Objectives

By the end of this lesson, you should be able to:

- Define protected health information (PHI) covered under HIPAA regulations
- Recall patients’ rights regarding PHI information maintenance, sharing and disclosure.
- Examine how UTHealth uses patient information in providing care to our patients and communicating with health care providers and others.
- Recognize employees’ responsibilities in upholding these rights and protecting our patients’ PHI confidentiality and privacy.
Health Insurance Portability & Accountability Act (HIPAA) was designed to improve efficiency and effectiveness of health care systems by standardizing the electronic exchange of administrative and financial data.
The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009, promote the adoption and meaningful use of health information technology.
What is HIPAA?

The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information.

At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.
Six Patient Rights

Introduction

Notice of Privacy Practices

- All patients are given a Notice of Privacy Practices upon their first visit to UTHealth or UT Physicians. This comprehensive document details the policies and procedures of UTHealth, and explains patient rights.

- The notice of Privacy Practices was updated in September 2013. It is available at: https://inside.uthouston.edu/hipaa/notice-of-privacy-practices.htm

Rights to Request Restrictions on Use or Disclosure
Six Patient Rights

Rights to Request Restrictions on Use or Disclosure

- Generally, the type of information that falls under this category is directory type information, which is basic patient information, such as the patient’s name, location in the facility, and general condition of the patient.
- Patients have the right to request further restriction on the use or disclosure of their PHI.
- The University must honor such requests if the patient has made other payment arrangements.
- The University will, in good faith, attempt to honor such requests.

- The patient may also restrict disclosure of religious affiliation to clergy. Or, the patient may not want family and/or friends involved in his or her care to be given PHI about him or her.
- Restricting these disclosures may cause operational difficulties; therefore, the institution may deny a request for a restriction. **However, if the patient requests that the institution not disclose information to a health plan, the institution MUST comply with such a request, if the patient pays in full for the service.** This policy may be accessed at [https://inside.uthouston.edu/hipaa/policy.htm?id=1484237](https://inside.uthouston.edu/hipaa/policy.htm?id=1484237).
Six Patient Rights

Right to Access PHI on Self

- The patient also has a right to access his or her protected health information. The patient specifically has the right to inspect and receive a copy of his or her PHI. A patient may review his or her PHI.
- The patient has the right to access his/her health information and receive of copy of it at his/her expense.
- The patient must review the information where staff can observe him/her at all times.
- UTHealth may deny access under certain circumstances, and the patient may request of review of the denial.
- **NEW:** If an individual’s request for access directs UTHealth to transmit the copy of PHI directly to another person designated by the individual, UTHealth must provide the copy to the person designated by the individual. The request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the PHI.
- This policy may be accessed at [https://inside.uthouston.edu/hipaa/policy.htm?id=1484243](https://inside.uthouston.edu/hipaa/policy.htm?id=1484243).

Right to an Accounting of Use / Disclosure About Self

Right to Revise Authorization
Six Patient Rights

Right to an Accounting of Use / Disclosure About Self

Patients have the right to an accounting of all disclosures that the UTHealth has made of his or her protected health information. This means that all departments and/or clinics must have a method of tracking disclosures made on each patient, starting with disclosures made six years ago. If the patient requests, the institution must provide a list of all disclosures made for the previous six years, except:

- Disclosures that are made to the patient;
- Disclosures that are made for treatment, payment, or health care operations;
- Disclosures that are made based on an authorization signed by the patient;
- Disclosures that are made to correctional facilities for inmates;
- Or, for disclosures made for national security or intelligence purposes.
- Disclosures that are required to be included on the list of disclosures include:
  - Child or elder abuse reporting;
  - Communicable disease reporting;
  - To the FDA regarding product recalls;
  - To trauma or tumor registries; in response to court orders;
  - To law enforcement regarding crime victims;
Six Patient Rights

- Disclosures that are required to be included on the list of disclosures include:
- Child or elder abuse reporting;
- Communicable disease reporting;
- To the FDA regarding product recalls;
- To trauma or tumor registries; in response to court orders;
- To law enforcement regarding crime victims;
  To coroners, medical examiners, or funeral directors.

These are examples of the types of disclosures that should be included on the accounting of disclosures and is not intended to be an exhaustive list. Although, particularly in this setting, there will probably not be very many disclosures that are required to be tracked; there may be operational challenges in tracking them. This policy may be accessed at https://inside.uthouston.edu/hipaa/policy.htm?id=1484252

Right to Revoke Authorization

Right to Request Correction or Amendment of PHI
Six Patient Rights

Right to Access PHI on Self

Right to an Accounting of Use / Disclosure About Self

Right to Revoke Authorization
- The patient may revoke an authorization that he or she has previously signed allowing use or disclosure of protected health information.
- After the authorization is revoked, in writing, we must ensure that no one releases the PHI. This could apply for general uses and disclosures, such as to a patient’s attorney, or for research purposes.
- The revocation cannot be applied to uses and disclosures that the institution may have already made in reliance on the patient’s authorization prior to the revocation.

This policy may be accessed: [https://inside.uthouston.edu/hipaa/policy.htm?id=1484213](https://inside.uthouston.edu/hipaa/policy.htm?id=1484213)

Right to Request Correction or Amendment of PHI
Six Patient Rights

Right to Request Correction or Amendment of PHI

A patient has the right to request an amendment or correction to protected health information. If the patient believes that there is erroneous or incomplete information in his or her health record, he or she has the right to request a correction or amendment in writing.

- UTHealth may deny the request if the PHI was not created by the institution; if it is not part of the designated record set; if it is not available for inspection by the patient; or if it is complete and accurate as it is.
- The “designated record set” is comprised of subsets of health records and may be maintained in various locations or files.
- If UTHealth denies the patient’s request for amendment, the denial must be in writing and communicated to the patient. The patient has the right to disagree with a denial, which also must be in writing. Whether UTHealth accepts or denies a patient’s request to amend his or her record, the documentation regarding the request is included in the official health record.
- UTHealth does not remove or obliterate the original documentation in the patient’s record. Amendments are documented on designated forms.

This policy may be accessed at: https://inside.uthouston.edu/hipaa/policy.htm?id=1484247

AMEND
Use and Disclosure of PHI

Protected Health Information (PHI) may only be used and disclosed under certain circumstances, following specific guidelines:

1. Treatment, Payment or Healthcare Operations
   
2. Some Public Policy exceptions, including the waiver of authorization granted by the Institutional Review Board (IRB) for research purposes
   
3. Authorization of the patient
Use – Sharing PHI Within UTHealth

**Point 1**
PHI may be used to treat patients, obtain payment for services, educate UTHealth students and residents, and conduct normal health care business.

**Point 2**
UTHealth may share information inside the institution *only* while following the privacy law and the privacy policies of the institution.

**Point 3**
That means we must ensure that the person to whom we give information is part of treatment, payment or healthcare operations or has an authorization signed by the patient.

**Point 4**
If the person is a researcher, even a UT researcher, they must present either an authorization signed by the patient or a waiver of authorization prepared by the IRB.
### Disclosure – Sharing Outside of UTHealth

<table>
<thead>
<tr>
<th><strong>“Disclosure” means:</strong></th>
<th><strong>Any entity:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>To release or transfer PHI outside of UTHealth, which includes giving access to or divulging information in any way.</td>
<td>That provides services to UTHealth to whom we disclose information under contract must also sign a “business associate agreement” which details the parameters under which they must use and disclose the PHI that they receive.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Before giving information:</strong></th>
<th><strong>In any setting:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>To others outside UTHealth, double check to ensure that the information is going to the right place and the person who says he has a right to the information, in fact, does so.</td>
<td>Where health care services are provided, a certain amount of incidental disclosure of PHI is unavoidable. Health care providers are required, under HIPAA, to take precautions to ensure that reasonable safeguards to protect incidental disclosures are in place.</td>
</tr>
</tbody>
</table>
Disclosure Continued

If reasonable safeguards are in place, the following activities are permitted:

- Using patient sign-in logs
- Calling out the patient’s name in the waiting room
- Disclosing PHI in group or family therapy sessions
- Disclosing PHI to family members or other person involved in the patient’s care
- Discussing a patient’s treatment among care providers, and posting patient schedules in treatment areas
Authorization

Disclosing Patient Information

• There are occasions when we must disclose the patients’ information for purposes other than treatment, payment, or operations.
• The patient must sign a specific authorization to give UTHealth the authority to disclose information for such purposes.

The Authorization Form:

• Must contain nine specific elements, and forms that outline these elements are available in the records departments.
• Please ask for assistance from the Privacy Office if you need to develop or fill out an authorization form.

Valid Authorization Form:

• If you are not sure if an authorization form is valid, check with the Privacy Office before making a use or disclosure pursuant to the form.
Introduction

Click the tabs on the left to learn more about Treatment Payment Operations.

After clicking each topic, wait for the arrow to blink and turn blue before clicking to proceed.
Treatment

Treatment includes provision, coordination, and management of patient care. Consultation and referrals for healthcare providers is permitted. Examples:

- A nurse calls in a referral to another physician's office and provides information to ensure proper care for a patient.
Treatment

- A nurse calls in a referral to another physician's office and provides information to ensure proper care for a patient.
- The lab tests ordered by the treating physician are returned to her for analysis.
- The treating physician shares the information from the lab with another physician to ensure that the patient receives quality care.
Payment

Payment includes activities to obtain or provide reimbursement for health care activities. Examples include:

- Administrative Assistant sends bill to patient's insurance company.
- Information is sent to the insurance company making the request, for documentation purposes.
Operations

Operations includes activities done to improve services, including education. Examples include:

- The nurse is giving information to the Legal department in order to manage risk information.
- A medical student is brought into a patient room to learn care procedures.
Authorization Exceptions

Sometimes it is okay to use or disclose PHI outside of TPO. Only the **minimum necessary** should be shared. These very specific cases are:

<table>
<thead>
<tr>
<th>For public health activities such as disease reporting</th>
<th>Where permitted by an IRB waiver, for research</th>
</tr>
</thead>
<tbody>
<tr>
<td>About victims of abuse, neglect or domestic violence</td>
<td>To avert a serious, imminent threat to public safety</td>
</tr>
<tr>
<td>For health oversight activities, like the FDA or a licensure board</td>
<td>Certain government functions</td>
</tr>
<tr>
<td>For judicial or administrative proceedings</td>
<td>Anything else required by law</td>
</tr>
<tr>
<td>For some law enforcement activities</td>
<td>Consult the UTHealth Privacy Handbook and/or the Privacy Officer for guidance</td>
</tr>
</tbody>
</table>
Introduction

Click each topic to learn more about Accidental Release or Breach.

After clicking each topic, wait for the arrow to blink and turn blue before clicking to proceed.

Definition

Electronic Examples of Breach

PROPERTIES
Allow user to leave interaction: After viewing all the steps
Show 'Next Slide' Button: Don't show
Completion Button Label: Next Slide
Accidental Release or Breach

Introduction

Definition

- A breach is the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI and is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment.

- The Privacy Officer and Chief Information Security Officer are responsible for conducting the risk assessment.

Electronic Examples of Breach
Accidental Release or Breach

Electronic Examples of Breach

- Workforce members access the electronic health records of a celebrity who is treated within the facility, and they are not involved in the patient’s care.
- Stolen/lost laptop containing unsecured protected health information.
- Lost flash drive containing database of patients participating in a clinical study.
- Workforce members accessing electronic health records for information on friends or family members out of curiosity/without a business-related purpose.
- Misdirected fax of patient records to a local grocery store instead of the requesting provider’s fax.

Mobile Device Examples of Breach
Accidental Release or Breach

- Medical student takes a cell phone picture of patient following a MVA and transmits photo to friends.
- PDA with patient-identifying wound photos lost.
Accidental Release or Breach

- Posting of patient’s HIV+ health status on Facebook by a laboratory tech who carried out the diagnostic study.
- Misdirected e-mail of listing of drug seeking patients to an external group list.
Accidental Release or Breach

**Introduction**

**Definition**

**Electronic Examples of Breach**

**Mobile Device Examples of Breach**

**Social Media Examples of Breach**

**Other Examples of Breach**

- Papers containing protected health information found scattered along roadside after improper storage in truck by business associate responsible for disposal (shredding).
- EOB (Explanation of Benefits) sent to wrong guarantor.
- Provider accessing the health record of divorced spouse for information to be used in a custody hearing.
- Misfiled patient information in another patient’s medical records which is brought to the organization’s attention by the patient.
- Medical record copies in response to a payers request lost in mailing process and never received.
- Misdirected fax of patient records to a local grocery store instead of the requesting provider’s fax.
- Briefcase containing patient medical record documents stolen from car in gym parking lot.
- Intentional and non-work related access by staff member of neighbor’s information.
- Medical record documents left in public access cafeteria.
Protocol

• If you discover that Protected Health Information is accidentally released, **you need to act immediately** to minimize risk and damage.

• Accidental release can be anything from calling the wrong patient to distributing a spreadsheet, to losing a portable device.

• You must report as soon as you discover the potential breach, as there is a limited time frame to respond.

  • **Inform your supervisor in writing.**
  
  • Notify the Office of Legal Affairs, UCT 1477 at (713) 500-3258.

  • If IT resources are involved send an e-mail to its@uth.tmc.edu or call (713) 486-4848.

• Breaches of the HIPAA Privacy and Security Rules have serious ramifications for all involved. In addition to sanctions imposed by UTH, such breaches may result in civil and criminal penalties.
In 2010, a former UCLA Health System employee became the first person in the United States to receive jail time in a federal prison for a misdemeanor HIPAA offense. The employee used his employee access to the University’s electronic medical records system to view the medical records of his supervisors, co-workers, and high-profile patients. While none of the information was “used” or sold, the access was nonetheless illegal because the employee lacked a valid reason for looking at the records.
**PHI and E-mail**

**All emails**

All emails containing PHI, including those sent to other University email addresses, must be digitally signed and encrypted.

If the recipient does not have a digital ID, you must find an alternate way to send the information.

**Digital IDs**

Remove PHI from unencrypted emails that you receive, before you reply or forward the email. Double check all email addresses when you send PHI. DO NOT RELY upon auto-complete to find the e-mail addresses for you.

**Digital IDs**

Remember that people using PDAs and Smart phones, or people moving from computer to computer, will not have the ability to install a Digital ID on their device and cannot read encrypted emails. This DOES NOT mean that you should send unencrypted emails with PHI.

**Disposal of PHI**

When disposing of documents that contain PHI follow the records retention schedule, archive records according to University policy and procedure, and shred all documents containing PHI.
Contact Information

- If you have questions about information contained in this module, please contact:

Christina Solis, JD
UTC 1447
(713) 500-3305
Christina.F.Solis@uth.tmc.edu