HIPAA Training: Ensuring Privacy for our Patients

Privacy Training for Harvard Medical Students

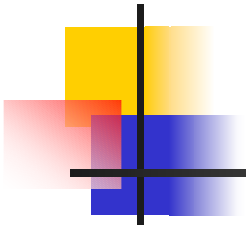
Goals

By the end of this program you will be able to

- Explain the basic principles of the Privacy Rule
- Understand who has to follow the Rule.
- Describe the basic policies/procedures an entity uses to protect patient information.
- Describe patients' rights under the Rule.
- Identify your role in protecting patient information.
- How to get help if you have a question.

Agenda for this program:

- What is privacy?
- What is HIPAA/The Privacy Law?
- Why is it important?
- Who must follow the law?
- What are an entity's responsibilities?
- What does this mean for you?

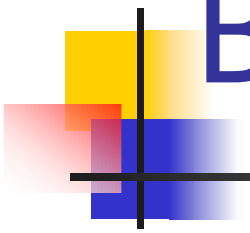


Privacy – what is it?

- Our right to keep information about ourselves from others if we choose.

We expect…

…that Healthcare providers and workers will protect the privacy of the information they learn about us.



But…

Sometimes our privacy is violated, even by those we most trust to protect it!

For example

The Situation:

- Country singer Tammy Wynette's medical records were sold to the National Enquirer and Star tabloids by a hospital employee for $2,610.

The Result:

- The public's trust in the hospital was damaged, and a valued patient's reputation was compromised.

What is HIPAA/ The Privacy Law?

- HIPAA—Health Insurance Portability and Accountability Act of 1996, Standards for Privacy of Individually Identifiable Health Information (45 CFR Parts 160 and 164)

The Privacy Law

- Protects patients privacy
- Supports our value of respecting patients' interests.
- Restores the public's faith in each of us as healthcare professionals, and in our institutions.

The Privacy Law

- Protects all health information created by a healthcare provider, health plan, or healthcare clearinghouse
- Defines who is allowed to see or use a patient's private health information

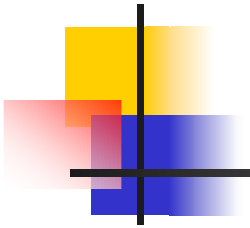
The Privacy Law

- Protects the information whether it is:

Oral 

Written 

Electronic 



Why is Patient Privacy important?

Why Is It Important?

- Safeguards protected identifiable patient health information
- Provides patients with more control over what happens with their information

Continues

Why is it Important?, *continued*

- Provides patients with informed choices about how their information is used
- Balances our need to use information to treat patients, teach, and conduct research with the patient's desire/need for privacy

What Does the Law Include?

- Protected Health Information (PHI)

Protected Health Information

- Any information created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse.
- 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 past, present, or future payment for the provision of health care to an individual.

Protected Health Information Includes, But is Not Limited to:

- Medical Records
- Billing information (bills, receipts, EOBs, etc.)
- Labels on IV bags
- Telephone notes (in certain situations)
- Test results
- Patient menus
- Patient information on a palm device
- X-rays
- Clinic lists

Who Must Follow the Law?

- Healthcare Providers (and their Workforce)
  - Anyone who provides services, care, or supplies that relate to the health of a person (such as a hospital, doctor, dentist, or others)
- Health Plans (such as Insurers, HMOs, etc.)
- Healthcare Clearinghouses

This means that workforce members of all the hospitals affiliated with Harvard Medical School must follow the law. This includes all students rotating at these institutions!

Am I Part of the Workforce?

- You are considered a part of the Workforce if you are a
  - Physician
  - Employee
  - Volunteer
  - Temporary Employee
  - Contractor
  - Consultant
  - Medical Student rotating at the institution

What Are the Responsibilities of the Institution?

- Provide patients with a notice of privacy practices.
- Protect the information from use or disclosure to those not allowed to see it by law or by the patient.
- Investigate complaints of breaches of confidentiality.
- Discipline breaches of confidentiality.

The Notice of Privacy Practices

- Describes the ways an institution may use a person's health information.
- Describes the rights the person has to protect their information.
- Describes the duties we have to the patient to protect their information.
- Informs the patient about the complaint and investigation process.
- Must be given to a patient before the first treatment encounter and written acknowledgment obtained.

What are the Patient's Rights?

- To have their information protected
- To be provided with a notice of our privacy practices
- To have their questions answered
- To see their information if they wish (restrictions apply)
- To obtain copies of their records (for a fee)
- To request to change their records
- To limit (under specific circumstances) the use/disclosure of their information

What Does This Mean for You?

- Be careful with information to which you have access. Ask yourself:
  - *Am I allowed to have this information? Is it required for me to do my job?*
  - *Is the person with whom I am about to share this information allowed to receive it? Do they need the information to do their job?*
  - *If I were the patient, and this were my information, how would I feel about it being shared?*

What Must I Do to Ensure Patient Privacy?

- Be aware of who is around you when you are discussing patient information
- Dispose of information appropriately
- Use cover sheets for faxing
- Share information only with those who are allowed to have it
- When in doubt, ask for help

You Should be Aware of Patient Privacy in

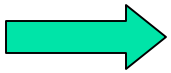
- Ensuring computer security
- Sending/receiving faxes
- Disposing of information
- Using/disclosing information
- Conducting everyday-work practices

Each of these aspects of Patient Privacy are discussed in detail in the next few slides.

Ensuring Computer Security

- Never share passwords.
- Lock workstation/log off when leaving a workstation.
- Position workstation so screen does not face a public area if possible.
- Be careful when sending email containing patient-identifiable information. Avoid it if possible.
- Refer to your institution's e-mail guidelines.

Continues



Sending/Receiving Faxes

- Fax is the least controllable type of communication
- When faxing information:
  - Use a cover sheet!!
  - Verify you have the correct fax number, and
  - The receiving fax machine is in a secure location, and/or the receiver is available immediately to receive the fax

Continues

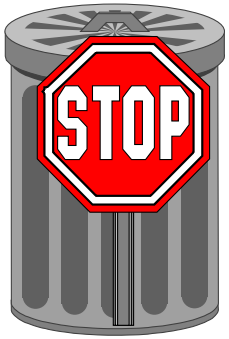
Sending/Receiving Faxes

continued

- When receiving faxed patient information
  - Immediately remove the fax transmission from the fax machine, and deliver it to the recipient.
  - If information has been sent in error, immediately inform the sender, and destroy the faxed information (deposit in shredding bin, or other method).

Disposing of Information

- Do not place identifiable health information in regular trash!
- Rip, shred, or otherwise dispose of identifiable health information
- Check on local institutional policy/procedure on the correct method for disposal of protected health information.



Using and Disclosing Information

- The next few slides describe ways of using and disclosing information, including
  - TPH/TPO
  - Authorizations
  - Incidental Use or Disclosure
  - Authentication

Continues

Using and Disclosing Information

- You may use/disclose patient information without specific authorization from the patient for
  - Treating a patient (**T**reatment)
  - Getting paid for treating a patient (**P**ayment)
  - Other healthcare operations (**O**perations)

Collectively known at TPO or TPH

Continues

About Authorizations

- What is an Authorization?
  - Permission from the patient to release information
  - Must be obtained where Protected Health Information is used for other than TPH (except psychotherapy)
  - Is time limited
  - May be revoked by the patient
- What is Needed for an Authorization?
  - State to whom information will go
  - State for what purpose the information will be used
  - State what information will be sent

There are Times when Information May be Disclosed Without Authorization

- If Required by Law
  - Court Order
  - Subpoena
- Public-Health Reporting
- Incidental Disclosures
  - Overhearing a patient's conversation with their doctor or nurse in a semi-private room

These are discussed in more detail on the following slides

Disclosures Required by Law

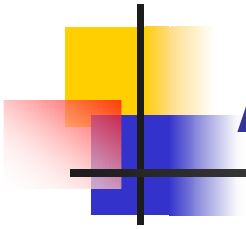
- If the release complies with and is limited to what the law requires, you may give information to (see "Authentication" below)
  - Public health authorities
  - Health oversight agencies
  - Employers responsible for workplace surveillance
    - Must post notice of privacy practices
  - Coroners, Medical Examiners, and Funeral Directors
  - Organ procurement organizations

About Incidental Use or Disclosure

Hallmarks

- Occurs as by-product of an otherwise permitted use or disclosure
- Cannot be reasonably prevented
- Is limited in nature
- Is permissible to the extent that reasonable safeguards exist

Example: being overheard by patient's roommate while discussion health problem with a patient in a semiprivate room.



Authentication

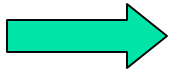
To the degree practicable you must ensure that the person to whom you give the information is the person allowed to receive it.

In other words, be certain to ask for identification!

Minimum Necessary

The Privacy Law generally requires that we all take reasonable steps to limit the use or disclosure of, and requests for Protected Health Information (PHI) to the minimum amount of information necessary to accomplish the intended purpose.

The next slide provides details on instances where "minimum necessary" does not apply.



Minimum Necessary

Does not apply to

- Disclosures to a health care provider for treatment purposes or made at the direction of an authorization by the patient.
- Disclosures to the patient themselves.
- Uses/disclosures required for compliance with standardized HIPAA transactions.
- Disclosures to DHHS required under the rule for enforcement.
- Uses/disclosures required by other law.

Accounting for Disclosures

- Upon request, covered entities *must* provide patients with a list of those to whom they have disclosed the patient's information *except* for
  - Instances when the information is disclosed to the individuals themselves.
  - When it was used/disclosed for TPO, or
  - Under a specific authorization

How to Account for Disclosures

Unless limited by the request, the accounting must cover the full six years prior to the request, but not earlier than April 14, 2003, and must include

- To whom information was disclosed
- When it was disclosed
- What was disclosed
- Why it was disclosed

Conducting Your Everyday-Work Practices

- Think about how and when you disclose patient identifiable data.
- Look for opportunities to reduce unnecessary uses and/or disclosures.
  - What data do you create?
  - What data do you send to others outside where you are working? For what purpose?
  - What data do you receive from others? For what purpose?

Important Guidelines for

- Communicating information.
- Recording and keeping information.
- Transporting and disposing information.

Guidelines for Communicating

- Watch where you talk about patients.
  - The cafeteria is not appropriate
- Be careful with whom you speak
  - Are they allowed to receive the information? Why?
  - Talking at a party about a patient you have seen just because it is interesting should not be done.
- Remember e-mail is not always safe.
- The Medical School is not an extension of the hospital or office.
  - Think twice before sharing information about patients.

Guidelines for Recording and Keeping Information

- You may keep records and lists containing protected information for education purposes.
- You are responsible for protecting the information.
  - Password protect PDA's and files
  - Encrypt when possible

Guidelines for Transporting and Disposing of information

- When carrying or transporting PHI protect it from being seen by others.
- Use a container if appropriate.
- Turn record and files face down

Guidelines for Transporting and Disposing of information

- Dispose of information correctly
  - Rip, shred, or otherwise destroy those 3x5 cards or notes about patients.
- Do not leave records and x-rays lying around conference rooms, lounges, etc.!
- If you find PHI lying around return it or destroy it.

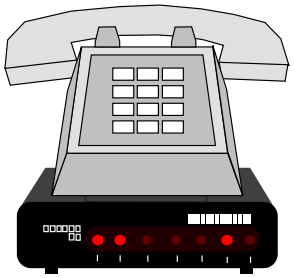
Who is Responsible?

- We are all responsible!
  - Anyone who cares for patients, works in the hospital environment, or is responsible for using identifiable information in order to perform their jobs
  - Anyone who works for providers that perform functions on our behalf that involve patient identifiable information

What Else Can You Do?

- Your responsibility for protecting patient privacy and confidentiality does not end with your work shift
  - Don’t divulge any patient information when in an informal atmosphere or social setting
  - If asked about a patient, simply reply “I’m sorry, that information is confidential”
  - Respect everyone as if they were your family member!

How to Get Help or Report a Privacy Concern or Breach



Contact

- Your course director
- The institutional privacy officer
- Consult the appropriate institutional policy.

Thank you

- You have completed the general training about the Privacy Rule
- More training may be provided by the course site, if they feel it is needed.
- Thank you for your support in our efforts to protect the private information of patients

Remember….

Be careful with information to which you have access.

Ask yourself

- *Am I allowed to have this information? Is it required for me to do my job?*
- *Is the person with whom I am about to share this information allowed to receive it? Do they need the information to do their job?*
- *If I were the patient, and this were my information, how would I feel about it being shared?*