of activities should be considered and organizations should have a clear sense of what type of information is appropriate in carrying them out.

But business associates are not off the hook! In general, business associates must also ensure that they limit the amount of PHI they use and disclose to the minimum amount necessary to carry out their plan administration functions on behalf of their clients. Business associates, including brokers, should be sure to review the terms of their BAAs to determine if there are specified limitations on the amount or type of PHI they are permitted to use or disclose on the covered entity's behalf. Brokers acting as business associates should also have policies and procedures in place that describe how they comply with the requirements of HIPAA Privacy and Security Rules. These policies will cover many things, but one important thing that should be addressed is exactly how the client's PHI is handled by the business associate, including who has access to that information and what the processes are for using and disclosing it.

While every effort has been taken in compiling this information to ensure that its contents are totally accurate, neither the publisher nor the author can accept liability for any inaccuracies or changed circumstances of any information herein or for the consequences of any reliance placed upon it. This publication is distributed on the understanding that the publisher is not engaged in rendering legal, accounting or other professional advice or services. Readers should always seek professional advice before entering into any commitments.