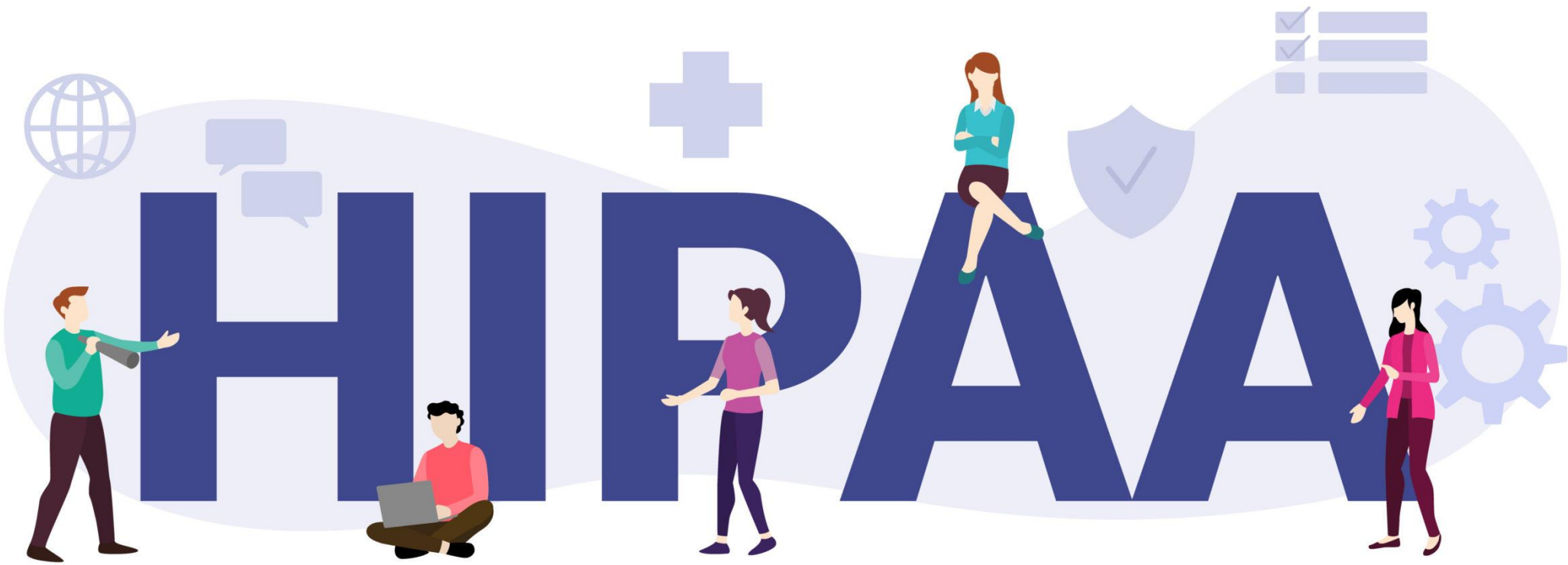


Health Insurance Portability and Accountability Act

PATIENT'S RIGHTS UNDER HIPAA

What is HIPAA?

- Acronym for Health Insurance Portability & Accountability Act of 1996 in the US.
- Provides a framework for protection of patient confidentiality, security of electronic systems, and standards and requirements for electronic transmission of health information.
- It provides data privacy & security provisions for safeguarding medical information
- The law has emerged in recent years with the proliferation of health data breaches caused by cyber attacks & other online attacks on health insurers & providers.

What is HIPAA?

1. **Privacy Rule**
2. **Security Rule**
3. **Electronic Data Exchange**

Privacy Rule

- Refers to protection of an individual's health care data.
- Defines how patient information used & disclosed.
- Gives patients privacy rights & more control over their own health information.
- Outlines ways to safeguard Protected Health Information (PHI).

Security Rule

- Security means controlling:
  - Confidentiality of electronic protected health information (ePHI).
  - Storage of electronic protected health information (ePHI)
  - Access into electronic information

Why Comply With HIPAA?

- To show our commitment to protecting privacy
- As an employee, you are obligated to comply with Your Organization Name privacy & security policies & procedures
- Our patients/members are placing their trust in us to preserve the privacy of their most sensitive & personal information
- Compliance is not an option, it is required.

- If you choose not to follow the rules:
  - You could be put at risk, including personal penalties & sanctions
  - You could put your organization at risk, including financial & reputational harm

HIPAA Regulations & PHI

HIPAA Regulations require we protect our patients' **Protected Health Information (PHI)** in all media including, but not limited to, PHI created, stored, or transmitted in/on the following media:

- Verbal Discussions (i.e. in person or on the phone)
- Written on paper (i.e. chart, progress notes, encounter forms, prescriptions, x-ray orders, referral forms & explanation of benefit (EOBs) forms)
- Computer Applications and Systems (i.e. electronic health record (EHR), Practice Management, Lab and X-Ray
- Computer Hardware/Equipment (i.e. PCs, laptops, pagers, fax machines, servers & cell phones

Why is Privacy & Security Training Important?

- Outlines ways to prevent accidental & intentional misuse of PHI.
- Makes PHI secure with minimal impact to staff & business processes.
- It's about doing the right thing!
- Shows our commitment to managing electronic protected health information (ePHI) with the same care & respect as we expect of our own private information

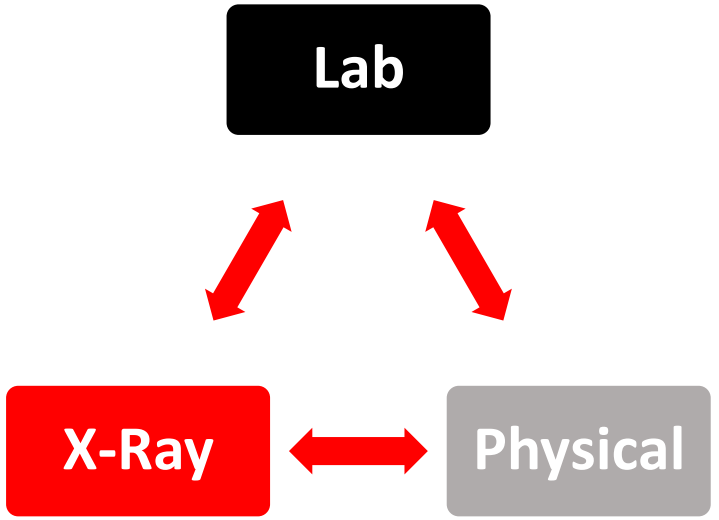
HIPAA Definitions:
What is Protected Health Information (PHI)?

Protected Health Information (PHI) is individually identifiable health information that is:

- Created or received by a HCP, health plan, & employer and that→
  - ✓ Relates to the past, present, or future physical or mental health or condition of an individual;
  - ✓ Relates to the provision of health care to an individual
  - ✓ The past, present or future payment for the provision of health care to an individual.

What Does PHI Include?

- Information in the health record, such as:
  - Encounter/visit documentation
  - Lab results
  - Appointment dates/times
  - Invoices
  - Radiology films & reports
  - History & physicals (H&Ps)
  - Patient Identifiers



What are Patient Identifiers?

PHI includes information by which the identity of a patient can be determined with reasonable accuracy & speed either directly or by reference to other publicly available information.

What Are Some Examples of Patient Identifiers?

- Names
- Medical Record Numbers
- Social Security Numbers
- Account Numbers
- License/Certification numbers
- Vehicle Identifiers/Serial numbers/License plate numbers
- Internet protocol addresses
- Health plan numbers
- Full face photographic images & any comparable images
- Web universal resource locaters (URLs)
- Any dates related to any individual (date of birth)
- Telephone numbers
- Fax numbers
- Email addresses
- Biometric identifiers including finger & voice prints
- Any other unique identifying number, characteristic or code

What Are Uses & Disclosures?

- **Uses:** When we review or use PHI internally (i.e. audits, training, customer service, or quality improvement).

- **Disclosures:** When we release or provide PHI to someone (i.e. attorney, patient or faxing records to another provider).

What is Minimum Necessary?

- To use or disclose/release only the minimum necessary to accomplish intended purposes of the use, disclosure, or request.

- Requests from employees at [Organization]:

✓ Identify each workforce member who needs to access PHI.

✓ Limit the PHI provided on a "need-to-know" basis.

- Requests from individuals not employed at [Organization]:

✓ Limit the PHI provided to what is needed to accomplish the purpose for which the request was made.

What is Treatment, Payment &Health Care Operations (TPO)?

- HIPAA allows Use and/or Disclosure of PHI for purpose of:
  - Treatment – providing care to patients.
  - Payment – the provision of benefits and premium payment.
  - Health Care Operations – normal business activities (i.e. reporting, quality improvement, training, auditing, customer service and resolution of grievances data collection and eligibility checks and accreditation).

Why Do We Need to Protect PHI?

- It's the law.
- To protect our reputation.
- To build trust between providers & patients.

- If patients feel their PHI will be kept confidential, they will be more likely to share information needed for care.

What Are the Patient's Rights Under HIPAA?

HIPAA Regulations

- The Right to Individual Privacy
- The Right to Expect Health Care Providers Will Protect These Rights

- Other Patient Rights Include:

✓Access,
✓Communications,
✓Special Requests,
✓ Amendment,
✓Accounting of Disclosures,
✓Notice of Privacy Practices and Reminders,
✓and the Right to File Complaints.

Patient Rights: Access & Inspect PHI

- Patient's have the right to inspect & copy their PHI.

- There are some situations where access may be denied or delayed:
  - Psychotherapy notes.
  - PHI compiled for civil, criminal or administrative action or proceedings.
  - If access would endanger a person's life or safety based upon professional judgment.
  - If a pt's request may jeopardize health & safety of the pt, other pts or others at the institution.
  - If a research study has previously secured agreement from the individual to deny access.
  - If PHI was obtained under promise of confidentiality & access would reveal the source of the PHI.

Patient Rights: Request Alternate Communication

- Patient has the right to request to receive communication by alternative means or location.

- For example:
  - The patient may request a bill be sent directly to him instead of to his insurance company.
  - The patient may request we contact her on cell phone instead of home telephone number.

To summarize.... HIPAA

HIPAA - Health Insurance Portability and Accountability Act

The HIPAA Privacy Rule:

- established standards to protect all forms of health information created by health care providers, health care institutions & other "covered entities."
- gives patients certain controls over their health information.

The HIPAA Security Rule:

- established standards to protect electronic health information (ePHI).
- outlines security procedures to ensure the confidentiality, integrity and availability of ePHI.

To summarize.... HIPAA: Patients Rights

Patients have the right to:

- be informed of their rights & how their PHI will be used or disclosed.
- have access to or obtain copies of their health information. Under HIPAA, facilitating patient access to their PHI is just as important as protecting the privacy of that information.
- request corrections of information in their records.
- restrict certain disclosures of their information.
- receive an accounting of certain disclosures of their health information.
- be notified if the privacy or security of their information has been compromised.

END