HIPAA Basics

TABLE OF CONTENT

I. TERMINOLOGY

- **Protected Health Information (PHI)**- identifiable health information that can be used to directly or indirectly identify an individual (patient identifier and/or diagnostic/clinical identifier)
  - Examples of patient identifiers include address, social security number, telephone number, birthday, e-mail address, account or medical record number, photographic image, etc.
  - Examples of diagnostic/clinical identifiers include health condition, illness, diagnosis, payment for treatment, etc.
- **Electronic Protected Health Information (ePHI)**- refers to PHI that is stored electronically
- **Covered Entity**- individual, organization, or corporation that directly handles PHI
  - Examples include healthcare providers, insurance companies, pharmacies, clearinghouses
- **Business Associate**- individual or entity who creates, receives, maintains, or stores PHI on behalf of a Covered Entity, not directly involved in handling PHI
  - Examples include answering services, medical transcription, IT groups, shredding services, cleaning services, building maintenance workers
- **Breach**- refers to an impermissible use or disclosure under the Privacy Rule that compromises the privacy or security of PHI
- **Notice of Privacy**- written information related to the patient's privacy, must be given to each patient. Information must include the covered entities' responsibilities and legal obligations as well as the patients' rights as they pertain to their PHI
- **De-identifiable Health Information**- neither identifies nor provides a reasonable basis to identify an individual. Two de-indefinable methods include formal determination by a qualified expert and removal of individual identifiers
- **Risk Security Analysis**- requires entities to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by covered entity or business associate
- **Cyber-attack**- unauthorized use against a computer system and its information

II. BACKGROUND

Health Information Portability and Accountability Act (HIPAA) was enacted in 1996 to regulate Protected Health Information. Historically it has been a benign law with no real consequences for actions, fines were low and rare, audits were almost non-existent, the law was practically non-enforceable.

Everything changed in 2003, 2005, and 2013, where major changes occurred. That's when the Department of Health and Human Services analyzed breaches and concluded that half of breaches occur in healthcare either through cyber-attack, theft, or incidental disclosure of PHI, that's why the federal government needed to address this issue and became more aggressive.

III. WHAT IS HIPAA?

HIPAA is a comprehensive federal law enacted to:

- Protect the privacy of a patient's personal and health information
- Provide for electronic and physical security of personal and health information
- Standardize coding to simplify billing and other transactions

"Privacy" and "Security" are not even in the name of HIPAA, yet they present the biggest challenge under the law.

IV. HIPAA COMPONENTS

- **The Privacy Rule**
  - Came into effect in 2003
  - Establishes national standards to protect individuals' medical records and other personal health information
  - Puts emphasis on "minimum necessary" data sharing
  - Its standards address the use and disclosure of PHI as well as standards for individuals' privacy rights to understand and control how their PHI is used and shared
    - Examples that require patient's authorization for disclosure of PHI include life insurance coverage, pre-employment physical, lab tests, pharmaceutical firms, etc.
    - Patient's authorizations for disclosure of PHI is NOT required for treatment, payment, and health care operations
  - The Privacy Rule does not restrict the use of disclosure of de-identified health information

- **The Security Rule**
  - Became effective in 2005
  - Establishes a national set of standards for protecting electronic PHI
  - Has several types of safeguards and requirements which one must apply:
    - Administrative Safeguards- actions, policies and procedures to prevent, detect, contain, and correct security violations. Involve the selection, development, implementation, and maintenance of security measures to protect ePHI
      - Central requirement is performing a risk security analysis
    - Physical Safeguards- physical measures, policies and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

- Organizations Safeguards-these standards require a CE to have contracts or other arrangements with Bas that will have access to the CE' ePHI
- Policies and Procedures- these standards require a CE to adapt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule
  - CE must maintain written security policies and procedures and written records of required actions, activities, or assessments

- Working with EHR and Health IT developers is key

- **The HITECH Act**

- Expanded privacy and security provisions that are included under HIPAA
- Expanded enforcement and set higher penalties for non-compliance and breaches
- Holds not only healthcare organizations for disclosing breaches, but also their business associates and service providers
  - HHS must be notified of breaches
  - BAs must comply with HIPAA to the same extent as CEs

V. COMPLIANCE

Fundamental to HIPAA compliance:

- Conduct a Security Risk Analysis
  - Although this can be done by office personnel, an independent security specialist (usually IT groups) may be more appropriate, based on the size of the organization
    - Consists of two parts- risk assessment and an IT assessment
    - Output includes a detailed report outlining identified problems to fix
  - The Office of National Coordinator for Heath Information Technology (ONC) has an online tool designed to help physicians navigate the process of conducting a risk assessment
    - https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment

- Implement HIPAA documentation such as policies and procedures
  - Policies are written rules that refer to the HIPAA regulations they support
  - Procedures are detailed steps that should refer to both policies and HIPAA requirements, checklists can be an important part as they document compliance and ensure that procedures are followed
  - Policy and procedures templates can be purchases and altered to organization's needs (IT groups sell them)
  - Disaster documentation must be in place to prioritize what to restore and who's in charge
  - A security file must be kept and maintained for 6 years

- Complete and conduct annual HIPAA trainings
  - HIPAA training must be conducted annually, or upon hiring new employees
  - Such trainings must be documented as part of compliance

VI. TOP 10 HIPAA VIOLATIONS

- Employees disclose PHI
- Medical records are mishandled
- Devices are lost or stolen
- Patient information is texted
- Social Media use with patient information/photos
- Illegal access of patient files by employees
- Breaches
- Unauthorized PHI release
- Accessing patient information on personal computers
- Lack of training

VII. PRIVACY AND SECURITY TRAINING GAMES

www.healthit.gov/topic/privacy-security/privacy-security-training-games

www.healthit.gov/sites/default/files/cybersecure/cybersecure.html

www.healthit.gov/sites/default/files/CyberSecure_103_FINAL/index.html

https://www.hhs.gov/hipaa/for-professionals/training/index.html

VIII. CONCLUSION

Audits are becoming more frequent; be proactive and stay compliant with the law.

- Conduct Risk Analysis
- Create written policies
- Train staff

These three things should keep you out of trouble.

IX. RESOURCES

https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

https://www.hhs.gov/hipaa/for-professionals/faq/index.html

https://www.hhs.gov/hipaa/index.html

https://www.nist.gov/topics/cybersecurity

https://www.healthit.gov/topic/hipaa-providers

http://www.ahima.org/topics/pcs?tabid=education

https://www.ahcancal.org/facility_operations/privacysecurity/Pages/HIPAAPolicyProcManual.aspx

HHS Contact- OCRPrivacy@hhs.gov