Introduction to HIPAA

What is HIPAA and its purpose? Health Insurance Portability and Accountability Act (HIPPA) prevents the disclosure of sensitive health information without a patient's consent. HIPPA gives patients the right to access and request corrections to their health information. HIPPA reduces health care fraud and abuse.

The three main HIPAA rules: Privacy, Security, and Breach Notification

1. PRIVACY

This gives patients more control over their health information, limits and conditions the use and release of health records. This gives patients the right to inspect and obtain copies of their records and request corrections.

(PHI) Protected Health Information, revers to any individually identifiable health information that is created, received, used, or disclosed by a healthcare provider, health plan, or healthcare clearinghouse.

PHI include:

- Name, address, date of birth, ad other demographic information
- Medical history, diagnoses, and treatment information
- Insurance information
- Payment information
- Electronic health records
- Medical device identifiers

2. SECURITY

Protects the confidentiality, integrity, and security of electronic protected health information (ePHI). This requires administrative, physical, and technical safeguards to protect (ePHI), protects ePHI against impermissible use or disclosure.

Administrative safeguards (policies, procedures, workforce training)

- Policies and procedures
    - Proper disposal of PHI
        - Any paper forms, fax, or other PHI we received is scanned into the correct charts, then disposed of using a document shredder service.
    - Results are kept strictly confidential and ONLY REPORTED TO THE ORDERING PROVIDER (Patient's inquiring about results is referred to the ordering provider)
    - Staff members must follow all HIPPA guidelines. The staff will;
        - NOT discuss patient information in public places.
        - NOT discuss patient information with those not caring for the patient.

        - NOT tell anyone that a friend or acquaintance is a patient, without their permission.
        - NOT access patient information unless we need it to do our job
        - NOT take pictures of patients without his/her permission.
        - NOT send text messages about patients on our personal devices.
    - We do not except verbal request over the phone for PHI
        - Any request for PHI have to be in written form with a signed patient information release form.
- Workforce training
    - Gentox employees have annual competencies and other training to stay up to date with new OSAH guidelines. We take all new information and facts into account when it comes to updating our HIPAA and PHI training.
    - Employee training, competencies, etc.. Are kept in the employee files for at least 1 year after employee has left

3. Breach Notification;

A HIPAA breach, is the unauthorized use or disclosure of protected health information (PHI) that compromises its security or privacy.

This requires covered entities to notify the Department of Health and Human services after any data breach. Covered entities include private medical clinics, hospitals, health insurance companies, and their-party health organizations.

In the case of a HIPAA breach, Gentox will;

- Notify affected individuals in writing (notify individuals within 60 days of discovery of breach)
- Notify the media if there are 10 or more affected individuals without contact information
- Notify the HHS (U.S. Department of Health and Human Services) through the Office of Civil rights breach reporting tool (notify the media and HHS within 60 days if the breach affects more than 500 people)

4. Specific Role-Based Scenarios:

- Clinical Staff:
    - Accessing patient records for treatment purposes
    - Sharing information with other healthcare providers
    - Documenting patient care appropriately
- Administrative Staff:
    - Managing patient registration and demographic data
    - Handling patient billing and insurance information
    - Communication with patients regarding appointments and reminders

- IT Staff:
    - Implementing security measures to protect ePHI
    - Monitoring system access and activity
    - responding to security incidents

5. Compliance and Enforcement:

Potential consequences of HIPAA violations

- Criminal penalties- fines and jail time for individuals and organizations who knowingly disclose protected health information (PHI)
- Civil lawsuits – patients can sue entities that breached their PHI if they can prove harm
- Financial penalties – fines for entities that violate HIPAA rules079

If you suspect a PHI violation, by HIPAA law you can file a complaint with the Office of Civil Rights (OCR) within the Department of Health and Human Services (HHS) within 180 days of the incident

HIPPA training an updates.

Gentox does annual training and applies updates to training every year. This is to ensure we maintain compliance with regulations, protect patient privacy by safeguarding sensitive health information, and minimize the risk of data breaches by keeping out employees informed about the latest measures.

Regular refreshers by conducting periodic training sessions to maintain compliance and address any updates to HIPAA regulations.