HIPAA

Developed by
The University of Texas at Dallas
Callier Center for Communication Disorders
Purpose of this training

Everyone with access to Protected Health Information (PHI) must comply with HIPAA (the Health Insurance Portability and Accountability Act).

The UT Dallas HIPAA Privacy Officer has assigned you this training because you are a student or employee working in one of the areas of UT Dallas that must be aware of this law.

- The Callier Center for Communication Disorders
- Office of Advancement
- Office of Budget and Finance
- Office of Environmental Health and Safety
- Office of Information Technology
- Office of Information Security
- Office of Institutional Equity and Compliance
- Office of Internal Audit
- Office of Procurement Management
- Office of Strategic Planning and Analysis
- Office of the University Attorney

This training gives an overview of selected aspects of HIPAA and outlines your responsibilities.
Part 1: The law

What is HIPAA?

HIPAA is a federal law designed to protect health information. It applies to the Callier Center clinic and to any UT Dallas faculty and staff—regardless of location—who use or might have access to Callier Center patient data.

Key Definition

Protected Health Information (PHI):

- The term used in HIPAA that refers to oral, written and electronic information HIPAA protects. PHI is any information about or an identifier of a patient, past, present or future, that can be used to recognize a patient.

- PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act (FERPA) and in employment records held by an employer.
Examples of Protection Required by HIPAA

HIPAA requires guarding Protected Health Information (PHI) in many ways. This training will cover information outlined in privacy-oriented sections of HIPAA. Additionally, employees must protect PHI by following UT Dallas information security policies, which further ensure the security of PHI.

Examples of information security policies that protect PHI:

- Encrypting all desktops and laptops which access PHI
- Keeping computers and software fully patched and running anti-malware software
- Not using hosted, or cloud based, services for storing PHI unless it is specifically approved by the Office of Information Security
- Encrypting email containing PHI
- Never disclosing your UTD NetID password or letting another individual access UTD information resources through your account
Protected health information (PHI) can take many forms.

- On paper
- Spoken or recorded
- Electronic
Different types of health information are PHI.

**PHI can be:**

- About a person who is alive or deceased
- Past, present, or future information about an individual’s health, the treatment of their health condition, or the billing/payment for their health services
- Any unique number or characteristic that could be linked to an individual

**For example:**

- Names (including names of relatives)
- Photographs or images
- Phone numbers
- Physical or Email Addresses
- A person’s health condition, treatment or diagnosis
- Device identifiers such as hearing aids or cochlear implant serial numbers
No matter its form, you must protect PHI.

HIPAA always requires you to protect PHI.
For example, you can protect PHI by:

Never using patients’ names or personal details when talking in or other public spaces

Never taking PHI outside of the clinic or campus office

Always using secure recycling or cross cut shredders
Securely storing all paper files and removable electronic media

Encrypting electronic files and emails

Using screen filters so no one can read the information on your computer screen
Email Encryption

The Information Security Office (ISO) has advised that email encryption is not required for most types of confidential information, including UTD-IDs.

However, due to HIPAA privacy and security requirements, the Callier Center has mandated encryption for all email containing Protected Health Information (PHI).

- Within UTD, this can be accomplished by using digital certificates to sign and encrypt email
- With outside parties, this can be accomplished by adding the tag [encrypt] to the subject line
Access PHI only on a need-to-know basis

HIPAA requires that you only access or disclose PHI as part of job-related duties. If you access or disclose PHI without a patient’s written authorization or for any reason other than treatment, payment, or health operations purposes, you are violating HIPAA; a federal offense.

It makes no difference if the information relates to a high-profile person or a close friend or family member. These rules apply to all employees, including health care professionals.

**Remember:** Just because you have access to PHI does not mean it is legal for you to look at or disclose the information to anyone not involved in the patient’s case management.
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 access to the university’s electronic medical records system to view the medical records of his supervisors, co-workers, and high-profile patients.

While he did not sell or use the information for any personal gain, the access was nonetheless illegal because he lacked a valid reason for looking at the records.

He was sentenced to four months in federal prison and fined $2,000.
Protecting PHI is your responsibility, even when not at work.

It is easy to forget about work rules when you are done with your work day, but HIPAA rules apply to you no matter where you are or what time of day it is.

- Do not discuss patient information casually with your friends or acquaintances in any setting.
- Do not talk about patients on personal social media (Facebook, Twitter, etc.). Anything posted by the Callier Center on social media sites is authorized for release to the public.

For example: People violate HIPAA when disclosing confidential information in conversations at restaurants or out with friends. It is not enough to avoid using a person’s name. *Any identifiable information about an individual is PHI.*
A doctor at Westerly Hospital in Rhode Island was fired for posting information on Facebook about a patient she treated.

Although the posting did not reveal the patient’s name, there was enough information that others could easily identify the person who had problems with alcohol and marijuana abuse.

In addition to losing her job, the doctor was also reprimanded by the state medical board and fined $500.
You must report breaches of PHI privacy/security.

A breach is a HIPAA violation that occurs when PHI is:

- Lost, stolen, or improperly destroyed. For example, the paper or device upon which PHI is recorded cannot be accounted for.
- Hacked into by people or computer programs that are not authorized to have access. For example, the system in which PHI is stored is compromised by a computer virus.
- Improperly communicated or sent to others who have no official need to receive it. For example, PHI is shared through gossip or text messaging.

**HIPAA requires you to report violations or breaches immediately to:**

- Your supervisor or any other Callier Center administrator
- The UT Dallas HIPAA Privacy Officer: Donise Pearson, 972-883-3601 HIPAAPrivacyOfficer@utdallas.edu
- The UT Dallas HIPAA Security Officer: Nate Howe, 972-883-6855 infosecurity@utdallas.edu
- UT Dallas HIPAA Privacy Breach Notification Policy
Retaliation is strictly prohibited.

Employees, volunteers, students, or contractors of the Callier Center may not threaten or take any retaliatory action against an individual for reporting or filing a HIPAA report or complaint, including notification of a privacy or security violation or breach.

UT Dallas Reporting Suspected Violations and Protection for Retaliation
HIPAA violations carry serious penalties.

In addition to losing your job, the federal government might order you to pay fines or serve a prison sentence or both, depending on the circumstances. Up to $250,000 in fines and 10 years in prison.

HIPAA violations can also result in criminal and civil penalties for the Callier Center. $50,000 per incident, up to $1.5 million per calendar year.

Although penalties are far more serious for those who intentionally break the law, HIPAA penalties apply to unintentional violations, too.
Part 2: Five HIPAA Program Components

The following pages provide a brief overview of the five HIPAA program components followed by the Callier Center:

- Individual patient rights
- “Minimum necessary” information standard
- Procedures for data use in research
- Limits for marketing and fundraising uses
- Business associates
Component 1: Patient rights

The first component sets forth the following individual rights for patients:

- To receive a copy of the Callier Center’s Notice of Privacy Practices
- To request restrictions and confidential communications of their PHI
- To inspect and obtain a copy of their healthcare records
- To request corrections of their healthcare records
- To obtain an accounting of disclosures (a list showing when and with whom their information has been shared)
- To file a complaint with a healthcare provider or insurer and the federal government, if the patient believes his or her rights were denied or that PHI was not protected.
Component 2: Minimum necessary

HIPAA states that, when the use or disclosure of PHI is permitted, only the minimum necessary information may be used or disclosed.

This is intended to protect the patient; it does not restrict the ability of healthcare providers to share information needed to treat patients, process payments, or to report public health concerns.

For any other disclosures:

Patients must always sign an authorization form before their PHI may be released by the Callier Center to outside parties such as a school, a life insurer, a bank, or a marketing firm.
HIPAA regulates how PHI may be obtained and used for research. This is true whether the PHI is completely identifiable or partially “de-identified” in a limited data set.

A researcher or healthcare provider is not entitled to use PHI in research without the appropriate HIPAA documentation, including an authorization or an Institutional Review Board approval.

**For example:**
If a researcher gets a signed Informed Consent Form from a research subject, but does not also get a signed HIPAA Authorization form/waiver, the researcher may not use collected data for research, presentations, or publications.
Component 4: Marketing and fundraising

Without a written authorization, the university may not use information about the medical treatment of an individual for targeted fundraising or marketing.

The Notice of Privacy Practices and other general fundraising and marketing communications advises patients of the right to opt out of being contacted for fundraising and marketing purposes.
Component 5: Business associates

An outside company or individual doing business with the Callier Center is considered a HIPAA Business Associate when providing services involving PHI maintained by the Center.

HIPAA requires that business associates:
• Enter into a Business Associate Agreement (referred to as a BAA) with the Callier Center
• Use appropriate safeguards to prevent the use or disclosure of PHI other than as permitted by a contract with the Callier Center
• Notify the Callier Center of any individual instances of a breach for which the business associate was responsible where PHI has been improperly accessed, used, or disclosed
• Ensure that their employees and subcontractors receive HIPAA training
• Protect PHI to the same degree as the Callier Center.
Robert works as a facilities maintenance employee. One afternoon, he is fixing a light fixture in a provider’s office and he notices a document with patient information in the trash.

What, if anything, should Robert do?
Answer to example Case #1

These patient records contain PHI and should not be discarded in an unsecured manner. Robert should tell the provider or his supervisor, so that the records are either shredded or properly secured.

Robert’s supervisor is responsible for informing the Callier Center administration of this violation.
Example Case #2

Jessica is an audiologist at the Callier Center. One evening, she enters another provider’s office to get some hearing aid supplies. On the desk, she sees a daily schedule with patient names.

What, if anything, should she do?
Answer to example Case #2

This list is PHI. Jessica should remove the list from the desk and store it in a secure place.

The next day, she should tell the other provider that she found the list. Jessica should remind the other provider to always put away papers and files and lock them up at the end of every day.
Knock, Knock
Who's there?
HIPAA
HIPAA who?

Sorry, I can't tell you that.....
For more information

This training is available at the UT Dallas [Office of Institutional Equity and Compliance website.](#)

If you have questions or need to report a violation

Contact a UT Dallas HIPAA Officers:

- HIPAA Privacy Officer
  Donise Pearson 972-883-3601

- HIPAA Security Officer
  Nate Howe 972-883-6855

Laws and policies

- UT Dallas [HIPAA Privacy Manual](#)
- UT Dallas [Information Security Policies and Standards](#)
- HIPAA ([Health Insurance Portability and Accountability Act of 1996 Rules 45 C.F.R. Parts 160 and 164](#))