AssuredPartners

Identifying Business Associates

Date Issued: May 2023

Part of any HIPAA compliance project involves the process of reviewing existing vendor relationships to determine which vendors are acting as business associates on behalf of the health plan and ensuring that compliant business associate agreements (BAAs) are in place with these vendors. While some business associates such as third-party administrators are easily identified, there are other, less obvious vendors that should also be considered in this process. In order to properly identify all business associates, employers must first consider which health plans they sponsor are subject to HIPAA's privacy and security requirements, what information they interact with on behalf of such plans, and how that information flows throughout their organization and to and from their vendors.

What are Business Associates?

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). Such services may involve third-party administration services; 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; care and disease management; provision of software platforms that store PHI; and even shredding services for paper PHI. Ultimately, it is important for employers to review its vendor relationships in light of two questions:

1. Does the vendor perform some type of plan administration service on behalf of the health plan? (In other words, is the service being provided related in some way to administration of the employer's health plan?)
2. In performing such service, does the vendor interact with PHI in any way?

Process for Identifying Business Associates

To answer the first question, employers must understand what health plans they sponsor that are subject to HIPAA, and what individually-identifiable information they interact with on behalf of such plans. Many employers know that their medical plans are subject to HIPAA, but aren't always aware that their health FSAs, long-term care, or certain voluntary products are also in scope. So having done a thorough analysis of health plans and the flow of information related to such plans is a necessary first step. Common plans sponsored by employers that are or may be subject to HIPAA include:

- Medical
- Dental

- Vision
- Prescription Drug
- Employee Assistance Programs (EAPs) when counseling is provided
- Wellness Programs that are integrated with the medical plan or that provide or pay for medical services
- Long-Term Care Plans
- Critical Illness/Hospital Indemnity Policies that pay on a per-service basis
- Health Flexible Spending Accounts (HFAs)
- Health Reimbursement Arrangements (HRAs)

Second, employers must consider what type of information they interact with on behalf of their health plans to administer them. Remember that "Protected Health Information," or "PHI," refers in general to "information that is created or received by the plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant." This includes things like demographic, enrollment, premium, and benefit information, along with claims, treatment and diagnosis information if that information comes from health plan records or is being used in some capacity related to plan administration. Next, employers must consider who internally has access to PHI, and where that PHI is stored/transmitted/exchanged. Common locations of PHI include:

- Shared network folders
- Document management systems (OneDrive, Box, etc.)
- HRIS systems
- Payroll systems
- Email
- Teams (or similar chat platforms)
- Internet-based telephone systems (VoIP)
- Paper files
- Printer hard drives (if PHI is printed)
- Mobile devices (e.g., when used for email or other platforms that contain PHI)

Typically, employees in HR, benefits, payroll, finance, and IT have some type of access to PHI. So reviewing these locations and internal business roles will usually yield a solid understanding of how PHI is received, stored, and transmitted for purposes of health plan administration.

Having accounted for all health plans, health plan information, and how that information flows/is stored, an employer is ready to review its vendor relationships and answer the second question to identify any business associates. (See how it all starts to fit together? No single compliance step really stands alone!).

As mentioned above, some business associates will be obvious – for example, the third-party administrator who administers one or more of the employer's health plan will be a business associate. (Note – carriers who administer fully insured plans are not considered business associates because they are covered entities in their own right and have to comply with HIPAA in that capacity.) Brokers will likely act as business associates, as will some attorneys. COBRA vendors may be business associates if they are receiving health plan information in order to administer COBRA benefits. These are some of the more obvious relationships. But there are other, less obvious relationships that must be considered as well. For example:

- The Department of Health and Human Services (HHS) has made it clear in its guidance that **cloud services providers** are business associates when they are providing software/applications that are used to store or transmit electronic PHI. Therefore, employers must consider who provides their HRIS/benefits platforms, and if PHI is exchanged via email or stored in network folders, what company provides those services?
- Many phone systems now operate through the internet rather than through landlines. If an **internet phone services provider** is able to store/record information that is transmitted, then it would also be a business associate if PHI is discussed verbally over the phone.
- IT Departments may want to consider whether it has **third-party IT vendors** who provide any sort of assistance that involves access to systems that contain PHI. And employers cannot forget about paper PHI! If they discard paper PHI properly by shredding it, then any vendor responsible for collecting that shredding would also be considered a business associate.
- Similarly, paper-based **document storage vendors** (e.g., Iron Mountain) are business associates if they are storing files that may contain PHI (like old enrollment files).
- HHS has recently issued guidance regarding **health application vendors** – i.e., vendors that provide certain wellness/fitness apps that collect and track individual data. If employees are using these applications in connection with a wellness program or the medical plan, then the vendors would be considered business associates and a BAA would be necessary.

Vendors that are not performing a plan administration function should not be accessing PHI, and vendors that are performing a plan administration function should have a BAA in place before they interact with any of the plan's PHI. 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 and secured.

Conclusion

To sum up, identifying business associates is one piece of the larger compliance puzzle, and must be addressed in tandem with other privacy and security considerations. We also see business associate relationships appearing in some less obvious situations, so it is vitally important that organizations thoroughly account for all PHI they interact with to properly identify the third parties who may interact with that information and ensure that compliant agreements are in place.

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.