THE HIPAA PRIVACY RULE

What is HIPAA?

- **H**ealth
- **I**nsurance
- **P**ortability and
- **A**ccountability
- **A**ct

(Passed into law in 1996)

Four Parts of HIPAA

1. Standardized Electronic Data Interchange **transactions** and codes for all covered entities
2. Standards for **security** of data systems
3. **Privacy** protections for individual health information
4. Standard national **identifiers** for health care

The Privacy Rule…

- establishes a Federal floor of safeguards to protect the confidentiality of medical information
- allows patients to make informed choices when seeking care and reimbursement for care based on how personal health information may be used
- took effect on April 14, 2003

What Does The Privacy Rule Protect?

Individually Identifiable Health Information, commonly referred to as "Protected Health Information" or "PHI"

PHI is information transmitted in any form, oral, written, or electronic that is:

1) Created or received by a covered entity; and

2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) There is a reasonable basis to believe the information can be used to identify the individual

Examples of PHI

- Name, address, telephone, fax, email and other contact information
- Social security number
- Health plan beneficiary number
- Medical diagnoses
- Medical records and account numbers
- Certificate and license numbers
- Photographs and images

Who Must Comply with HIPAA?

1) Health Plans
2) Health Care Clearinghouses
3) Health Care Providers who conduct certain financial and administrative transactions electronically

These entities are commonly known as Covered Entities (CE).

What must a covered entity do to be in compliance with HIPAA?

A. Notify patients about their privacy rights and how their information can be used
B. Adopt and implement privacy procedures
C. Train employees so they understand the privacy procedures
D. Designate a Privacy Officer
E. Secure patient records containing PHI

Vocabulary of HIPAA

- **Protected Health Information (PHI)** is individually identifiable health information that contains unique features or details by which the individual can be identified.
- **Treatment, Payment and Health Care Operations (TPO)** are common uses of PHI for which HIPAA does not require an authorization.

Vocabulary of HIPAA

- **Disclosure** means the release, transfer, provision of access to, or divulging of information outside the entity holding the information.
- **Use** means the sharing, employment, application, utilization, examination, or analysis of individually identifiable information within an entity

Notice of Privacy Practices

- Plain language
- Specified uniform header
- Description & at least one example of each type of use and disclosure made for TPO
- Description of each permitted or required use or disclosure without authorization
- Sufficient detail of each use and disclosure to put individual on notice
- Statement that all other uses or disclosures will only be made with the individual's authorization
- Delineation of individual's privacy rights

New Patient's Rights

- Right to written Notice of Privacy Practices (NPP) that informs consumers how PHI will be used and to whom it is disclosed
- Right of timely access to see and copy records for reasonable fee
- Right to request amendment of record
- Right to restrict access and use
- Right to an accounting of disclosures
- Right to revoke authorization

Requests for Amendment

- **A patient may request, in writing, to have health information or a record about the patient amended.**
- **The CE does not have to agree to the amendment, however, the request to amend becomes a part of the patient's medical record.**

Requests for Restrictions

- **Patients may request, in writing, a restriction or limitation on the health information that a CE uses or discloses.**
- **The CE is not required to agree to the restriction.**

Accounting of Disclosures

- **Patients are entitled to request a list of people and organizations who have received their PHI.**
- **Patients must submit a written Request for Accounting of Disclosures.**
- **A CE must respond to a patient's request for an accounting within 60 days of receipt of the request.**

The accounting of disclosures should include disclosures…

- Required by law
- For public health activities
- About victims of abuse, neglect or domestic violence
- For health oversight activities
- For judicial and administrative proceedings
- For law enforcement purposes
- For research purposes
  (if authorization was waived)
- For specialized government functions
- For workers' compensation

AUTHORIZATION…

- Is a detailed document that gives covered entities permission to use PHI for specified purposes.
- Is required for the use and disclosure of PHI not otherwise allowed by the Privacy Rule
- Does not apply to TPO
- Does not apply to uses and disclosures required by law
- May be revoked at any time in writing

Authorization Requirements

An authorization must describe:

- the PHI to be used and disclosed;
- the person authorized to make the use or disclosure;
- the person to whom the covered entity may make the disclosure;
- an expiration date; and
- the purpose for which the information may be used or disclosed.

Minimum Necessary Standard

HIPAA requires covered entities to take reasonable steps to disclose only the information that is necessary for the purpose for which the disclosure is to be made (i.e. the minimum necessary amount of information).

Minimum Necessary Does Not Apply To:

- Treatment
- Disclosures to the individual who is the subject of the PHI
- Uses or disclosures made pursuant to an individual's authorization
- Uses or disclosures that are required by law

Do I need to know?

Ask yourself:

- Do I need this information to do my job and provide good patient care?
- What is the least amount of information I need to do my job?

Incidental Disclosure

A secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and occurs as a by-product of an otherwise permitted use or disclosure.

EXAMPLE

Miguel shares a semi-private room with Victor. Dr. Nixon, Miguel's doctor, comes in to talk to Miguel. Dr. Nixon draws the curtain between the two patients. During this bedside consult, Victor overhears Dr. Nixon say that Miguel needs a hernia operation.

Protecting Patient Privacy "Do's"

Do:

- **Close curtains and speak softly when discussing treatments in semi-private rooms**
- **Log off of the computer when you are finished**
- **Dispose of patient information by shredding or storing in locked containers for destruction**
- **Clear patient information off of your desk when you leave your desk**

Protecting Patient Privacy "Don'ts"

Don't:

- **Tell anyone what you overhear about a patient**
- **Discuss a patient in public areas such as elevators, hallways, or cafeterias**
- **Look at information about a patient unless you need it to do your job**

Rules for Using Computers

- **Keep your password a secret**
- **Do not log in using someone else's password**
- **Log off of the computer when you are finished using it**
- **Turn the computer screen away from public view**
- **Do not remove equipment, disks, or software without permission**

Rules for Using Faxes

Sending:

- Call the intended recipient before sending the fax
- Double-check the fax number before sending
- Use cover sheets for faxes

Receiving:

- Tell the person faxing information to alert you when he/she is about to send the fax
- Take faxes off of the machine immediately
- Do not let faxed patient information lie around unattended

Business Associate

A person or entity that performs a function or activity on behalf of a CE that requires the creation, use or disclosure of PHI but who is not considered part of the CE's workforce.

Business Associates

- Must be helping the covered entity carry out its health care functions
- Must have a written contract or agreement with the covered entity that assures that they will appropriately safeguard any PHI they receive or create

HIPAA's Impact on Research Activities

- **NO ONE is permitted to use PHI for research without complying with the new HIPAA requirements**
- **These HIPAA requirements are entirely separate from the existing federal human subject research regulations.**

Please Note:

The Privacy Policies and Procedures do not replace or override other rules or procedures established by the Institutional Review Board ("IRB"). Both must be complied with in order to conduct human subject research.

State Law vs. HIPAA

If there is a conflict or inconsistency between an applicable state law and the HIPAA Privacy Rule, follow the law that provides the patient:

- Greater privacy rights,
- Greater access to information, or
- Greater privacy protections.

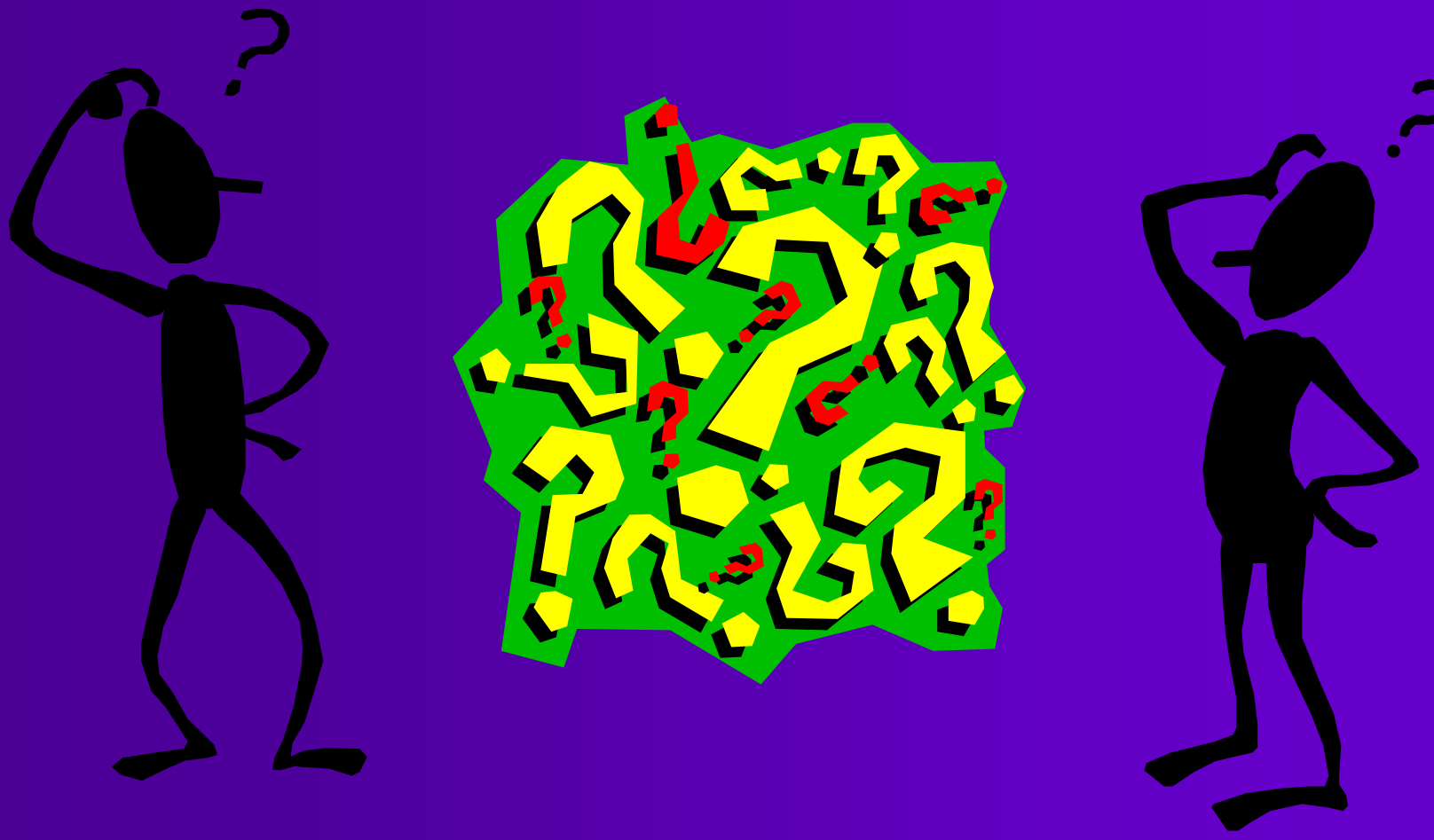
Penalties for Privacy Violations

- **Civil Penalties under HIPAA:** Maximum fine of $25,000 per violation
- **Criminal Penalties under HIPAA:** Maximum of 10 years in jail and/or a $250,000 fine for serious offenses
- **Organization Actions:** Employee disciplinary actions including suspension or termination for violations of UNM's policies and procedures

The Privacy Rule Requirement

- **You may not retaliate against or intimidate an employee who files a HIPAA complaint.**

TEST YOUR KNOWLEDGE!



CASE STUDY

Lori, a nurse who works on 5-West, has a lot of access to PHI. Terri, a nurse who works on 4-North, learns that her friend and elderly neighbor, Ms. Pate, was admitted to 5-West. Terri is concerned and wants to help so she asks Lori to see Ms. Pate's medical record. Together, they review and discuss their findings.

CASE STUDY

In deep conversation, Drs. Andrews and Day enter a crowded elevator and continue discussing a code yellow. Their conversation is quite detailed and graphic, but never mentions the patient's name. Engaged in their conversation, they do not notice the onlookers intently listening to their conversation.