COMPLIANCE ALERT

When Is a BAA Required?

June 1, 2023

Quick Facts

- Part of Health Insurance Portability and Accountability Act (HIPAA) compliance includes determining whether vendor partners are business associates of a covered entity, requiring a business associate agreement.
- A business associate agreement passes down the same privacy and security protections that apply to the health plan to the business associate.
- Covered entities should complete a thorough analysis of health plans and the flow of information related to such plans is a necessary first step in determining which plans are subject to HIPAA as sometimes who is a business associate is not obvious.

Background

Part of compliance with HIPAA, 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 (TPAs) are easily identified, other, less obvious vendors should also be considered in this process. 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.

Business Associate Agreements

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
- shredding services for paper PHI.

Ultimately, employers need to review their vendor relationships in light of two questions:

1. Is the service that's being provided related in some way to the administration of the employer's health plan?

2. In performing such a service, does the vendor interact with PHI in any way?

Vendors that are not performing a plan administration function should not access 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 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.

Which Plans Are Subject to HIPAA?

Employers must understand which health plans they sponsor 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 may also be within HIPAA's scope. Completing a thorough analysis of health plans and the flow of information related to such plans is a necessary first step in determining which plans are subject to HIPAA. 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 (HFSAs)
- Health Reimbursement Arrangements (HRAs)

Employers must consider what type of information they interact with on behalf of their health plans. For this purpose, they 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.)
- Human Resource Information System (HRIS) programs
- Payroll systems
- Email
- Teams (or similar chat platforms)
- Internet-based telephone systems
- Paper files

Typically, employees in human resources (HR), benefits, payroll, finance, and information technology (IT) have some type of access to PHI. Employers should review these internal business roles to 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 to identify any business associates.

Unlikely Business Associates

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, however, that 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. Vendors that administer coverage under the consolidated omnibus budget reconciliation act (COBRA) 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 other, less obvious relationships 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, and what company provides those services.
- Many phone systems now operate through the Internet rather than through landlines. If an **internet phone services provider** has the ability to store/record information that is transmitted, then it would also be a business associate if PHI is discussed verbally over the phone.
- An employer's IT Department should consider whether it has **third-party IT vendors** who provide any sort of assistance that involves access to systems that contain PHI. Additionally, if employers discard paper PHI properly by shredding it, then any vendor responsible for collecting that shredding would also be considered a business associate.
- Paper-based **document storage vendors** are business associates if they store files that may contain PHI (such as old enrollment files).
- HHS recently issued guidance for **health application vendors** – i.e., vendors that provide certain wellness/fitness apps that collect and track individual data stating that employees use these applications in connection with a wellness program or the medical plan, then these vendors would be considered business associates and a BAA would be necessary.

Summary

Identifying business associates is one piece of the larger compliance puzzle and must be addressed in tandem with other privacy and security considerations. Business associate relationships appear in some less obvious situations, so it is vitally important that organizations thoroughly account for all protected health information they interact with to properly identify the third parties who may interact with that information and ensure that compliant agreements are in place.

EPIC Employee Benefits Compliance Services

For further information on this or any other topic, please contact your EPIC benefits consulting team.