BCLP. Client Intelligent

Insights

THE HIPAA TRAP: ARE YOU ACTUALLY A COVERED ENTITY?

Aug 05, 2025

Whenever the topic of health and medical data comes up, the prevailing assumption often is that any of 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, though, HIPAA actually 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.

ARE YOU A COVERED ENTITY?

HIPAA's privacy and security rules apply to **covered entities** and their service provider, **business associates**. While both covered entities and business associates are directly responsible for complying with HIPAA and can face related enforcement, covered entities have primary responsibility for HIPAA compliance.

To qualify as a covered entity, an organization must fall into one of the following three categories of entities:

- Health plans;
- Health care clearinghouses; or
- Health care providers (including traditional providers, laboratories and pharmacies) that transmit any health information in electronic form in connection with a transaction covered by HIPAA.

For purposes of this alert, we focus on what types of health care providers are in-scope for HIPAA, as this is the area in which we often see confusion. As indicated in the definition, not all health care providers are covered by HIPAA. To be a covered entity, health care providers must also engage in certain covered transactions that involve the electronic transmission of PHI between two parties to carry out financial or administrative activities related to health care. Such transactions include those related to claims, health care payments, coordination of benefits, eligibility verification, or

referral authorizations. Although a bit of an oversimplification, a good rule of thumb is if a health care provider (including a pharmacy) does not accept insurance and, instead, requires patients to self-pay for their care, the provider is likely not subject to HIPAA. Common examples of these types of organizations are specialty or small medical or other practices (e.g., physical therapists, counselors, chiropractors) or specialty pharmacies that may not take insurance for a variety of reasons (administrative burdens, cost/reimbursement issues, enhanced legal liability).

Business associates are persons or entities that perform certain functions or activities involving the use or disclosure of PHI on behalf of, or provides services to, a covered entity. Again, though, if a service provider receives health and medical data from an entity that does not qualify as a covered entity, then neither the service provider nor the health and medical data is subject to HIPAA in this context.

WHY DOES IT MATTER?

Companies that are subject to HIPAA but do not meet their privacy and security obligations can face significant penalties and other repercussions, including enhanced monitoring and reputational harm. On the flip side, companies that wrongfully assume that they or information they receive in a given instance is subject to HIPAA could miss complying with state privacy and other laws that apply when HIPAA does not (e.g., the Washington My Health My Data Act or the sensitive personal information provisions of the California Consumer Privacy Act).

We have also seen a significant uptick in data breaches targeting health care providers, particularly smaller providers whose security might be more vulnerable to an attack. It is imperative for providers and other companies that handle health and medical data to understand where they sit in the regulatory framework with respect to this data so they can appropriately meet their legal obligations.

RELATED CAPABILITIES

- Data Privacy & Security
- Healthcare & Life Sciences

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
