HIPAA Business Associate Awareness Training

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

• Everyone with access to others’ health and medical information must comply with HIPAA (the Health Insurance Portability and Accountability Act).

• All UT Dallas departments under the Memorandum of Understanding with the Callier Center are assigned HIPAA awareness training.

• This training provides an overview of selected aspects of HIPAA and outlines responsibilities related to the law.
HIPAA at UT Dallas

• The Callier Center for Communication Disorders is a HIPAA covered entity as it provides and bills health care services.
• A Callier Center Business Associate is any section of UT Dallas that works directly or indirectly with the Callier Center.
• UT Dallas is considered a “hybrid entity” as some operations are for health care services and some operations are not. UT Dallas is responsible for implementing an entity wide compliance program for the Callier Center and its business associates.
Knock, Knock
Who's there?
HIPAA
HIPAA who?

Sorry, I can't tell you that.....
What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is a law that was passed in 1996 and has been amended several times with many outcomes:

- Provided patients privacy
- Provided patient access to their own records
- Provided increased security of information
- Provided increase portability of insurance information and use
Health Information Technology for Economic and Clinical Health Act

The HITECH Act was passed in 2009 and amended HIPAA, which:

• Incorporated a breach notification requirement
• Incorporated more stringent penalties
• Provided the Office of Civil Rights funding and authority to ensure HIPAA compliance through investigation, audits, and penalties
Privacy vs. Security

- Privacy – Individual right to have confidentiality of services and records
- Security – Control, maintain, and protect access to information

You can have security without privacy, but you cannot have privacy without security.
HIPAA Individual Rights

A patient, health insurance plan member, or personal representative has the right to:

• Receive a Notice of Privacy Practices
• Access their records
• Receive an accounting of who has accessed their protected health information
• Ask to amend their records
• Ask for restrictions on Disclosures and Use
• Receive confidential communications
• File a complaint
• Receive a breach notification
**HIPAA Covered Entity and Business Associate Responsibilities**

- Provide a Notice of Privacy Practices
- Have a Privacy Officer
- Provide access to an individual’s own records
- Grant certain requests
- Maintain HIPAA privacy (and security) policies
- Provide HIPAA training on the policies
- Provide documentation of Disclosures, if required

- Provide accounting of certain Uses/Disclosures
- Receive complaints/investigate violations
- Sanction violators
- Protect security of protected health information
- Mitigate harm caused by lack of compliance
- Provide breach notifications
- Maintain compliance records

*Applies to covered entity only (not business associates)*
The Privacy Officer (PO)

- Privacy is “patient” centered.
- The PO is responsible for establishing HIPAA compliance for all offices subject to HIPAA at UT Dallas.
- Information Security, Information Technology, Audit and Compliance, and other offices work with the PO. However, the PO has ultimate authority on most issues related to HIPAA.
- The PO investigates and ensures sanctions for all HIPAA privacy violations.
- Offices that make operational changes must consult the PO to determine the impact on the Callier Center.
Protected Health Information (PHI)

Information transmitted or maintained in any form or medium including electronic, written, or oral, that:

- Is created or received by a health care provider, health plan, employer, or health care clearing house
- Relates to past, present, or future physical or mental health condition(s) of an individual or the past, present, or future payment(s) for the provision of health care to an individual
- Either identifies the individual or provides a reasonable basis to believe the information can be used to identify the individual.
No Really – What is PHI?

- “Health Information” is pretty much anything that comes out of a patient’s mouth about his or her own health when he or she is talking to a doctor, nurse, or other health care provider.
- PHI also includes information that comes from a patient’s medical record that contains identifiable information about the person as the recipient or payment of medical treatment.
- PHI is all health information that is protected under HIPAA and maintained by a HIPAA covered entity or business associate.
What is not Protected Health Information?

• De-identified information is not PHI.
• However, even information stripped of an identifier can still identify an individual and constitute PHI. Previous information about a claim that gives sex, age, and a diagnosis would be enough to allow a colleague to identify the individual.
Identifiers that Constitute PHI

- Names
- Postal address
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints (DNA)
- Identifiable photographic images (e.g., face, tattoo, birthmark)
Exceptions to PHI Definition (not PHI)

Information Maintained as Employee Records is not PHI.

- Timekeeping and leave time
- Family Medical Leave Act (FMLA) and sick leave records
- Americans with Disabilities Act (ADA) information
- Family Education Rights and Privacy Act (FERPA) and student treatment records from student health centers are not PHI.
HIPAA Privacy Rules Apply to both the Use and Disclosure of PHI

• Use - any access to protected health information (PHI) for internal purposes. PHI internally should only be accessed by a workforce member to perform a duty the member is authorized to do as part of his/her job.

• Disclosure - any sharing or providing PHI to any individual or entity outside of the internal workforce.

• If PHI is used for any reason other than to perform a specific duty a workforce member is authorized to do, then a HIPAA violation has occurred. This includes reading your own PHI or those of your dependents.
Who must comply with HIPAA?

• Covered entities
• Plan sponsors (employers who purchase health insurance for employees)
• Business associates (BAs) of covered entities who perform business functions for a covered entity that require access to PHI. BAs may be third parties such as vendors or governmental entities (e.g., Office of General Council).
What’s a Covered Entity?

- Health care providers (physicians, hospitals, etc.) that send or store PHI electronically
- Health plans and HMOs
- Clearinghouse (third-party billers)
- The Callier Center is a covered entity, because it is a health care provider that bills insurance carriers electronically.
What’s a Hybrid Entity?

- A hybrid entity houses a covered entity within the services they provide (e.g., UT Dallas primarily educates students, but includes the speech-language-hearing healthcare services of Callier Center).

- The offices that are subject to HIPAA are collectively called the “Health Care Component.” This component includes the covered entity and all in-house business associates even if they do not provide health care.

- UT Dallas is a hybrid entity
  - The university has the Health Care Component (offices using/maintaining PHI) and non-healthcare departments.
  - Only the Health Care Component must comply with HIPAA, but the entire institution is responsible for compliance and subject to penalties and fines for HIPAA violations.
Business Associates

• Anyone who, on behalf of a Covered Entity
  • Performs a function involving the Use or Disclosure of PHI or another function regulated by HIPAA; or
  • Provides services such as legal, actuarial, or administrative services involving Use or Disclosure of PHI from a Covered Entity or another Business Associate of the Covered Entity.

• Business associates are directly responsible for complying with HIPAA. They can be subject to investigations, audits, and penalties by the Secretary of Health and Human Services.
Business Associates

- Penalties for a covered entity or business associate that willfully neglects to have HIPAA privacy policies or comply with them can be fined up to $1,500,000 a year.

- The relationship between a covered entity and a business associate (outside of a health care component) or a business associate and subcontractor that access the BA’s PHI, must be formalized by a written Business Associate Agreement (BAA) or, in the case of a governmental entity, a Memorandum of Understanding (MoU).

- Also BAs must be designated as part of the Health Care Component; the whole office, not just the people that access the PHI.
UT Dallas Business Associates within the Health Care Component

- University Attorney – provides legal counsel and representation
- Information Security – accesses electronic records that contain PHI
- Procurement Management - processes invoices for reimbursements
- Information Resources – provides technical support
- Budget and Finance – reconciles accounts and performs other business functions
- Internal Audit – audits and provides assurances of services
- Institutional Compliance – facilitates high-risk monitoring
- Environmental Health and Safety - destroys records containing PHI
- Advancement – conducts fundraising activities
- Strategic Planning and Analysis – supports data maintenance, planning, and institutional research/evaluation
Notice of Privacy Practices (NOPP)

• Roadmap to UT Dallas’ HIPAA Policies
• Provided to all patients at the Callier Center and posted at each location
• Must be revised and a new copy provided each time it is amended
• UT Dallas offices that provide business associate services to the Callier Center follow the NOPP. Business associates do not send out a separate notice.
The Basic Rule

Protected health information (PHI) cannot be released to anyone outside of the covered entity unless:

• The covered entity has a signed authorization.
  OR

• An exception in the privacy rules permits the release without an authorization from the patient.

• One exception is that PHI can be released to a covered entity’s BA in accordance with the terms of the Business Associate Agreement or Memorandum of Understanding without an authorization.
Exceptions for Release without Authorization

- To law enforcement officials
- To health oversight agencies/public health
- To government agencies authorized by law to receive reports
  - For abuse or neglect
  - For health conditions and epidemics that threaten public health
- To military authorities
- To prevent imminent threats
- For judicial or administrative proceedings
- When required by law not pre-empted by HIPAA – Note Texas Attorney General says The Public Information Act release is ‘required by law’
Exceptions for Release without Authorization Continued

• To business associates of the covered entity
• To another covered entity
• To Personal Representatives
• To coroners/medical examiners/funeral directors
• For inspections by the Secretary of Health and Human Services
• For workers’ compensation
• For Use or Disclosures for treatment, payment, or operations (TPO)
Biggest Exception to Authorization Requirement: TPO

- **Treatment** – records needed to provide health care. The provider may access the entire designated record.

- **Payment** – records needed to collect or pay for health care. The provider may access the entire designated record.

- **Health Care Operations** – everything else a covered entity does as part of its business activities that requires Use or Disclosure of PHI.
Minimum Necessary Rule

Access within the covered entity to PHI must be limited to information an employee needs to perform his or her job duties

- Exceptions may be made for payment & treatment
- Applies to any Use by or Disclosure of PHI to or by a Business Associate

Failure to comply with the minimum necessary rule (unless inadvertent access) is a violation and a breach.
Business Associates

- BAs are limited to using and disclosing PHI only as set forth in the Business Associate Agreement or Memorandum of Understanding.
- Any Use or Disclosure not part of their routine duties under the MOU that is a release must be documented by the BA.
What is the BA’s Role?

- Protect all information about individuals contained in agency records that *could* be PHI as if it is PHI.
- Do not discuss or disclose information from medical records.
- Direct requests for PHI (or requests for any information you do not routinely provide) to the Privacy Officer.
Safeguarding PHI

- Paper documents: lock up documents with PHI and separate from other documents (e.g., do not leave paper copies unattended)
- Computers database: password protect and limit access
- E-mail: encrypt emails containing PHI
- Personal devices: never store PHI on a personal computer or PDA
- Conversations: limit use of names, speak softly
- Mail: sealed envelope, mark ‘Confidential’ when applicable
- Faxes: mark confidential, verify numbers
- Social media: do not post PHI
Breaches of HIPAA

• The Privacy Officer must notify affected individuals and the Department of Health Services within 60 days of when a covered entity knows or should have known of the breach.

• Law enforcement exception may permit delay of notifications, but supporting documentation is required.

• Violations or breaches experienced by business associates are to be reported immediately to the Privacy Officer.

• The Privacy Officer will work with the breach response team to investigate, and if necessary mitigate and notify affected individuals.
For more information

If you have questions or need to report a violation, contact a UT Dallas HIPAA Officer:

HIPAA Privacy Officer
• Donise Pearson (214) 905–3133

HIPAA Security Officer
• Nate Howe (972) 883-6855

Law and Policies
• UT Dallas (HIPAA Privacy Manual)
• UT Dallas (HIPAA Security policy)
• UT Dallas (Information Security policies)