

HIPAA Training Video Transcript: Video Length Approx. 3 minutes

The Health Insurance Portability and Accountability Act (HIPAA), is also called the privacy rule. This deals with making sure organizations, or covered entities, provide security and privacy of all electronic, protected, health information.

HIPPA is a set of security standards that began in 1996 in the US. Prior to that, there weren't any regulations or generally accepted standards to protect individuals' information. Most felt this was acceptable before 1996 most of the healthcare industry was paper-based with no automated processes or electronic information.

In today's environment essentially everything is electronic, including physician orders, health records, and billing requests. All covered entities, or anyone that deals with healthcare information, must maintain the confidentiality, integrity, and availability of the information and abide by the standards and maintain continuous, reasonable, and appropriate security precautions.

HIPPA has several guidelines that include:

- Identify and protect against any anticipated threats to the security or integrity of the data. The organization should implement appropriate security measures to address and reduce overall risks.
- Ensure workforce compliance by providing training for all individuals in the organization.
- Conduct a periodic risk analysis to ensure they are in compliance, and that they are in line with the security policies and processes.
- Access to data should only be the minimum necessary to complete a job or task.
- Provide physical safeguards that include facility access and control along with workstation and device security.
- In order to adhere to all these regulations, each organization must have a dedicated security officer. And there must be appropriate sanctions against anyone who is in violation of the policies and procedures.

HIPPA legislation governs data privacy and security practices that safeguard patient medical information in US medical facilities, along with reporting any breach activity.