Haekka

Lesson 2 | Organizations and contracts under HIPAA

Updated 2020-09-12

Entities under HIPAA

HIPAA is strict in how it defines entity types. And those entity types determine whether organizations need to comply with HIPAA and determine the liability of the organization.

When HIPAA was written, it was explicit about the types of organizations that needed to comply with it. HIPAA defines two types of organizations:

1. **Covered Entities.** These include healthcare providers, healthcare insurance companies, and healthcare clearinghouses (healthcare transaction processors).
2. **Business Associates.** These are organizations that covered entities work with 3rd party organizations to help carry out operations and have access to health data. The most common business associates are electronic health record (EHR) companies and revenue cycle management (RCM) companies.

Covered entities are a relic of traditional healthcare delivery. HHS defines covered entities as entities that deliver care and "electronically transmit health information in connection with certain transactions"; "transactions" here mean traditional insurance claims. The last ten years have seen new technology-enabled healthcare delivery models and services, many of which do not fit the mold of how HIPAA defines covered entities and, as such, do not have to comply with HIPAA. Direct to consumer mobile or web apps that collect and provide medical guidance or "care", either by providers or AI / ML, but do not transmit standard transactions, are not covered entities under HIPAA.

In 2013, HIPAA was updated to extend the definition of business associates to include 3rd party organizations that assist business associates. It called this new layer of business associates "subcontractors", or essentially business associates of business associates. The most common subcontractors are technology companies like cloud service providers (AWS, Microsoft Azure, and Google Cloud Platform).

Under HIPAA, covered entities are the owners of health data. They also own the liability for health records if a data breach occurs. When a covered entity works with a business associate, they extend that liability to the business associate through a business associate agreement. When a business associate works with a subcontractor, they extend their own liability to the business associate through a business associate agreement.

As you can imagine, there are 1,000s of covered entities and almost all of them are large organizations with complex operations. Most covered entities work with many different 3rd party organizations as business associates. Business associates, increasingly reliant on technology partners, have many subcontractors. Because of this chain of liability from covered entities to business associates to subcontractors, there are tons of business associate agreements and tons of liability in healthcare. It's a mess and a lawyer's dream.

Business Associate Agreements

The most important form of agreement under HIPAA is the business associate agreement (BAA). Much of where the rubber meets the road in HIPAA is defined in business associate agreements. BAAs are a key requirement of HIPAA and are mandated between business associates and covered entities as well as business associates and subcontractors.

BAAs define the responsibilities and liabilities of entities under HIPAA. Covered entities are at the root of HIPAA and all liability under HIPAA emanates out from them. Covered entities technically "own" PHI and patients. Business associates provide technology and services to covered entities.

A business associate agreement could include clauses on breach reporting times, use of de-identified data, responsibilities during a breach, liability for certain security features, and configurations. and a host of other elements.

There is not a standard template for BAAs. As BAAs chain together entities from covered entities through multiple business associates, the responsibilities and liabilities become very opaque.

Below is an example of a chain of organizations linked by business associate agreements.

- A covered entity works with a telemedicine provider. There is a BAA in place between them that mandates the telemedicine provider to notify the covered entity of a breach within 72 hours.
- The telemedicine provider leverages a cloud platform for its technology. There is a BAA between the telemedicine provider and the cloud platform provider. Under the BAA, the cloud platform provider is mandated to notify the telemedicine provider of a breach within 60 days (max allowable under HIPAA).

The above is a simple and pretty typical example. In this example, the telemedicine provider may not learn about a data breach for 60 days, and only then would be able to notify the covered entity. Many times, BAAs from covered entities put clauses into BAAs that require their business associates to have terms as strict, or more stringent, than the covered entities BAAs. In practice, this can easily be violated.