Lesson 3 | Agreements Under HIPAA - BAAs

Updated 2020-09-12

Agreements under HIPAA - Business Associate Agreements (BAAs)

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.

If you are a business associate, read and understand your BAAs as they will define many of your requirements under HIPAA.