Lesson 5 | HIPAA Recap

Updated 2020-09-12

This is a short HIPAA course. If HIPAA is new to you, the objective is to introduce you to the fundamental concepts contains within HIPAA. If HIPAA is not new to you, the goal is to ideally reiterate things you already know or terms you've already learned.

Before closing out this course, we want to quickly cover several HIPAA-related topics (some new, some we already covered but want to make sure they stick).

HIPAA Compliant

Contrary to popular belief, there is no such thing as "HIPAA Compliant." The term has no meaning since there is no approved certifications, audit process, or assessor. And, even if an audit is done, it is a point in time assessment. The only way to comply with HIPAA is to create and operationalize policies and procedures for all requirements in HIPAA. Then, on a continual basis, you need to monitor and document these. A more accurate way to say "We are HIPAA Compliant" is to say, "We comply with the rules of HIPAA."

Roles under HIPAA

HIPAA does require that you assign individuals to specific roles. There are two roles that need to be assigned - a privacy role and a security role. Roughly speaking, the privacy role is accountable for things in the Privacy Rule, while the security role is accountable for the items in the Security Rule. The titles your company uses do not matter. And one person can fill both roles though this is not best practice as it does not create a system of checks and balances. One person filling both roles is common for small companies and startups.

The Cloud and HIPAA

Modern technology companies run on the cloud. Usually, all of the internal software they run is cloud-based (SaaS) - Salesforce for sales, Hubspot for marketing, Zendesk for support, Google for email and docs, Zoom for video conferences, Slack for messaging, on and on. And their products are hosted on cloud providers like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). The cloud, whether SaaS or a cloud provider, is allowed under HIPAA. The key things, if you're using the cloud for PHI, are 1) to make sure you have business

associate agreements (BAAs) in place with cloud providers and 2) to configure these services and platforms to align with your company policies, which should, in turn, align with HIPAA.

Protected Health Information (PHI)

PHI is what matters to HIPAA. It is health information that can be associated or linked to an individual and is *held by a covered entity*. The last part in italics is important. If you aren't a covered entity - meaning you don't deliver care, aren't an insurance company, or don't process healthcare claims - or a business associate working for a covered entity, then HIPAA does not apply to you.

Covered Entities and Business Associates

There are two types of entities under HIPAA. Covered entities, who own PHI. Covered entities work directly with end-users, either as patients or members, or are a special class of companies called a clearinghouse. Business associates provide products and services to covered entities and somehow touch (store, transmit, or process) PHI. Business associates also provide products and services to other business associates, like a cloud provider to a digital health company.

Business Associate Agreements

Business associate agreements (BAAs) are required by HIPAA between covered entities and their business associates and between business associates and their business associates, sometimes referred to as subcontractors. These agreements outline the obligations of each party under HIPAA for things like breach investigations and reporting times. BAAs are essential, and there are not industry templates.

Privacy Rule and Security Rule

For the purposes of this course, HIPAA has two sections. The Privacy Rule defines PHI, allowable disclosures of PHI, and mandates the creation of company policies and procedures. The Security Rule outlines the requirements for securing operations and technology.

There's much more to HIPAA than what we've included in this training. We have specialized HIPAA courses for those in sales and marketing, technology, and operations. As opposed this general-purpose HIPAA primer, those courses focus the HIPAA regulation to the specific needs of your job function. You should do some kind of annual HIPAA refresher, whether retaking this course (we update the scenarios, so the content is not the same) or one of our other HIPAA courses.