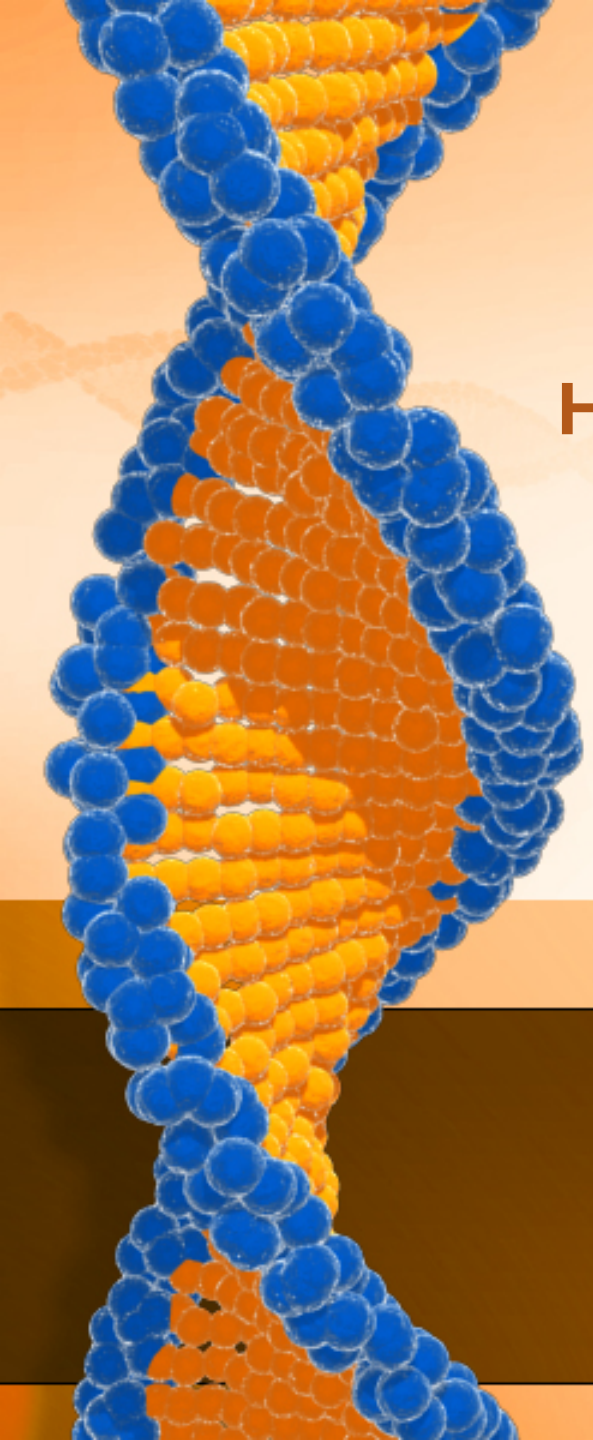


Health Insurance Portability and Accountability Act (HIPAA) Compliance Training

UTHealth
The University of Texas
Health Science Center at Houston

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 communication with health care providers and others.
- Recognize employees' responsibilities in upholding these rights and protecting our patients' PHI confidentially and privacy.

HIPAA

The 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.

HITECH

The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009, promotes the adoption and meaningful use of health information technology.

What is HIPAA?

The HIPAA Privacy Rule provides federal protections for protected 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 protected health information needed for patient care and other important purposes.

Six Patient Rights: HIPAA

1. Notice of Privacy Practices
2. Right to Request Restrictions on Use or Disclosure
3. Right to Access PHI on Self
4. Right to an Accounting of Use/Disclosure about Self
5. Right to Revoke Authorization
6. Right to Request Correction or Amendment of PHI

1 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.

It is available at: https://inside.uth.edu/hipaa/notice-of-privacy-practices.htm

2 Right to Request Restrictions on Use or Disclosure

A patient may ask that the university restrict the use or disclosure of his or her PHI beyond what is protected in by the Privacy Rule.

- 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.

2 Right to Request Restrictions on Use or Disclosure

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.uth.edu/hipaa/policy.htm?id=1484237

3 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 a review of the denial.

3 Right to Access PHI on Self

- If a patient asks for a copy of his or her records, under most circumstances, members of the UTHealth workforce should direct the patient to medical records to process the request.
- **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.uth.edu/hipaa/policy.htm?id=1484243.

4 Right to an Accounting of Use/Disclosure About Self

Patients have the right to an accounting of all disclosures that 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
- Disclosures made for national security or intelligence purposes.

4 Right to an Accounting of Use/Disclosure About Self

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.

This policy may be accessed at: https://inside.uth.edu/hipaa/policy.htm?id=1484252

5 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 at: https://inside.uth.edu/hipaa/policy.htm?id=1484213

6 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 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.

6 Right to Request Correction or Amendment of PHI

- 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.uth.edu/hipaa/policy.htm?id=1484247

Use and Disclosure of PHI

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

1. Authorization of the patient
2. Treatment, payment or operations
3. Some public policy exceptions, including the waiver of authorization granted by the Institutional Review Board (IRB) for research purposes

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 laws 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 health care operations or has an authorization signed by the patient.

Point 4

If the person is a researcher, even a UTHealth researcher, they must present either an authorization signed by the patient or a waiver of authorization prepared by the IRB.

Use – Sharing PHI Within UTHealth

Patent Privacy Monitoring

In order to ensure that systems are properly used, UTHealth has implemented FairWarning, a patient privacy monitoring software that alerts administrators that a record may have been improperly accessed.

An alert may be sent if workforce members access their own records, the records of their family members, neighbors or co-workers.

All alerts are investigated to ensure that false positives are dismissed and workforce members are given the opportunity to explain why a record was accessed.

Disclosure – Sharing Outside of UTHealth

"Disclosure" means:

To release or transfer PHI outside of UTHealth, which includes giving access to or divulging information in any way.

Any entity:

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 they receive.

Before giving information:

To others outside UTHealth, double check to ensure that the information is going to the right place and the person who says he or she has a right to the information, in fact, does so.

In any setting:

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.

Disclosure – Sharing Outside of UTHealth

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 people involved in the patient's care
- Discussing a patient's treatment among care providers and posting patient schedules in treatment areas

Use and Disclosure of PHI (Review)

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

1. Authorization of the patient
2. Treatment, payment or operations
3. Some public policy exceptions, including the waiver of authorization granted by the Institutional Review Board (IRB) for research purposes

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.
- 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.

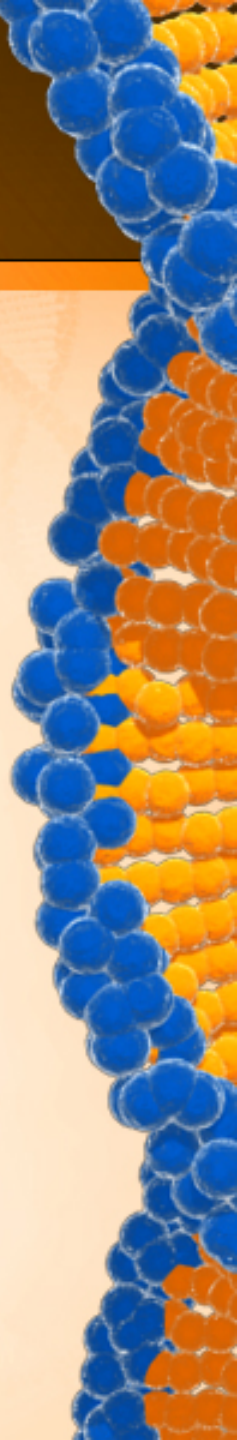
Authorization

Media

- All disclosures to the media MUST be coordinated through the Media Relations Team in the Office of Public Affairs, which will provide both an authorization for the disclosure of PHI and a separate consent for the media appearance. See HOOP Policy.

Fundraising:

- Most disclosures for fundraising and development purposes must also be accompanied with an authorization. Limited information may be disclosed to the Office of Development. See the HIPAA Policy for more information.



Treatment

"Treatment" includes the provision, coordination, and management of a patient's care. It includes consultations and referrals to other health care providers. We are permitted to exchange PHI between health care providers for treatment purposes.

Examples

- **The lab tests ordered by the treating physician are returned to her for analysis.** The physician who orders the test and the laboratory that returns the tests to the physician do not have to obtain separate authorization from the patient in order to exchange information.
- **The treating physician shares the information from the lab with another physician to ensure that her patient receives quality care.** Consulting with other providers within the treatment context is considered "treatment" under the privacy rule.

Treatment

Examples

- **A nurse calls in a referral to another physician's office and provides information to ensure proper care for a patient.** Often, permitted disclosures occur over the phone. This is a treatment disclosure and permitted under the Privacy Rule. However, safeguards must be maintained. Be certain that you are talking to the right office and be sure that you are talking about the right patient. Make sure to avoid sending any information by fax or mail without double checking to see that ONLY the information that you intend to send is in the packet. Sometimes piles of paper will accidently contain information about other patients.

Payment

Examples

Payment activities include, but are not limited to:

- Determinations of eligibility or coverage,
- Billing, claims management, collection activities, and related health care data processing,
- Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges,
- Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services,
- Disclosure to consumer reporting agencies

Payment

Examples

- **Clerk sends bill to patient's insurance company.** The information contained in bills can be quite voluminous. Ensure that the proper bills are going to the proper health plans.
- **The physician submits charge sheets to the office staff.** Be aware that charge sheets are often left on desks in plain sight. Be sure to leave them in a secure place until they can be processed and placed in their proper storage.
- **Information is sent to the insurance company making the request for documentation purposes.** Sometimes, insurance companies will ask for further documentation. When sending information, ensure that only the information that is necessary for filing the claim is sent to the insurance company.

Operations

HIPAA bundles a large number of functions into the term "health care operations.” These are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment.
The disclosure of PHI for health care operations must be limited to the minimum necessary information to get the job done.

Operations

Examples

A medical student is brought into a patient room to learn care procedures. We can use PHI to educate students and residents involved in the patient's care. "Using PHI for education" also means we can use PHI within the institution for classroom lectures and case presentations. The patient's PHI, including photographs or other images that identify the patient, must not be used in any other way without the patient's authorization.

For external conferences, manuscripts, and the like, if we use PHI, we must obtain the patient's specific authorization to do this. Residents and students are not permitted to take any PHI with them when they leave their affiliations unless the patient has specifically authorized them in writing to do so.

Operations

Examples

The nurse is giving information to the legal department in order to manage risk information. The offices of legal affairs, institutional compliance, finance, and internal audit may ask for protected health information for health care operations purposes.

The offices of development and public affairs will need an authorization from the patient before protected health information can be shared for most fundraising purposes or for media relations purposes.

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:

- For public health activities such as disease reporting
- About victims of abuse, neglect or domestic violence
- For health oversight activities, like the FDA or a licensure board
- For judicial or administrative proceedings: All subpoenas must be forwarded to the Office of Legal Affairs.
- For some law enforcement activities
- Where permitted by an IRB waiver, for research
- To avert a serious, imminent threat to public safety
- Certain government functions
- Anything else required by law

Consult the UTHealth Privacy Handbook and/or the Privacy Officer for guidance

Accidental Release or Breach

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 demonstrates 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 the risk assessment.

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 patient 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

Accidental Release or Breach

Mobile Device Examples of Breach:

- Medical student takes a cell phone picture of patient following a MVA and transmits photo to friends
- PDA with patient-identifying wound photos is lost

Social Media Examples of Breach

- Posting of patient's HIV+ health status on social media by a laboratory tech who carried out the diagnostic study
- Misdirected email of listing of drug seeking patients to an external group list

Accidental Release or Breach

Other Examples of Breach:

- Papers containing PHI found scattered along roadside after improper storage by business associate responsible for disposal (shredding)
- EOB sent to wrong guarantor
- Providing accessing the health record of divorced spouse for information to be used in custody hearing
- Misfiled patient information in another patient's record which is brought to our attention by the patient
- Medical record copies in response to a payor's request lost in the mail and never received
- 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, or 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 and mitigate.
- **Inform your supervisor in writing**.
- Notify the Office of Legal Affairs, UCT 1477, at **713-500-3268.**
- If IT resources are involved, email 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 UTHealth, **such breaches may result in civil and criminal penalties.**

In the News…

Published February 2014 Compliance Training

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 illegal because the employee lacked a valid reason for looking at the records.

PHI and Email

All emails

All emails containing PHI, including those sent to other UTHealth email addresses, must be 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 email addresses for you.

Digital IDs

If your recipient does not have a digital ID, this DOES NOT mean that you should send unencrypted emails with PHI. Either find another way to encrypt the information or do not send PHI.

Disposal of PHI

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

Contact Information

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

Senior Legal Officer and Privacy Officer
Christina Solis, J.D., M.P.H.
713-500-3305
Christina.F.Solis@uth.tmc.edu