HIPAA CHECKLIST

The Health Insurance Portability and Accountability Act of 1996.

- National standards for electronic health care transactions and code sets, unique health identifiers, and security.
- Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

HIPAA PRIVACY RULE[1]

- ☐ **Establishes national standards** to protect individuals' medical records and health information.
- ☐ **Applies to health plans,** health care clearinghouses, and health care providers that conduct certain health care transactions electronically.
- ☐ **Requires appropriate safeguards** to protect the privacy of protected health information.
- ☐ **Sets limits and conditions** on the uses and disclosures that may be made of such information without an individual's authorization.
- ☐ **Gives individuals rights** over their protected health information.

HIPAA SECURITY RULE[2]

- ☐ **Establishes national standards** to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity.
- ☐ **Requires appropriate administrative**, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
- ☐ **Requires covered entities** to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.

Specifically, **covered entities must**:

- ☐ Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain, or transmit.
- ☐ Identify and protect against reasonably anticipated threats to the security or integrity of the information.
- ☐ Protect against reasonably anticipated, impermissible uses or disclosures.
- ☐ Ensure compliance by their workforce.

1. Privacy | HHS.gov
2. The Security Rule | HHS.gov

HIPAA COVERED ENTITIES: WHO MUST COMPLY TO HIPAA?

Health care providers who electronically transmit any health information

Healthcare clearing houses

Health plans

Business associates that act on behalf of a covered entity, including claims processing, data analysis, utilization review, and billing, or provide service to a covered entity, including use or disclosure of covered information.

Researchers are covered entities if they are also health care providers who electronically transmit health information in connection with any transaction for which HHS has adopted a standard.

HIPAA PERMITTED USES AND DISCLOSURES

The law permits, but does not require, a covered entity to use and disclose PHI, without an individual's authorization, for the following purposes or situations:

- Disclosure to the individual (if the information is required for access or accounting of disclosures, the entity MUST disclose to the individual).
- Treatment, payment, and healthcare operations.
- Opportunity to agree or object to the disclosure of PHI.
  - An entity can obtain informal permission by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object.
- Incident to an otherwise permitted use and disclosure.
- Limited dataset for research, public health, or healthcare operations.
- Public interest and benefit activities — The Privacy Rule permits use and disclosure of PHI, without an individual's authorization or permission, for 12 national priority purposes:

  - When required by law
  - Public health activities
  - Victims of abuse or neglect or domestic violence
  - Health oversight activities
  - Judicial and administrative proceedings
  - Law enforcement
  - Functions (such as identification) concerning deceased persons
  - Cadaveric organ, eye, or tissue donation
  - Research, under certain conditions
  - To prevent or lessen a serious threat to health or safety
  - Essential government functions
  - Workers' compensation[3]

3. https://www.cdc.gov/phlp/publications/topic/hipaa.html

HIPAA BUSINESS ASSOCIATE AGREEMENTS

Business Associate Agreements (BAAs) are required for the covered entities to legally enforce the security requirements expected from the business associates acting on their behalf or providing services.

What is a "Business Associate"? A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

Examples of Business Associates:

- A third-party administrator that assists a health plan with claims processing.
- A CPA firm whose accounting services to a health care provider involve access to protected health information.
- An attorney whose legal services to a health plan involve access to protected health information.
- A consultant that performs utilization reviews for a hospital.
- A healthcare clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a healthcare provider and forwards the processed transaction to a payer.
- An independent medical transcriptionist that provides transcription services to a physician.
- A pharmacy benefits manager that manages a health plan's pharmacist network.[4]

HIPAA BREACH NOTIFICATION RULE

The **HIPAA Breach Notification Rule** is mandatory for covered entities and business associates to follow in case of a breach of unsecured protected health information.

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the protected health information or to whom the disclosure was made.
- Whether the protected health information was actually acquired or viewed.
- The extent to which the risk to the protected health information has been mitigated.[5]

4. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html
5. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html