

HIPPA

The Security Rule requires healthcare organizations to implement physical, technical, and administrative safeguards to secure patient data.

Some examples of safeguards include:

- 1. Password-protected systems**
- 2. Encryption technology**
- 3. Firewalls**
- 4. Security cameras**
- 5. Restricted access controls**

HIPPA (Health Insurance Portability and Accountability Act)

Series of **National Standard** that health care organizations must have in place - in order to save the privacy and security of HC info or PHI.

Provide the rules for the privacy and security of protected health information (PHI).

Demographic information which is used for identifying patients.

Information

- Name
- SSN
- Images
- DOB
- Phone Number
- Address
- Email
- Medical records number
- Health Insurance
- Acc. Number
- Biometric
- Digital Identifier
- Certificate/Licence

So on

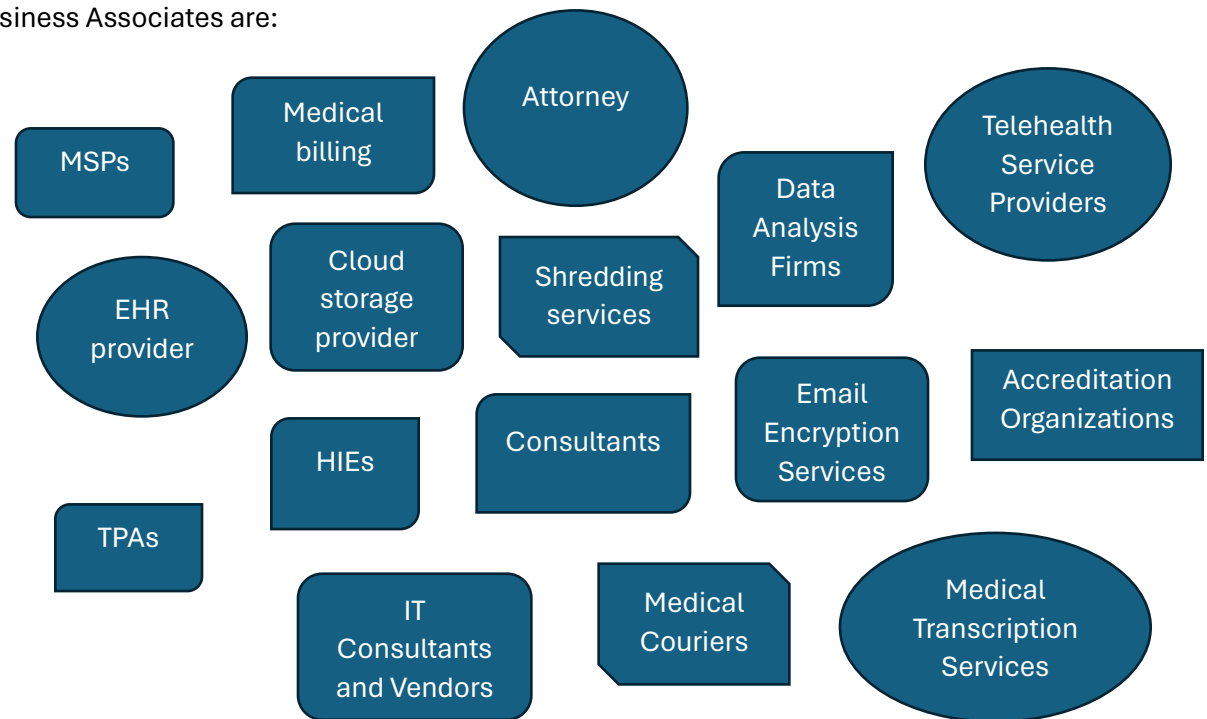
Covered Entities.

- Doc. Offices.
- Hospital
- HC provider
- Health Plan.
- HC clearing houses.

Info about the Health care or payment for healthcare – directly linked to individual.

Another group of PHI is **Business Associate** – like Vendors provide services to Covered Entity.

Business Associates are:



Managed Service Providers (MSPs): These entities manage IT infrastructure and services, including cloud storage and cybersecurity solutions, for healthcare organizations.

Electronic Health Record (EHR) vendors: Companies that provide systems for electronic records of patient health information. They must ensure their systems safeguard PHI.

Medical Billing Companies: Firms that handle coding and billing for healthcare services, dealing directly with PHI in the process.

Health Information Exchanges (HIEs): Organizations that facilitate the sharing of health information among different healthcare institutions.

Pharmacy Benefit Managers (PBMs): Entities that manage prescription drug programs for insurers and employers, interacting with patient medication records.

Attorneys: Legal professionals who work with healthcare entities on matters involving PHI must ensure its confidentiality in their legal practices.

Consultants: Advisors on healthcare practices, compliance, or management who have access to PHI in their consulting roles.

Accreditation Organizations: Bodies that assess healthcare providers for quality and compliance, accessing PHI during audits and evaluations.

Answering Services: Companies that handle call management and messaging services for healthcare providers, possibly dealing with PHI.

Cloud Service Providers: Entities offering cloud computing resources and platforms where PHI might be stored, processed, or transmitted.

Data Analysis Firms: Organizations that perform data aggregation, analysis, or management services involving PHI for healthcare entities.

Document Shredding Companies: Services that securely destroy paper records containing PHI on behalf of healthcare organizations.

Email Encryption Services: Providers of secure email services that protect the confidentiality of PHI communicated electronically.

Medical Transcription Services: Companies that convert voice-recorded reports as dictated by physicians or other healthcare professionals into text format, dealing with PHI.

Third-party Administrators (TPAs): Entities that administer group health plans and handle claims and benefits administration, interacting with PHI.

Healthcare Marketing Services: Firms that conduct marketing on behalf of healthcare providers, which may involve access to PHI for targeting or personalization.

IT Consultants and Vendors: Specialists in information technology who work with healthcare systems, ensuring their operations are secure and compliant with PHI regulations.

Medical Device Manufacturers: Companies that produce devices used in healthcare that may collect, store, or transmit PHI as part of their functionality.

Telehealth Service Providers: Organizations offering remote clinical services, which involve the use of electronic communications and software to facilitate healthcare delivery and may involve handling PHI.

Medical Couriers: Services that transport medical records, specimens, or other items containing PHI, ensuring secure and confidential delivery.

Additional Resources:

A Framework-based Approach to HIPAA Compliance. Retrieved from

<https://hitrustalliance.net/uploads/HITRUST-Approach-to-HIPAA-Compliance-0619.pdf>

Implementing a HIPAA Cybersecurity Framework. Retrieved from:

<https://compliance-group.com/implementing-a-hipaa-cybersecurity-framework/>