Lesson 1 | Introduction to HIPAA

Updated 2020-09-12

What is HIPAA?

HIPAA isn't hard. It's just opaque, and the organizational penalties can be high, so people fear it.

HIPAA stands for Health Insurance Portability and Accountability Act. It was enacted by Congress in 1996. It went into effect in stages from 2001 to 2006. The intention of HIPAA is to standardize healthcare transactions and to create protections for the use of protected health information (PHI).

For the purposes of this HIPAA training, the area we are focused on is the protection of PHI. When it comes to protecting PHI, the essence of the HIPAA rules can be distilled down into two sections.

1. **Privacy**. Ensuring access to PHI is only allowed for approved purposes (care delivery and billing are the most common purposes under HIPAA). This is where your privacy policies and procedures come from. This is the when and why of HIPAA.
2. **Security**. Ensuring best practices to secure processes and technology. This is where your policies and procedures are implemented. This is the how of HIPAA.

Data covered under HIPAA

HIPAA is concerned with protected health information (PHI). Think of PHI as identifiable data, or personally identifiable information (PII), that is associated with health data. PII + health data = PHI. Health data can be health status (condition, medication, etc), payment for health services, and delivery of care.

To determine if data is PHI, one additional filter needs to be applied. According to Health and Human Services (HHS) - PHI is personal health information *held by covered entities*. Identifiable health data held by an Internet site or mobile app that is not owned or being used by a covered entity is not PHI. Many direct to consumer health companies, such as personal health record

storage companies, are not covered entities so the identifiable health data they collect, store, and process is not PHI.

HIPAA is focused on traditional care delivery organizations and has not been updated to reflect new approaches to care, especially direct to consumer health offerings. As such, not all identifiable health data is PHI.

While HIPAA remains behind the times when it comes to care delivery models, the definition of PII has evolved over the last several years with expanded digital footprints and new technologies. In addition to traditional items like names, social security numbers, medical records numbers, things like social media account names, IP addresses, cookies, and even web browser profiles can identify individuals or be used to trace the identity of individuals.

The US Government defines PII as “information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.”

A (slowly) evolving standard

At the time it was written in the late 90s and early 2000s, HIPAA was almost exclusively concerned with traditional healthcare organizations - care delivery organizations and health insurance companies. Because HIPAA was focused on data exchange and portability, It also covered healthcare clearinghouses that process and facilitate the exchange of healthcare data.

HIPAA was originally written before the first Internet bubble. Since that time, both the healthcare market and the technology market have changed considerably. As such, HIPAA has been updated, most notably in 2013 with the HIPAA Omnibus Rule, which expanded coverage to service and technology partners of healthcare organizations.

The 2013 HIPAA Omnibus Rule expanded HIPAA to cover cloud and SaaS providers that have healthcare customers. In a world of APIs, app ecosystems and marketplaces, and data sharing, HIPAA coverage can expand across multiple technologies and organizational layers. The Omnibus Rule was partially designed to account for this.

When you are uncertain about compliance in any of your day-to-day work, do not hesitate to reach out to your manager, human resources, compliance people, or data protection officer (if you have one). It is their job, and a requirement of regulation, for them to help you navigate these waters. You are not alone.

Your responsibility, regardless of the functional area in which you work, if you work for an organization that in some way touches PHI, is to make sure you are always focused on protecting PHI from unauthorized access.