BCLP. Client Intelligent

Insights

THE HIPAA TRAP (PART 2): ARE YOU ACTUALLY A BUSINESS ASSOCIATE?

Oct 02, 2025

Whenever the topic of health and medical data comes up, there is often a prevailing assumption that this information is subject to the federal Health Insurance Portability and Accountability Act (HIPAA) just by virtue of being health and medical data. In reality, HIPAA applies to a much narrower set of organizations than generally understood, and the consequences for getting it right are significant. This alert provides a brief roadmap for companies trying to understand their role under HIPAA and the related implications. In our first alert on this short series ("The HIPAA Trap: Are You Actually a Covered Entity?"), we focused on covered entities. In this installment, we focus on business associates.

ARE YOU A BUSINESS ASSOCIATE?

HIPAA's applies to **covered entities** and their service providers, **business associates**. Covered entities have primary responsibility for HIPAA compliance, but business associates are also directly responsible for complying with significant portions of HIPAA and can face related enforcement for failure to comply with these obligations. Contractual liability can also be layered on, as business associates are required to enter into a Business Associate Agreement ("BAA") with all covered entity customers.

HIPAA defines a "business associate" as: a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information ("PHI") on behalf of, or provides services to, a covered entity. The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other regulated functions or activities.

Business associate functions and activities include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Services specifically identified under HIPAA as business associate services are legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial services, but other types of services can also qualify.

An organization needs to unpack the various pieces of this definition to determine whether it qualifies as a business associate. If the customer is not a HIPAA covered entity, then the provider is *not* a business associate. If the services do not require use (including access to) or disclosure of PHI, then the organization is *not* a business associate. Finally, the services generally need to fall into one of the types of services listed above; although, most activities that meet the first two points generally qualify as business associate functions. There is a tendency for covered entities to assume that any service provider is a business associate and to try to push down a related BAA, so it is important that service providers undertake this analysis for themselves and document their decision-making process, particularly when they do not fall into the business associate category.

WHAT IS A BUSINESS ASSOCIATE REQUIRED TO DO?

HIPAA is broken into the Privacy Rule, the Security Rule, and the Breach Notification Rule. Each of these rules applies either indirectly or directly to business associates.

PRIVACY RULE

The Privacy Rule imposes a number of obligations on organizations to protect the privacy of PHI by requiring notices of privacy practices, the implementation of appropriate safeguards, and by setting limits and conditions on the uses of PHI, including establishing when individual consent is required. Many of the obligations established by the Privacy Rule (e.g., obligation to provide a HIPAA compliant notice to patients) *do not* apply directly to business associates, but covered entities are required by the Privacy Rule to push down BAAs on business associates. HIPAA establishes specific mandatory, detailed minimum content for such agreements that imposes many of the Privacy Rule obligations onto business associates. As a result, business associates are contractually bound to comply with many of the HIPAA Privacy Rule requirements. Similarly, business associates are required to impose these same obligations on any subcontractor (sub- or downstream-BAA) that has access to or receives PHI as part of its services.[1]

SECURITY RULE

As opposed to the Privacy Rule, business associates are *directly* responsible for compliance with most sections of the Security Rule, and compliance with this dense portion of HIPAA is a significant effort both in terms of meeting the requirements as well as documenting compliance in the manner required by HIPAA. Business associates are obligated under the Security Rule to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information ("ePHI") [it holds]" (the "risk analysis") as well as to develop a plan to address and manage gaps identified by the risk analysis.

A business associate must also document its compliance with specific security requirements established by the Security Rule, which includes both "Required" and "Addressable" safeguards.

“Required” safeguards are those that HIPAA mandates the entity to implement. “Addressable” safeguards are those that are not required if it would not be reasonable and appropriate to implement the safeguard. In determining whether an addressable safeguard should be implemented, an entity must assess whether the safeguard is a reasonable and appropriate safeguard in its environment, when analyzed with reference to its likely contribution to protecting ePHI. If the safeguard is a reasonable and appropriate safeguard, the entity must implement the safeguard. If the entity determines the safeguard is not reasonable and appropriate, the entity must:

1. Document why it would not be reasonable and appropriate to implement the safeguard, and

2. Implement an equivalent alternative safeguard if reasonable and appropriate to do so.

Complying with the Security Rule is the most complicated aspect of building a HIPAA compliance program and one that often also goes overlooked for business associates. It is not unusual for organizations to assume that the implementation of a robust security program is sufficient to meet these requirements, but they must also map their security measures to the specific requirements of the Security Rule and document them in accordance with the rule.

BREACH NOTIFICATION RULE

The Breach Notification Rule requires covered entities and business associates to provide notification in the event of a qualifying breach of unsecured PHI, but notification requirements differ between covered entities and business associates. Whereas a covered entity may be obligated depending on the circumstances to notify individuals, the HIPAA enforcement agency (Office of Civil Rights) and the media, a business associate must only provide notice to the covered entity, without unreasonable delay and no later than 60 days from the discovery of the breach. Where possible, the notification must identify those individuals whose PHI has been or is reasonably believed to have been breached and also provide information that the covered entity needs for its own notifications. Covered entities can and do, however, negotiate the terms of BAAs to make them stricter than the requirements under HIPAA and also often impose indemnification and limitation of liability carve outs for qualifying breaches, such that compliance with the breach notification rule is often the floor of requirements that apply to business associates.

WHY DOES IT MATTER?

Business associates have been directly subject to HIPAA since the 2013 HITECH amendments, but it continues to be common for organizations to execute BAAs without a real evaluation as to whether they actually fit this role or whether they have met their obligations under HIPAA. This approach is risky, however, for a number of important reasons. Business associates that do not meet their privacy and security obligations can face significant penalties and other repercussions, including enhanced monitoring and reputational harm. Violations of HIPAA can lead to the

imposition of significant penalties on business associates, including fines that can range from $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for each violation (noting that these amounts are adjusted for inflation). Business associates can also face contractual liability for violations of their agreements with their covered entity customers. Because most business associates serve multiple customers, the multiplier effect of a violation across the underlying agreements along with negative publicity and reputational harm can be catastrophic.

On the flip side, companies that assume that they act as a business associate – either based on a misunderstanding of the role or the presumption from customers – set themselves up for significant contractual compliance obligations that they are not legally required to undertake and significantly limit that manner that they might otherwise be able to use information received under the agreement (e.g., negotiated rights to use data for internal purposes, AI model training and other uses that would generally be restricted under HIPAA). Companies may also overlook obligations under state privacy laws regarding health and medical data if they assume that HIPAA would otherwise apply. Therefore, it is critical for organizations to truly understand their role with regard to health and medical data and to tailor their compliance efforts accordingly.

[1] *See* 45 C.F.R. §§ 164.502(e) & 164.504(e).

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Andrea Rastelli

Boulder

andrea.rastelli@bclplaw.com
+1 303 417 8564
