

<b>Policies of the University of North Texas</b>	<b>Chapter 7</b>
<b>07.010 Protected Health Information Privacy</b>	<b>Student Affairs</b>

**Policy Statement.** This policy is developed to ensure the privacy of protected health information and to comply with the Health Insurance Portability and Accountability Act (HIPAA) and the Texas Medical Records Privacy Act, and any other applicable federal or state privacy laws or regulations. The University of North Texas (UNT) must communicate clear and specific compliance standards and procedures to applicable parties regarding the prohibited and required uses and disclosures of Protected Health Information (PHI).

This policy is one component of the requirements of 45 CFR 164.530 that UNT have a policy that is consistent in scope with its covered health care activities. **Each health care component of UNT must also elaborate on any sections of this policy that its mission and scope requires. Each health care component must also create procedures and forms that comply with this policy, federal, and Texas laws and regulations, and that are consistent with its mission and its operations. It must also train its workforce in the use of its procedures and forms.**

**Application of Policy.** All University of North Texas faculty, staff, students, volunteers, and business associates or agents who are associated with a UNT designated health care component.

**Table of Contents.**

1. UNT as a HIPAA Hybrid Entity
  - a. Identification of UNT’s Health care Components
  - b. Privacy Officer and Contact Person
  - c. Documented Training Program
  - d. Signed Employee Confidentiality Statement
  - e. Changing Policies and Procedures
  - f. Documentation of Policies and Procedures
2. Relationship Between HIPAA and FERPA
3. General and Oversight Policies
  - a. Patient Notice of Privacy Practices
  - b. Consent for the Use and Disclosure of PHI
  - c. Specially Protected Medical Records
  - d. De-identification of Protected Health Information
  - e. Business Associates
4. Uses and Disclosures of Protected Health Information

- a. Minimum Necessary Requirement
  - b. Authorization for Use or Disclosure of PHI
  - c. Uses and Disclosures to Carry Out Treatment, Payment, or Health Care Operations
  - d. Authorization Required: Psychotherapy Notes
  - e. Authorization Required: Marketing
  - f. Authorization Required: Sale of PHI
  - g. Uses and Disclosures Required by Law
  - h. Uses and Disclosures for Public Health Activities
  - i. Disclosures about Victims of Abuse, Neglect, or Domestic Violence
  - j. Uses and Disclosures for Health Oversight Activities
  - k. Disclosures by Whistleblowers and Workforce Victims of Crime
  - l. Disclosures for Judicial and Administrative Proceedings
  - m. Disclosures for Law Enforcement Purposes
  - n. Uses and Disclosures about Decedents
  - o. Research Use of Health Information
  - p. Uses and Disclosures to Avert Serious Threat to Health or Safety
  - q. Workman’s Compensation Disclosures
  - r. Use and Disclosure to Family and Friends—Individual Care and Notification
  - s. Disclosures for Fundraising
  - t. Personal Representatives, Minors, and Deceased Individuals
5. Patient Rights
    - a. Access and Denial of Patient Request for PHI
    - b. Patient Right to Request Restriction of Uses and Disclosures
    - c. Confidential Communications
    - d. Right to Amend One’s Own Protected Health Information
    - e. Accounting for Disclosures and Patient Access to Disclosure Logs
  6. Security Safeguards
    - a. Electronic Communication of PHI
    - b. Storage of PHI
    - c. Printing and Copying of PHI
    - d. Disposal of PHI
  7. Administrative Requirements
    - a. Mitigation of Harmful Effects from Unauthorized Use
    - b. Reporting Violations of HIPAA
    - c. Sanctions for Breaches
    - d. Prohibition of Retaliation

**Definitions.**

1. Designated record set. “Designated record set” means a group of records maintained by or for UNT that are:

- a. The medical records and billing records about individuals maintained by or for a covered health care provider;
  - b. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
  - c. Used, in whole or in part, by or for UNT to make decisions about individuals.
2. Disclosure. “Disclosure” means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.
3. Health care operations. “Health care operations” means any of the following activities to the extent the activities are related to providing health care:
- Conducting quality assessment and improvement activities, patient safety activities, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting patients with information about treatment alternatives, and related functions that do not involve treatment;
  - Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
  - Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing or placing a contract for reinsurance of risk relating to claims for health care;
  - Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
  - Business planning and development, such as conducting cost management and planning related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or covered policies; and
  - Business management and general administrative activities:
    - Management activities related to HIPAA compliance;
    - Customer Service;
    - Resolution of internal grievances;
    - Due Diligence; and
    - Activities designed to de-identify health information and fundraising activities for the benefit of the institution.
4. HIPAA Privacy Rule. The “HIPAA Privacy Rule” establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers

that conduct certain health care transactions electronically. The HIPAA Privacy Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The HIPAA Privacy Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. The HIPAA Privacy Rule is located at 45 CFR Part 160 and Subparts A and E of Part 164.

5. HIPAA Security Rule. The “HIPAA Security Rule” establishes national standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. The HIPAA Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164.
6. Marketing. Except as otherwise provided in this policy, “marketing” means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.
7. Mental health records. “Mental health records” means any communication or records relating to the identity, diagnosis, evaluation or treatment of an individual with a mental or emotional condition or disorder, including alcoholism or drug addiction.
8. Payment. “Payment” means any activities undertaken either by a health plan or by a health care provider to obtain or provide reimbursement for the provision of health care. These activities include but are not limited to:
  - Determining eligibility, and adjudication or subrogation of health benefit claims;
  - Risk adjusting amounts due based on enrollee health status and demographic characteristics;
  - Billing, claims management, collection activities, obtaining payment under a contract for reinsurance, 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 pre-certification and preauthorization of services, concurrent and retrospective review of services; and
  - Disclosure to consumer reporting agencies of certain PHI relating to collection of premiums or reimbursement.
9. Protected Health Information (PHI). “Protected Health Information” or “PHI” means any individually identifiable health information that is transmitted or maintained in

any form or medium, including oral, written, and electronic. Protected health information excludes individual identifiable health information in education records covered by the Family Educational Rights and Privacy Act.

10. Psychotherapy notes. “Psychotherapy notes” means notes recorded by a mental health professional documenting or analyzing the contents of conversations during a private counseling session or a group, joint or family counseling session and that are separated from the rest of the individual’s medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, modalities and frequencies of treatment furnished, results of clinical tests , and any summary of the following items:
  - Diagnosis;
  - Functional status;
  - Treatment plan;
  - Symptoms;
  - Prognosis;
  - Progression to Date
11. Sale of PHI. “Sale of PHI” means, except as provided in section 4(f), a disclosure of PHI by a covered entity or business associate where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.
12. Substance abuse treatment records. “Substance abuse treatment records” means any records of the identity, diagnosis, prognosis or treatment of any individual that (1) relates to substance abuse education, prevention, training, treatment, rehabilitation or research and (2) is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States.
13. TPO. “TPO” means treatment, payment and health care operations.
14. Treatment. “Treatment” means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.
15. Use. “Use” with respect to individually identifiable health information means the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

16. Workforce. “Workforce” means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

**Procedures and Responsibilities.**

**1. UNT as a HIPAA Hybrid Entity**

UNT is a covered entity whose business activities include both covered and non-covered functions. Accordingly, UNT has elected to consider itself a hybrid entity for HIPAA purposes and will designate its health care components. UNT’s designated health care components must comply with the HIPAA Privacy Rule and the HIPAA Security Rule. UNT’s non-health care components need not comply with these requirements.

**a) Identification of UNT’s Health care Components, 45 CFR §164.504(b)**

UNT’s HIPAA Compliance Officer and the UNT System Office of General Counsel shall define UNT’s health care components. The remaining components will be designated as non-covered components. The HIPAA Compliance Officer and the UNT System Office of General Counsel will review this list every two years and will update it as needed.

**Each UNT health care component shall develop the procedures, forms, and training for its workforce members that are necessary to carry out the requirements of this policy.**

**b) Privacy Officer and Contact Person, §164.530(a)**

**Each health care component shall designate a Privacy Officer, who will maintain accountability for privacy within the unit or clinic.** This individual may share this role with other duties, as long as a conflict of interest is not created by their multiple duties. In cases where a conflict of interest might arise, the Privacy Officer shall consult with the health care component’s management and with the UNT HIPAA Compliance Officer so that an alternate person may be designated to assume those duties that create the conflict of interest.

**Each health care component shall also designate a Contact Person, who may be the same individual as the Privacy Officer. The role of the Contact Person is to accept complaints.**

The Privacy Officer will oversee the health care component’s Privacy Program, including:

- Developing and implementing privacy policies and procedures, in accordance with federal and Texas privacy requirements.
- Receiving and processing authorizations.

- Receiving and processing restrictions on authorizations.
- Receiving and processing revocations of authorizations.
- Overseeing that all members of the component’s workforce who come into contact with PHI are properly trained.
- Approving all disclosures that do not require an authorization, or opportunity for the patient to agree or object.
- Drafting and distributing the Notice of Privacy Practices.
- Mitigating the effects of all disclosures that are not compliant with federal or Texas law or with the policies or procedures of the unit or clinic.
- Conducting, at least annually, a review of the implementation of the “minimum necessary” requirements.
- Conducting, at least annually, a review of the component’s access procedures and relevant records.
- Guiding and assisting in the identification, implementation, and maintenance of privacy policies and procedures in conjunction with the component’s management, the UNT System Office of General Counsel, and the UNT HIPAA Compliance Officer.
- Reviewing all patient information security plans to align security and privacy practices.
- Performing initial and periodic risk assessments or “privacy audits” and conducting ongoing compliance monitoring activities.
- Overseeing that the component maintains appropriate consent and authorization forms, information notices, and materials that reflect current organization and legal practices and requirements.
- Overseeing compliance with privacy practices and application of sanctions for failure to comply with privacy practices.

This list provides an overview of the duties of the Privacy Officer and is not comprehensive.

**c) Documented Training Program, §164.530(b)**

**The Privacy Officer of each health care component shall be responsible for ensuring that members of the component’s workforce are properly trained in the requirements of federal and Texas law.** All members of the workforce who come into contact with PHI in performing their job functions shall be trained on the privacy laws and the procedures regarding PHI.

The term “workforce” includes, employees, volunteers, and any other individual performing work for the health care component, who is under direct control of the component’s management, regardless of whether or not they are paid.

Training shall meet the following requirements:

- All current members of the workforce shall complete training within 60 days following the date when they start their duties and every two years thereafter.
- The supervisor of the workforce member shall be responsible for initiating training.
- Workforce members whose duties are affected by a material change in the privacy laws or policies shall be retrained with 60 days after the change becomes effective.
- Workforce members who have violated privacy laws, policies, or procedures shall be retrained within thirty days of the determination.

The Privacy Officer shall document each training session and the names of the workforce members who completed training. Such documentation shall be maintained within the health care component's privacy records for at least seven years from the date of training.

**The Privacy Officer shall provide a summary annual report of the component's training activities to the UNT HIPAA Compliance Officer.**

**d) Signed Employee Confidentiality Statement**

All workforce members who come into contact with PHI in performing their job function, and who have completed required training in confidentiality procedures, shall acknowledge in writing that they have completed their training and that they will comply with the provisions of federal and Texas law, University policy, and the health care component's policies and procedures.

The health care component shall provide a form for this purpose and shall keep it on file for a period of seven years from the date when it was signed.

**e) Changing Policies and Procedures, §164.530(i)(2)**

The UNT HIPAA Compliance Officer is responsible for maintaining this policy. If changes in federal or Texas laws or regulations require changes in this policy, the UNT HIPAA Compliance Officer will consult with necessary parties both within and outside UNT to develop the required policy changes.

Changes in this policy may also be requested by UNT management or by the management or Privacy Officer of any health care component within UNT. Proposed changes will be submitted to the UNT HIPAA Compliance Officer for consideration and development.

Health care components within UNT must also develop a procedure for changing their policies and procedures and for updating forms, records, and agreements.



If changes in policies or procedures materially affect the way in which workforce members carry out their duties, the affected workforce members will be retrained in compliance with Section 1(c) of this policy.

**f) Documentation of Policies and Procedures, §164.530(j)**

The UNT HIPAA Compliance Office must retain documentation of these changes for a period of seven years from the time the documentation was created, unless a longer period is prescribed by other federal or Texas regulations.

**UNT and its health care components must maintain the policies and procedures required by this policy in written or electronic form. Whenever a communication is required to be in writing, UNT or its health care components, as appropriate, shall maintain a record of this communication, or an electronic copy, as documentation. Whenever an action, activity, or designation is required to be documented, UNT or its health care components, as appropriate, shall maintain a written or electronic record of such action, activity, or designation.**

**2. Relationship Between HIPAA and FERPA**

The HIPAA Privacy Rule safeguards “protected health information,” whereas the Family Educational Rights and Privacy Act (FERPA) addresses privacy of “education records.” FERPA’s education records are specifically exempted from the HIPAA definition of “protected health information.”

FERPA defines education records as those records that contain information directly related to a student that are maintained by an education agency, institution or a person acting for the agency or institution. FERPA education records do not include records of students who are 18 years or older, or are attending post-secondary educational institutions, that are:

- Created or maintained by a physician, psychiatrist, psychologist, or recognized professional or paraprofessional acting or assisting in that capacity;
- Created, maintained, or used only in connection with the provision of treatment to the student; and
- Not available to anyone, except a physician or appropriate professional reviewing the record as designated by the student.

These treatment records are not available to anyone other than professionals providing treatment to the student, or to physicians or other appropriate professionals of the student’s choice. Any use or disclosure of the above treatment records for other purposes, including providing access to the individual student who is the subject of the information, turns the record into an educational record protected by FERPA (requiring

written consent or other FERPA exception to disclose). A student may access his or her medical records (now “education records” because they’re not being used for treatment) by making a request under the Texas Public Information Act.

To avoid the need to apply two different standards to student records, HIPAA excludes from its definition of “protected health information” health information in education records and treatment records. Accordingly, uses and disclosures of education records and treatment records must be in accordance with FERPA.

This policy recognizes that both HIPAA and FERPA require authorization from an individual to disclose their protected health information. In some circumstances, FERPA requirements may be more stringent than HIPAA requirements. To facilitate the operation of all UNT health care components, all discussions of consents and authorizations in this policy apply to both HIPAA and FERPA records. **UNT health care components shall develop only one set of forms and procedures to comply with both sets of federal regulations. Each health care component Privacy Officer shall be responsible for overseeing the processing of authorizations and requests for PHI, regardless of which set of regulations applies. However, the Privacy Officer will ensure that the permissions needed to approve a HIPAA or FERPA request will be obtained from the proper authority.** The UNT System Office of General Counsel shall have the authority to approve all FERPA requests, and is designated as the final authority for many types of HIPAA requests.

There will be instances in which student records will be converted from HIPAA records to FERPA records. For example, students with disabilities requesting accommodations are often asked to produce a physician’s certification of disability before the institution makes the requested accommodation. The information disclosed by the non-institution-affiliated physician ceases to be protected health information under HIPAA once the information is shared, at the student’s request, with the institution. UNT must accept this information and protect it as it would receive and protect any other HIPAA PHI. However, now that the student has made the medical information available to the institution, it falls under the protections of FERPA and may not be further released without the student’s permission.

### **3. General and Oversight Policies**

#### **a) Patient Notice of Privacy Practices, 45 CFR §164.520**

**An individual has a right to adequate notice of the uses and disclosures of PHI that may be made by UNT and its health care components, and of the individual’s rights and UNT’s responsibilities with respect to PHI. UNT health care components are required to provide a Notice of Privacy Practices (NPP) to all patients or clients, as well as to other individuals requesting a copy. Those persons who register patients or clients will be responsible for distributing a copy of the NPP to all patients or clients.**

### General Requirements

#### **UNT health care components must:**

- Develop the required NPP, forms, procedures, and workforce training related to this section;
- Provide the notice no later than the date of the first service delivery, including service delivered electronically to an individual;
- Make a good faith effort to obtain a written acknowledgement of the receipt of NPP from the patient or client and document the receipt of the NPP, using an appropriate acknowledgement form and filing system;
- Have the NPP available at the service delivery site for individuals to take with them;
- Post the NPP in a clear and prominent location where it is reasonable to expect individuals seeking service from the UNT health care component to be able to read the NPP; and
- Whenever the NPP is revised, provide the new NPP to all patients or clients on their next visit on or after the effective date of the revision.

If a patient or client is treated on an emergency basis, the UNT health care component may delay providing the NPP and receiving an acknowledgement until a practical time.

### Notice

The NPP must be written in plain language and must contain the following elements:

- Header. “THIS NPP DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.” This header must be at the top of the notice, in capital letters, or otherwise in a prominent location on the notice.
- Uses and disclosures. The NPP must contain:
  - A description of the types of uses and disclosures that the UNT health care component is permitted to make, including at least one example for each of the following purposes: Treatment, Payment, and Health Care Operations (TPO);
  - A description of each of the purposes for which UNT is permitted or required to use or disclose PHI without the individual’s written authorization;
  - A description of the types of uses and disclosures that require an authorization, including a statement indicating that most uses and disclosures of psychotherapy notes (where appropriate), uses and disclosures of PHI for marketing purposes, and disclosures that constitute a sale of PHI require authorization;

- A statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization, and that the individual may revoke such authorization, using the appropriate forms;
- A statement that the UNT component may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual;
- A statement that UNT may contact the individual to raise funds for UNT and the individual has a right to opt out of receiving such communications; and
- A statement that the individual's protected health information is subject to electronic disclosure.
- Individual rights. The NPP must contain a statement of the individual's rights with respect to PHI and a brief description of the procedures that the individual would use to exercise these rights, including the following:
  - The right to request restrictions on certain uses and disclosures of PHI, including a statement that UNT is not required to agree to a requested restriction except in the case of a disclosure to a health plan where the disclosure is for the purpose of carrying out payment or health care operations and the PHI pertains solely to a health care item or service for which the individual, or a person other than the health plan on behalf of the individual, has paid in full;
  - The right to receive confidential communications of PHI;
  - The right of the individual to inspect and obtain a copy of the individual's own PHI;
  - The right to request an amendment to PHI;
  - The right to receive an accounting of disclosures of PHI; and
  - The right of an individual, including an individual who has agreed to receive the NPP electronically, to obtain a paper copy of the NPP on request.
- Health care component's duties. The NPP must contain a statement that the UNT health care component:
  - Is required by law to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy practices with respect to PHI and to notify affected individuals following a breach of unsecured protected health information;
  - Is required to abide by the terms of the NPP currently in effect; and
  - Reserves the right to change the terms of its NPP and to make the new provisions effective for all PHI that it maintains. The statement must also describe how it will provide individuals with a revised NPP.
- Complaints. The NPP must contain a statement that individuals may complain to the UNT health care component, and to the Department of Health and Human Services, if they believe that their privacy rights have been violated, a brief description of how the individual may file a complaint with the UNT health care

component or the UNT Office of Institutional Compliance, and a statement that the individual will not be retaliated against for filing a complaint.

- **Contact.** The NPP must contain the name, or title, and telephone number of a person or office to contact for further information.
- **Effective date.** The NPP must contain the date on which the NPP is first in effect, which may not be earlier than the date on which the NPP is printed or otherwise published.

#### **Electronic Notice**

- The UNT health care component's NPP must be posted on its web site.
- If electronic mail is used to send a copy of the NPP to an individual, the electronic mail communication must comply with Section 6(a) of this policy. If the UNT health care component becomes aware that the email transmission was not successful, it must provide a paper copy of the NPP to the individual.
- Electronic notice by the UNT health care component satisfies the notice requirement if receipt of the NPP is documented and retained by the health care component.
- The individual who is the recipient of an electronic notice retains the right to obtain a paper copy of the NPP from the UNT health care component on request.

#### **Documentation of Notice**

The UNT health care component must make a good faith effort to obtain a written acknowledgment of receipt of the NPP. Those persons who register patients or clients shall be responsible for distributing the NPP to all patients or clients, documenting receipt of the acknowledgment form in an appropriate filing system, and retaining the original signed form in the patient's or client's file or record. If the individual refused to sign the acknowledgement form or if it was otherwise impossible to receive an acknowledgement from the individual, the health care component must document on the acknowledgement form the reason why written acknowledgement was not obtained.

#### **Revisions to the Notice**

The UNT health care component must promptly revise and distribute its NPP whenever there is a material change to its uses or disclosures, an individual's rights, UNT's legal duties, or other privacy practices that are stated in the NPP. Except when required by law, a material change to a term of the NPP may not be implemented prior to the effective date of the NPP in which such material change is reflected. The UNT health care component must document compliance with the notice requirements by retaining copies of the NPP's they have issued.

## **b) Consent for the Use and Disclosure of PHI**

UNT health care components shall obtain written consent prior to using and/or disclosing a student's PHI for treatment, payment or health care operations (TPO) purposes.

Consents for the use and disclosure of PHI for TPO must have the following elements for the consent to be effective:

- Inform the patient or personal representative that PHI may be used and disclosed to carry out TPO;
- Specify the type of records that will be used or disclosed (eg. medical records);
- Identify the class of parties to whom disclosure may be made;
- Refer the patient or personal representative to the NPP for a more complete description of such uses and disclosures;
- State the patient or personal representative may request a restriction be placed on the consent (see Section 5(b)); and
- The consent must be signed by the patient or personal representative and dated.

## **c) Specially Protected Medical Records**

### Substance Abuse Treatment Records

Substance Abuse Treatment Records must be treated differently from other types of PHI. The content of a Substance Abuse Treatment Record may be disclosed pursuant to and in accordance with the prior written authorization of the individual. Absent an authorization, UNT may only disclose an individual's Substance Abuse Treatment Record under the following circumstances:

- To medical personnel to the extent necessary to treat the individual in an emergency situation.
- To qualified personnel for the purpose of conducting scientific research, management audits, financial audits, or program evaluation, but such personnel may not identify, directly or indirectly, any individual receiving treatment in any report of such research, audit, or evaluation, or otherwise disclose individual identities in any manner.
- To a person who is authorized by an appropriate order of a court of competent jurisdiction to receive the information in the Substance Abuse Treatment Record.

### Other Specially Protected Medical Records

The following medical records are subject to special confidentiality protection and shall not be disclosed except as permitted by law:

- Psychotherapy notes (see Section 4(d));
- Mental health records;

- HIV/AIDS records.

UNT health care components should contact the UNT HIPAA Compliance Officer with questions on using or disclosing these records. The UNT HIPAA Compliance Office will consult with the UNT System Office of General Counsel on using or disclosing these records.

**d) De-identification of Protected Health Information, 164.502(d), 164.514(a),(b)**

PHI is rendered anonymous whenever its identifying characteristics are completely removed. PHI must be de-identified prior to disclosure to non-authorized users. De-identified PHI should be used for any permitted purpose whenever this is possible and feasible.

All personnel must strictly observe the following standards for de-identification of PHI:

To de-identify PHI, the following identifiers of the patient must be removed:

- Names
- Geographic subdivisions smaller than a State, including street address, city, county, and zip code.
- All elements of dates, except the year
- Telephone numbers
- Fax numbers
- Email addresses
- Social security numbers
- UNT identification numbers and medical record numbers
- Health beneficiary plan numbers
- Account numbers
- Certificate or license numbers
- Vehicle identifiers, including license plate numbers
- Device ID and serial numbers
- Web Universal Resource Locators (URL)
- Internet Protocol (IP) addresses
- Biometric identifiers
- Full face photographic images and other comparable images
- Any other unique identifying number, characteristic, or code

Whenever possible, de-identified PHI should be used for routine reporting and for quality assurance monitoring or audits.

An authorized user who wishes to encrypt PHI to de-identify it must ensure that the encryption code is not based on information about the individual whose information is being de-identified, and that the code cannot be translated so as to identify the individual.

**e) Business Associates**

A business associate is a person or entity, other than a workforce member, that performs a function that involves PHI for a health care component of UNT.

**Notwithstanding anything to the contrary, each health care component must establish a business associate agreement with each of their business associates prior to using or disclosing PHI.** The business associate contract must establish the permitted and required uses and disclosures of PHI by the business associate. This use or disclosure must comply with all the federal and Texas privacy laws and regulations in the same way that the health care component must also comply. The contract must meet the requirements of 45 CFR §164.504 and must be approved by the UNT System Office of General Counsel before it is executed.

The health care component must determine and document that the business associate has provided satisfactory assurances that it is able to meet the requirements of the contract and to protect the privacy of PHI. The contract must authorize termination of the contract if the business associate violates a material term of the contract.

If the health care component becomes aware of a business associate's violation of the terms of the contract or of federal and Texas laws and regulations, it must take reasonable steps to prevent or to mitigate any improper use or disclosure of PHI. If reasonable steps to correct a business associate's contract violations are not successful in preventing or mitigating improper use or disclosure of PHI, the health care component must terminate the contract, if feasible.

**4. Uses and Disclosures of Protected Health Information**

**a) Minimum Necessary Requirement, 164.502(b), 164.514(d)**

When using or disclosing PHI or when requesting PHI from another covered entity or business associate, UNT must limit the use, disclosure or request to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. Minimum Necessary does not apply in the following circumstances:

- Disclosures to or requests by a health care provider for treatment;
- Uses and disclosures made to the individual;
- Uses and disclosures based upon a valid written authorization;
- Disclosures made to the Department of Health and Human Services;



- Uses and disclosures required by law; and
- Uses and disclosures required by other sections of the HIPAA privacy regulations.

Limitations on Use and Disclosure

All persons who handle PHI in any manner are expected to know and to abide by the following:

- Determining workforce access to PHI. Access to PHI shall be granted to persons based on their role, as determined by their supervisor, manager, and unit head. **The UNT health care component shall identify:**
  - Those persons or classes of persons in the UNT workforce, including students, trainees, and volunteers, who need access to PHI to carry out their duties, and
  - For each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.
- **Requests for Uses or Disclosures of PHI. Except in emergency situations, any person requesting PHI from the medical record custodian must include the requestor's name, unique identifier, and the amount of information requested.**
- **Audits. The UNT health care component Privacy Officer shall be responsible for facilitating random checks to ensure that the minimum necessary standard is being applied when using and disclosing PHI.**
- **Requests for uses and disclosures of entire medical records. Medical record custodians must not use, disclose, or request the entire medical record except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.**

Disclosures for Payment

Only the minimum necessary PHI shall be disclosed for payment functions. Persons handling PHI for payment shall not discuss or disclose information about an individual's diagnosis or treatment. This policy shall apply to checks collected, credit card paper receipts, envelopes and invoices sent to patients or clients.

Disclosures Required by Law

PHI about a victim of crime or abuse: UNT may only release the minimum necessary amount of information to law enforcement officials, unless the law requires certain other information to be released, in which case UNT must comply with relevant statutes, laws, regulations, and subpoenas.

In response to an order of a court or an administrative tribunal, UNT must release all information, but only that information, required by the order. The minimum necessary standard does not apply.

Disclosures for Worker's Compensation

PHI may be disclosed to comply with Worker's Compensation laws and regulations without the consent, authorization, or opportunity to object by an individual. Such disclosure will be only the minimum necessary information.

Minimum Necessary Use and Disclosure for Student Workers, Trainees, and Volunteers

Students, trainees, and volunteers are to adhere to the minimum necessary standard. They shall have access to records only to the degree that their duties require this access, and their supervisor shall train them in the privacy regulations of the UNT health care component in which they provide services.

Minimum Necessary Use and Disclosure for Educational Purposes

Faculty, staff, students, and trainees are to use de-identified information when in a classroom setting. A patient's identifying information is not needed for educational purposes.

**b) Authorization for Use or Disclosure of PHI, 45 CFR 164.508**

General Requirements

Except as otherwise permitted by this section, UNT and its health care components may not use or disclose PHI without a valid authorization from the individual. An individual requesting the release of the individual's own PHI must complete and sign the authorization form developed by the health care component. UNT's release of PHI must comply with the directives stated in the authorization. The UNT health care component must save all signed authorizations in the individual's record. PHI may be disclosed without an authorization if the law requires such disclosure. The UNT health care component from which PHI is released must document the disclosure in its database used for this purpose.

Requirements for a Valid Authorization, 164.508(b)

All authorizations must contain the required core elements.

Core Elements

A valid authorization must contain at least the following elements and must be written in plain language:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful way.

- The name or other specific identification of the person or the class of persons who are authorized to make the requested use or disclosure;
- The name or other specific identification of the person or the class of persons to whom a health care component of UNT may make the requested use or disclosure;
- A description of each purpose of the requested use or disclosure;
- An expiration date for the request. Unless it is revoked sooner, the authorization is valid for 180 days after the date it is signed;
- A statement of the individual's right to revoke the authorization in writing, any exceptions to the right to revoke, and a description of the process that the individual would use to revoke the authorization;
- A statement that the information use or disclosed pursuant to the terms of the authorization is no longer protected by the HIPAA privacy regulations, and it may be re-disclosed by the recipient; and
- Signature of the individual and the date. If a personal representative signs for the individual, a description of the representative's authority to act for the individual.
- A statement that UNT or the health care component will not condition treatment, payment, or eligibility for benefits on the individual providing the authorization, unless one of these exceptions exist:
  - UNT may condition the provision of research-related treatment on provision of an authorization, or
  - UNT may condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of the PHI to such third party.
- If use or disclosure of the requested information will result in remuneration to UNT from a third party, a statement of such remuneration must be included

### Defective Authorizations

An authorization is considered defective and invalid if any material information in the authorization is known by UNT or any member of its workforce to be false, or if any of the following defects exist:

- The expiration date has passed or the expiration event is known by the UNT health care component to have occurred;
- The authorization has not been filled out completely or signed;
- The authorization is known by the UNT health care component to have been revoked;
- The authorization lacks any of the core elements; or
- The authorization violates the exception allowing compound authorizations or the prohibition on conditioning of authorizations.

## Compound Authorizations

An authorization for use and disclosure of PHI may not be combined with any other document to create a compound authorization, except for the following:

- An authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same or another research study;
- An authorization for the use and disclosure of psychotherapy notes may only be combined with another authorization for use and disclosure of psychotherapy notes; or
- An authorization, other than that for a use and disclosure of psychotherapy notes, may be combined with any other such authorization if neither authorization conditions the provision of treatment, payment, or eligibility for benefits on the provision of the authorization.

### **c) Uses and Disclosures to Carry Out Treatment, Payment, or Health Care Operations**

HIPAA does not require an authorization for uses or disclosures of PHI for carrying out the following treatment, payment or health care operations (“TPO”):

- Use or disclosure for the purpose of UNT’s own treatment, payment or health care operations.
- Disclosure for treatment activities of another health care provider.
- Disclosure to another covered entity or a health care provider for the payment activities of the entity receiving the information.
- Disclosure to another covered entity for the health care operations of the entity receiving the information, as long as UNT and the covered entity has or had a relationship with the individual who is the subject of the PHI requested, the PHI pertains to that relationship and the disclosure is for either the first or second bullet points in the definition of “health care operations” or is for health care fraud and abuse detection or compliance.

However, some records maintained by UNT health care components are covered by FERPA and not HIPAA. To cover all records maintained by UNT health care components, UNT requires that UNT workforce members obtain from each patient a signed Consent for the Use and Disclosure of PHI form prior to any use or disclosure of PHI to carry out TPO. Each UNT health care component shall develop the necessary Consent form and ensure that individuals receive it when they receive the NPP. See Section 3(b) for additional information.

**d) Authorization Required: Psychotherapy Notes**

UNT and its health care components must obtain an authorization for any use or disclosure of psychotherapy notes, except:

- To carry out the following treatment, payment, or health care operations:
  - The notes originated in the same UNT health care component that is carrying out treatment;
  - Use or disclosure for training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint family, or individual counseling; or
  - Use or disclosure for UNT to defend itself in a legal action or other proceeding brought by the individual;
- When the health care component must use or disclose the information as required by the Secretary of Health and Human Services to investigate, audit, or determine compliance with privacy regulations in the UNT health care component. However, psychotherapy notes relating to a student may not be released to HHS, as these are either medical records exempt from FERPA or they may be student records, both of which are not covered by HIPAA;
- The use or disclosure is required by law and is limited to relevant requirements of the law;
- The health care component makes the disclosure to a health oversight agency that is carrying out its responsibilities to oversee the treatment and operations of the originator of the psychotherapy notes. The health care component may be required to enter into Business Associate Agreements with certain health oversight agencies; or
- The health care component discloses information to coroners or medical examiners for the purpose of identifying a deceased individual determining a cause of death, or other duties authorized by law.

**e) Authorization Required: Marketing**

UNT and its health care components must obtain an authorization for any use or disclosure of PHI for marketing, except if the communication is in the form of:

- Providing information on health-related products and services in a face-to-face encounter with a patient or client.
- Providing a patient or client with refill reminders or other information on a drug or biologic that is currently being prescribed for the individual, as long as any financial remuneration received by UNT in exchange for making the communication is reasonably related to the cost of making the communication.
- Providing treatment of an individual by a health care provider, except where UNT receives financial remuneration in exchange for making the communication.

- Providing promotional gifts of nominal value (pens, calendars, etc.).

If the marketing involves financial remuneration to UNT from a third party the authorization must state that such remuneration is involved.

If UNT or a UNT health care component sends a written marketing communication through the mail, the communication must be sent in an envelope showing only the names and addresses of the sender and recipient and must (1) state the name and toll-free number of the entity sending the marketing communication; and (2) explain the recipient's right to have the recipient's name removed from the sender's mailing list. The name shall be removed not later than the 5th day after the date UNT receives the request.

**No written marketing communication may be sent to an individual without an authorization from the individual.**

**f) Authorization Required: Sale of PHI, 164.508(a)(4)**

UNT and its health care components must obtain an authorization for any disclosure of PHI which is a sale of PHI. Sale of PHI does not include a disclosure of PHI (1) for public health purposes, (2) for research purposes where the only remuneration received is a cost based fee to cover the cost to prepare and transmit the PHI, (3) for treatment and payment purposes, (4) for the sale, transfer, merger or consolidation of all or part of the covered entity, (5) providing access or accounting to an individual, and (6) as otherwise required by law. Such authorization must state that the disclosure will result in remuneration to UNT.

For example, if a pharmaceutical company offers to pay UNT for a list of patients who suffer from a particular affliction to be used to send discount coupons for a new medication directly to the patients, the arrangement between UNT and the pharmaceutical company would constitute a sale of PHI, and UNT would need to obtain specific patient authorization prior to providing the patient list. Alternatively, if UNT receives grant funding to conduct a program and, in return, must supply PHI to the funder, the provision of PHI is a byproduct of the arrangement and not a sale of PHI.

**g) Uses and Disclosures Required by Law, 164.512(a)**

UNT may use or disclose PHI to the extent the use or disclosure is required by law. The information used or disclosed must be limited in scope to comply with and to meet the requirements of the law.

**h) Uses and Disclosures for Public Health Activities, 164.512(b)**

UNT may use or disclose PHI for the public health activities outlined in HIPAA, including reporting disease to a public health authority.

**i) Disclosures about Victims of Abuse, Neglect, or Domestic Violence, 164.512(c)**

UNT may disclose to a government agency PHI about an individual whom the person has reasonably determined to be a victim of abuse, neglect, or domestic violence if:

- The disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of the law;
- The individual agrees to the disclosure; or
- The disclosure is expressly authorized by statute or regulation and:
  - The disclosure is necessary to prevent serious harm to the individual or other potential victims, or
  - If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that:
    - The PHI sought is not intended to be used against the individual; and
    - An immediate enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

The Privacy Officer of the UNT health care component that disclosed PHI pursuant to this section must promptly inform the individual that such a report has been or will be made, unless:

- Informing the individual would place the individual at risk of serious harm, or
- A personal representative would be the legally appropriate party to inform, and this personal representative is responsible for the abuse, neglect, or other injury, and informing this person would not be in the best interests of the individual under medical care.

**j) Uses and Disclosures for Health Oversight Activities, 164.512(d)**

UNT may disclose PHI without an authorization to a health oversight agency for oversight activities authorized by law. These activities include:

- Audits
- Civil, administrative, or criminal investigations, proceedings, or actions
- Inspections
- Licensure or disciplinary actions
- Other activities necessary for appropriate oversight of:
  - The health care system
  - Government benefit programs for which health information is relevant for beneficiary eligibility
  - Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards, or
  - Entities subject to civil rights laws for which health information is necessary for determining compliance.

Disclosure is *not* permitted if the individual is the subject of an investigation or activity and the investigation or activity is not directly related to:

- The individual's receipt of health care
- A claim for public benefits related to health (for example, food stamps), or
- The individual's qualification for or receipt of public benefits or services when the individual's health is integral to the claim for public benefits or services.

If a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation related to a claim for public benefits that are not related to health, the joint activity or investigation shall be considered a health oversight activity.

#### **k) Disclosures by Whistleblowers and Workforce Victims of Crime**

Members of the UNT workforce are encouraged to report conduct that is unlawful or that violates professional or clinical standards to the UNT HIPAA Compliance Officer or the UNT Office of Institutional Compliance. Disclosure of PHI to the Compliance Office for the purpose of reporting unlawful conduct or a violation of professional or clinical standards is always in compliance with this policy.

A member of the UNT workforce or a business associate may disclose PHI if the following conditions are met:

- The workforce member or business associate believes in good faith that UNT or one of its health care components has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by UNT or its health care components potentially endangers one or more patients, workers, or the public, and



- The disclosure is to:
  - A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of UNT,
  - An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct at UNT, or
  - An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to conduct believed to be unlawful or in violation of professional or clinical standards.

A member of the UNT workforce may also disclose PHI without violating this policy if:

- The workforce member is a victim of a criminal act; and
- The disclosure is to a law enforcement official, provided that:
  - The PHI disclosed is about the suspected perpetrator of the criminal act; and
  - The PHI disclosed is limited to the suspected perpetrator's:
    - Name and address
    - Date and place of birth
    - Social security number
    - ABO blood type and Rh factor
    - Type of injury
    - Date and time of treatment
    - Date and time of death, if applicable, and
    - Description of the individual's distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars or tattoos

**I) Disclosures for Judicial and Administrative Proceedings, 164.512(e)**

UNT may disclose PHI in the course of any judicial or administrative proceeding if the following conditions are met:

- The disclosure is in response to a court order or administrative tribunal, but only the PHI expressly authorized by the order may be disclosed
- The disclosure is in response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or an administrative tribunal (such as a subpoena from a government agency) provided that:
  - UNT receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to ensure that the subject of the requested PHI has been given notice of the request, evidenced by an affidavit from the requesting party, or

- UNT receives satisfactory assurance from the party seeking the information that this party has made reasonable efforts to secure a qualified protective order. A qualified protective order is an order of a court or an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:
  - Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested, and
  - Requires returning the PHI to UNT or requires destroying the PHI and all copies made at the end of the litigation or proceeding.

If the above conditions are not met, UNT has the option to disclose PHI in response to lawful process without receiving full satisfactory assurances, provided that UNT has made its own reasonable efforts:

- To provide notice to the individual sufficient to meet the requirements of this section, or
- To seek a qualified protective order.

**m) Disclosures for Law Enforcement Purposes, 164.512(f)**

UNT may disclose PHI to a law enforcement official for a law enforcement purpose under the following conditions:

- For the purpose of complying with laws that require reporting certain kinds of wounds or other physical injuries, UNT may disclose PHI to appropriate law enforcement officials or agencies.
- For the purpose of complying with a court order, warrant, subpoena, summons, grand jury subpoena, administrative request or subpoena, a civil or authorized investigative demand, or similar process authorized by law, UNT may disclose PHI to authorized officials, provided that in the case of an administrative request:
  - The information requested is relevant and material to a legitimate law enforcement inquiry;
  - The request is specific and limited in scope to the purpose for which the information is sought; and
  - De-identified information cannot reasonably be used.
- For the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, UNT may release PHI in response to a request by a law enforcement official, provided that the information is limited to the following:
  - Name and address
  - Date and place of birth
  - Social security number
  - ABO blood type and rh factor

- Type of injury
- Date and time of treatment
- Date and time of death, if applicable, and
- A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos

PHI related to an individual's DNA or DNA analysis, dental records, or typing, sample, or analysis of bodily fluids or tissues may NOT be disclosed in response to such a request for PHI by law enforcement official.

- To provide information about an individual who is or is suspected to be a victim of a crime, UNT may release PHI in response to a request by a law enforcement official, provided:
  - The individual agrees to the disclosure, or
  - UNT is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:
    - The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and that such information is not intended to be used against the victim;
    - The law enforcement official represents that immediate law enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
    - The disclosure is in the best interests of the individual as determined by the UNT health care component in the exercise of their professional judgment.
- For the purpose of alerting law enforcement of the death of the individual, UNT may disclose PHI about a deceased individual to law enforcement officials, if UNT has a suspicion that such death may have resulted from criminal conduct.
- For the purpose of providing evidence of criminal conduct that occurred on UNT premises, UNT may disclose PHI to law enforcement officials that UNT believes in good faith constitutes evidence of the crime.

**n) Uses and Disclosures about Decedents, 164.512(g),(h)**

UNT may disclose PHI about a deceased individual for the following purposes:

- To coroners and medical examiners for the purposes of identifying a deceased person, determining a cause of death, or other duties as authorized by law;
- To funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the deceased. If necessary for the funeral directors to carry out their duties, UNT may disclose PHI prior to and in reasonable anticipation of the individual's death; or

- To organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissues for the purpose of facilitating organ, eye, or tissue donation and transplantation.

**o) Research Use of Health Information, 164.512(i)**

The use and disclosure of PHI in research must have appropriate authorizations and safeguards in place. The UNT IRB review process is responsible for determining which federal and Texas standards apply to the use and disclosure of PHI for research. All researchers and their staff must rigorously comply with the procedures of the IRB and of the Office of Research Services in the use of PHI.

Faculty, staff, and students of UNT may not initiate research involving human subjects without approval of the IRB before the research starts. Please see , and its associated procedures, for an explanation of the requirements of the IRB approval process.

Whenever possible, de-identified PHI should be used for research. When de-identified PHI is to be used for research, including public health research, the standards listed in Section 3(d) below must be followed. In addition:

- PHI used for research should be de-identified at the point of data collection for research protocols approved by the IRB, unless the participant voluntarily and expressly consents to the use of his or her personally identifiable information or the researcher(s) obtain an IRB waiver of authorization.
- If PHI is de-identified by means of encryption, anyone involved in the research project must not disclose the encryption code and must not disclose the mechanism used to re-identify the information.

**p) Uses and Disclosures to Avert Serious Threat to Health or Safety, 164.512(j)**

Consistent with applicable law and standards of ethical conduct, UNT may disclose PHI, provided:

- UNT, in good faith, believes that the use or disclosure:
  - Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and
  - Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or
  - Is necessary for law enforcement authorities to identify or apprehend an individual:
    - Because of a statement by an individual admitting participation in a violent crime that UNT reasonably believes may have caused serious physical harm to the victim, or

- Such use or disclosure is not permitted if UNT learned the protected information in the course of treatment that is designed to alter or change the desire to commit the criminal conduct that would be the basis for making a disclosure, or when an individual initiates or is referred to a health care component of UNT for treatment, counseling, or therapy.
- Where it appears from all the circumstances that the individual has escaped from lawful custody.

UNT may only release the statement relating to the serious threat and the PHI related to the serious threat.

**q) Workman’s Compensation Disclosures, 164.512(l)**

UNT may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers’ compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

**r) Use and Disclosure to Family and Friends—Individual Care and Notification, 164.510(b)**

UNT health care components may disclose to an individual’s family member, other relative, a close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to that person’s involvement with the individual’s health care or payment related to the individual’s health care. UNT may use or disclose PHI to notify, or assist in the notification of, a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual’s location, general condition, or death.

If the individual is present or otherwise available and if the individual has the capacity to make health care decisions, the UNT health care component may use or disclose the PHI if it:

- Obtains the individual’s verbal or written agreement to do so
- Provides the individual with the opportunity to object to the disclosure, and the individual does not object, or
- Reasonably infers from the circumstance, based on the exercise of professional judgment, that the individual does not object to the disclosure.

The workforce member attending the individual shall note in the individual’s chart or record whether or not the individual was able to consent, whether or not consent was given, and what if any limitations on disclosure the individual requested.

If the individual is not present or if because of the individual's incapacity or because of emergency circumstances the individual does not have the capacity or opportunity to agree or to object, the UNT health care component may, in its exercise of professional judgment, determine whether the disclosure is in the best interest of the individual. If so, it shall disclose only the PHI that is directly relevant to the person's involvement with the individual's health care. UNT health care components may use professional judgment and experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X rays and other diagnostic media, and similar forms of PHI.

**s) Disclosures for Fundraising, 164.514(f)**

UNT or a UNT health care component may use or disclose to a business associate or to an institutionally related foundation the following PHI without an authorization for the purpose of raising funds for UNT's benefit:

- Demographic information relating to an individual, including- name, address, other contact information, age, gender, and date of birth;
- Dates of health care provided to an individual;
- Department of service information;
- Treating physician;
- Outcome information; and
- Health insurance status

With each fundraising communication made to an individual under this section, UNT must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost. If an individual chooses to opt-out of receiving fundraising communications, UNT must ensure that the individual is not sent such communications.

Each UNT health care component that wishes to use or disclose PHI for fundraising in accordance with this section must include the fundraising statement to this effect in the Privacy Notice (see Section 3(a)).

**t) Personal Representatives, Minors, and Deceased Individuals, 164.502(g)**

A *personal representative* is any person who has the authority act on behalf of a patient or client. A personal representative would include an individual who has authority, by

law or by agreement from the individual receiving treatment, to act in place of the individual. This includes parents, legal guardians, or properly appointed agents (those with Durable Power of Attorney for health care), or individuals designated by state law.

A *minor* is an individual under the age of 18 who has not been legally emancipated by a court, and who is not and has not been married or has not had disabilities of minority removed for general purposes.

As a general rule, minors, incapacitated, and deceased individuals must have a personal representative in order to provide consent or authorization to use and disclose the individual's PHI. UNT must recognize a personal representative who is properly designated as the individual responsible for providing consents and authorizations for any other use or disclosure of PHI.

If a person has authority by law to act on behalf of an individual in making decisions related to the use and disclosure of PHI, UNT will treat this person as a personal representative of the individual. Once a minor is emancipated, a parent or guardian may no longer be recognized as a personal representative.

A minor may consent to the furnishing of medical, health, dental, surgical and psychological care and treatment if the minor:

- Is on active duty with the armed forces of the United States;
- Is 16 years of age or older and resides separate and apart from his parents, managing conservator, or guardian, and regardless of duration of such residency is managing his own financial affairs regardless of the source of income;
- Consents to the diagnosis and treatment of any infectious, contagious, sexually transmitted disease, or communicable disease which is required by law to be reported;
- Is unmarried and pregnant, and consents to hospital, medical, or surgical treatment, other than abortion, related to her pregnancy;
- Consents to examination and treatment for drug or chemical addiction, drug or chemical dependency, or any other condition related to drug or chemical use; or
- Is unmarried and is the parent of the child and consents to medical, dental, psychological, or surgical treatment of that child.

#### Abuse, Neglect, and Endangerment

Unless a state law requires otherwise, UNT need not recognize a person as the personal representative of an individual if UNT reasonably determines that it is not in the best interest of the individual to do so, and also if it reasonably determines or believes that one of the following conditions exist:

- The individual has been or may be subjected to domestic violence, abuse, or neglect by such person.
- Treating the person as a personal representative could endanger the individual.

### Deceased Individuals

PHI generated during the life of an individual is protected from disclosure after death. UNT and its workforce members cannot release PHI regarding a deceased individual unless a personal representative has requested the PHI through the proper authorization process.

If an executor, administrator, or other person has authority under applicable law to act on behalf of a deceased individual or the individual's estate, UNT must recognize this person as a personal representative.

## 5. Patient Rights

### a) Access and Denial of Patient Request for PHI, 164.524

**The Privacy Officer of the health care component that retains the individual's records shall be responsible for processing or denying requests by an individual to that individual's own PHI.**

Individuals have a right to inspect and receive a copy, at their own expense, of the PHI that is in their designated record set, except for the following:

- Psychotherapy notes, which are discussed in Section 4(d). Individuals are entitled to request and receive a summary of psychotherapy notes;
- Information compiled in anticipation of use in a civil, criminal, or administrative action or proceeding;
- PHI subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA) and the disclosure is prohibited by law; and
- PHI exempt from CLIA, pursuant to 42 CFR 493.3(a)(2), which is PHI generated by:
  - Facilities or facility components that perform forensic testing;
  - Research laboratories that test human specimens but that do not report patient-specific results for diagnosis, prevention, treatment, or assessment of the health of patients; and
  - Laboratories certified by the National Institutes on Drug Abuse (NIDA) in which drug testing is performed that meets NIDA guidelines and regulations. However, other testing conducted by a NIDA-certified laboratory is not exempt.



**Each UNT health care component shall develop the procedures, forms and workforce training to enable individuals to request access to and copies of their own PHI. The procedures developed must comply with the following:**

- Individuals have the right to request access to their own PHI as long as the PHI is maintained in the records of the health care component;
- If UNT or one of its health care components does not maintain the requested PHI but knows where the requested information is maintained, then it must inform the individual where to direct the request for access;
- The individual must make the request in writing, using the appropriate form;
- **Based on Texas law, UNT or the health care component must act on the individual's request no later than the 15th calendar day after receipt of the request and payment of any necessary fee.** UNT or the health care component shall:
  - Make the information available, in full or in part, for examination; or
  - Inform the authorized requestor in writing if the information does not exist, cannot be found, or is not yet complete. On completion or location of the information, UNT or the health care component shall notify the individual.
- If access is granted, in whole or in part, UNT or the health care component must comply with the following requirements:
  - UNT or the health care component must provide the individual access to his or her PHI in the designated record set, including inspection or receiving a copy, or both. If the same PHI that is the subject of a request for access is maintained in more than one designated record set or at more than one location, UNT or the health care component need only produce the PHI once in response to a request for access;
  - UNT or the health care component must provide the individual with access to the PHI in the form or format requested by the individual, if it is readily reproducible in such a form or format, or if not, in a readable hard copy or other form or format that is agreed on by both parties. However, if the PHI that is the subject of the request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, UNT or the health care component must provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format, or if not, in a readable electronic form and format as agreed to by UNT and the individual;
  - UNT or the health care component may provide the individual with a summary of the PHI requested, in lieu of providing access to the PHI, or may provide an explanation of the PHI to which access has been provided, if:
    - The individual agrees in advance to such a summary or explanation; and

- The individual agrees in advance to the fees imposed, if any, by UNT or the health care component for a summary or explanation.
- UNT or the health care component must provide access as requested by the individual in a timely manner, including arranging with the individual for a convenient time and place to inspect or receive a copy of the PHI, or by mailing the copy of the PHI at the individual's request. UNT or the health care component may discuss the format, scope, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access;
- If the individual's request for access directs UNT or the health care component to transmit the copy of PHI directly to another person designated by the individual, UNT or the health care component must provide the copy to the person designated by the individual. The individual's request must be in writing, signed and must clearly identify the designated person and where to send the copy of PHI; and
- If the individual requests a copy of the PHI or agrees to a summary or explanation of its information, UNT or the health care component may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:
  - Labor for copying the PHI, whether in paper or electronic form. The fee schedule for these services is set by the State of Texas;
  - Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media; and
  - Preparing an explanation or summary of the PHI, if agreed to by the individual.

*Denial of Access to PHI*

- UNT or the health care component must allow an individual to request access to inspect or receive a copy of PHI maintained in their records. However, UNT or the health care component may deny an individual's request without providing an opportunity for review when:
  - The PHI is excepted from the right of access by 45 CFR 164.524(a)(1) as listed in the first paragraph of this section;
  - The individual agreed to temporary denial of access when consenting to participate in research that includes treatment, and the research is not yet complete;
  - The records are subject to the Privacy Act of 1974, and the denial of access meets the requirements of that law; and
  - The PHI was obtained from someone other than UNT under a promise of confidentiality, and access would likely reveal the source of the information.

- UNT or the health care component may also deny an individual access for the following reasons, provided that the individual is given the right to have such denials reviewed:
  - A licensed UNT health care professional has determined that the access is likely to endanger the life or physical safety of the individual or to another person;
  - The PHI makes reference to another person, who is not a health care professional, and a licensed health care professional has determined that the access requested is likely to cause substantial harm to this other person; or
  - The request for access is made by the individual's personal representative and a licensed health care professional has determined that access is likely to cause substantial harm to the individual or to another person.
- If access is denied on a ground permitted above, the individual has the right to have the denial reviewed by a licensed UNT health care professional, who is designated by the HIPAA Compliance Officer and who did not participate in the original decision to deny, to act as the reviewing official. UNT or the health care component must provide access or deny access in accordance with the determination of the reviewing official;
- If UNT or the health care component denies access, in whole in or part, to PHI, UNT or the health care component must comply with the following:
  - To the extent possible, give the individual access to any other PHI requested, after excluding the PHI to which access was denied;
  - Provide in a timely manner written denial to the individual, in plain language and containing the following information:
    - The reason for the denial;
    - If applicable, a statement of the individual's review rights, including a description of how the patient may exercise such review rights; and
    - A description of how the individual may complain to UNT or to the Department of Health and Human Services pursuant to Section 7(b).
  - If the individual has requested a review of a denial, the UNT HIPAA Compliance Officer must designate a licensed UNT health care professional who was not directly involved in the decision to deny access. UNT must promptly refer a request for review to this licensed health care professional. The licensed health care professional must determine, in a reasonable period of time, whether to provide or to deny access to the requested PHI. The UNT HIPAA Compliance Officer must promptly provide written notice to the individual of the findings of the reviewing health care professional, and must then direct that the appropriate action be taken to provide or deny access, as addressed in this section.

**b) Patient Right to Request Restriction of Uses and Disclosures, 164.522(a)(1)**

UNT health care components must permit an individual to request that the health care components restrict:

- Uses and disclosures of PHI about the individual to carry out TPO;
- Permitted uses and disclosures as outlined elsewhere in this policy.

**Each health care component shall develop the necessary forms and procedures to enable individuals to request restrictions and shall provide workforce members with the training necessary to carry out these procedures.**

UNT health care components are not required to agree to a restriction, except that they **must** agree to the request to restrict disclosure of PHI to a health plan if the disclosure is for the purpose of carrying out payment or health care operations and the PHI pertains solely to a health care item or service for which the individual, or a person other than a health plan on behalf of the individual, has paid out of pocket in full. If a UNT health care component does agree to a restriction, then UNT or the health care component must document the restriction and may not use or disclose PHI in violation of the restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide emergency treatment, UNT or a health care component may use the restricted PHI itself or may disclose the restricted PHI to a health care provider to provide required treatment to the individual. If restricted PHI is disclosed to another health care provider for emergency treatment, UNT or its health care components must request that the health care provider not further use or disclose the PHI.

*Terminating a Restriction*

A UNT health care component may terminate its agreement to a restriction if:

- The individual agrees to or requests the termination in writing;
- The individual orally agrees to the termination and the oral agreement is documented; or
- The UNT health care component informs the individual that it is terminating the restriction, except that such termination is not effective for PHI restricted for items paid out of pocket. The termination is only effective with respect to PHI created or received after the health care component has informed the individual.

**c) Confidential Communications, 164.522 (b)(1)**

UNT health care components must permit individuals to request and must accommodate reasonable requests to receive communications of PHI by alternative means or at alternative locations. UNT health care components:

- May require that individuals make a request for confidential communication in writing;
- May condition the provision of a reasonable accommodation on:
  - Information regarding how any payment will be handled, if appropriate; and
  - Specification of an alternative address or other method of contact.
- May not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

It is the individual's responsibility to change an address back to the original designated address.

**d) Right to Amend One's Own Protected Health Information, 164.526(a)-(f)**

Patients have the right to amend information collected and maintained about them in their designated record set.

All UNT health care components must strictly observe the following standards:

- An individual has the right to have a UNT health care component amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set;
- A UNT health care component may deny an individual's request for amendment, if it determines that the PHI or record that is the subject of the request:
  - Was not created by the UNT health care component, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
  - Is not part of the individual's designated record set;
  - Would not be available for inspection under the Access and Denial of Patient Request for PHI section of this policy (see Section 5(a)); or
  - Is accurate and complete.
- The individual must make the request to amend the PHI in writing to the UNT health care component with a reason to support the requested amendment. **The request shall be on the form developed for this purpose by the health care component.**
- The UNT health care component must accept all requests to amend PHI in the designated record set. However, the health care component is not required to act on the individual's request if one of the conditions for denying the request is found to exist.

- The health care component must act on the individual's request for an amendment no later than 60 days after the receipt of the request. If the health care component is unable to act on the amendment within the required 60 day time limit, it may extend the time for its action by no more than 30 additional days, provided that:
  - The health care component provides the individual with a written statement of the reasons for the delay and the date by which action on the request will be completed, and
  - The health care component may have only one such extension of time for action on a request for an amendment.
- If the amendment is granted, in whole or in part, the UNT health care component must:
  - Make the appropriate amendment to the PHI or record that is the subject of the request for amendment by at least identifying the records that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.
  - Inform the individual in writing in a timely manner that the amendment is accepted and obtain the individual's identification of and agreement to have the health care component notify the relevant persons with which the amendment needs to be shared.
  - Make reasonable efforts to inform and provide the amendment within a reasonable time to:
    - Persons identified by the individual as having received PHI about the individual and needing the amendment, and
    - Persons, including business associates, that the health care component knows have the PHI that is the subject of the amendment and that may have relied, or might reasonably rely, on this information to the detriment of the individual.
- If the requested amendment is denied, in whole or in part, the health care component must provide the individual with a timely, written denial. The denial must use plain language and contain:
  - The basis for the denial, in accordance with the procedures specified in this section.
  - Notice that the individual has a right to submit a written statement disagreeing with the denial and how the individual may file such a statement.
  - A statement that, if the individual does not submit a statement of disagreement, the individual may request that the health care component provide the individual's request for amendment and the denial of the amendment whenever it makes future disclosures of the individual's PHI.
  - A description of how the individual may file a complaint with UNT or to the Department of Health and Human Services pursuant to Section 7(b).
- Additionally, for denials:

- The health care component must permit the individual to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such a disagreement. The health care component may reasonably restrict the length of any statement of disagreement;
- The health care component may prepare a written rebuttal to the individual's statement of disagreement. Whenever a rebuttal is prepared, a copy of the rebuttal must be provided to the individual who submitted the statement of disagreement;
- The health care component must identify, as appropriate, the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the denial of the request, the individual's statement of disagreement, if any, and the rebuttal, if any, to the designated record set;
- In its future disclosures:
  - If a statement of disagreement has been submitted by the individual, the health care component must include the individual's request for an amendment, the denial of the request, the individual's statement of disagreement and the rebuttal, if any, or an accurate statement of any such information, with any subsequent disclosures of the PHI to which the disagreement relates;
  - If the individual has not submitted a written statement of disagreement, the health care component must include the individual's request for amendment and its denial, or an accurate summary of this information, with any subsequent disclosures of the PHI only if the individual has requested such action; or
  - When a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included with the disclosure, the health care component may transmit the material required under separate cover to the recipient of the standard transaction.
- If the health care component is informed by another provider or payer of an amendment they have made to the individual's PHI within the outside entity's records, the UNT health care component must amend the PHI in the designated records that have been received from that outside entity. However, the UNT health care component is not required to amend the PHI in its own records based on the determination of the outside entity, unless the health care component regards the findings of the outside entity reliable.
- Each UNT health care component's Privacy Officer will be responsible for receiving and processing amendment requests.

**e) Accounting for Disclosures and Patient Access to Disclosure Logs,  
164.528(a)-(d), 164.530(i)(1)**

Individuals shall have the right to receive an accounting of disclosures of their PHI made by UNT health care components in the six years prior to the request (or a shorter time period if requested). Disclosures include those to and by business associates.

UNT health care components must account for disclosures of PHI except for the following disclosures:

- To carry out treatment, payment and health care operations;
- To individuals of PHI about them;
- Incidental disclosures;
- For the facility's directory or to persons involved in the individual's care or other notification purposes;
- To correctional institutions or law enforcement custodial officials;
- As part of a limited data set; and
- Pursuant to an authorization.

UNT health care components must provide the individual with a written accounting that meets the following requirements:

- The accounting for each disclosure must include:
  - The date of the disclosure;
  - The name of the entity or person who received the PHI and, if known, the address of this entity or person;
  - A brief description of the PHI disclosed; and
  - A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or in lieu of such a statement, a copy of a written request for a disclosure, if any.
- If a UNT health care component has made multiple disclosures of the PHI to the same person or entity for a single purpose, or resulting from a single authorization, the accounting may provide, for these multiple disclosures:
  - The information required above for the first disclosure during the accounting period;
  - The frequency, periodicity, or number of the disclosures made during the accounting period; and
  - The date of the last such disclosure during the accounting period.
- The health care component must act on the individual's request for an accounting no later than 60 days after receipt of the request, as follows:
  - Provide the individual with the accounting requested, or
  - If unable to provide the accounting within the time required, it may extend the time to provide the accounting by no more than 30 days, provided that:



- The health care component, within the 60 day time limit, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting, and
  - The health care component may have only one such extension of time for action on a request for an accounting.
- The health care component must provide the first accounting to an individual in any 12-month period without charge. The health care component may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the same 12-month period, provided that the health care component informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or to modify the request for a subsequent accounting in order to avoid or to reduce the fee. The fee schedule for these services is set by the State of Texas.

Exceptions to the Right of Accounting of Disclosures

In accounting for disclosures of PHI:

- The UNT health care component must temporarily suspend an individual’s right to receive an accounting of disclosures to a health oversight agency or law enforcement official if this agency or official provides the health care component with a written statement that such an accounting to the individual would reasonably be likely to impede the agency’s activities. The written statement must specify the time for which such a suspension is required.
- If the agency or official suspends an individual’s right to receive an accounting of disclosures and the statement is made orally, the UNT health care component must:
  - Document the statement, including the identity of the agency or official making the statement.
  - Temporarily suspend the individual’s right to an accounting of disclosures subject to the statement.
  - Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement from the suspending agency or official is submitted during this 30-day time period.

Documentation for Accounting of Disclosures

**The workforce members of the UNT health care component are required to account for disclosures of PHI by documenting any such disclosure. Each health care component shall develop the necessary procedures, training of workforce members, and database or filing system that will contain the accounting of disclosures and that will comply with this section.**

**6. Security Safeguards**

**Each UNT health care component must develop and implement administrative procedures and practices, as well as technical and physical safeguards that reasonably protect health information from intentional and unintentional use and disclosure that violates federal or Texas law and regulations.**

**a) Electronic Communication of PHI**

*Fax Transmittal of PHI*

**Each UNT health care component must develop procedures and forms that adhere to the following standards relating to facsimile communications of an individual's medical records, and each workforce member must follow the designated procedures:**

- PHI may only be sent by fax when the original record or mail-delivered copies will not meet the needs for the treatment, payment and health care operations (TPO).
- Information transmitted must be limited to the minimum necessary to meet the requester's needs.
- The following types of medical information are protected by federal and/or state statute and may not be faxed or photocopied without specific written patient authorization, unless required by law:
  - Psychiatric/Psychological records, including the following records:
    - Psychotherapy treatment by a psychiatrist or a licensed psychologist.
    - Other professional services of a licensed psychologist.
  - Social work counseling and therapy.
  - Domestic violence victims' counseling.
  - Sexual assault counseling.
  - HIV test results. An individual's written authorization is required for each separate release request.
  - Records relating to sexually-transmitted disease.
  - Alcohol and drug abuse records protected by federal confidentiality rules (cf. 42 CFR Part 2).
- A designated fax cover page must be used to send faxes containing PHI. All pages plus the cover page must be marked "CONFIDENTIAL" before they are transmitted.
- Workforce members must take reasonable precautions to send the PHI to the correct location, using the correct phone number. If they are uncertain of the fax number, they must first call the location and verify the fax number with a person at the remote location.

### Documentation of Successfully Transmitted Faxes

The UNT health care component sending a fax for TPO purposes may wish to maintain a copy of the fax transmittal or fax confirmation sheet in the individual's record, but it is not required to do so.

The UNT health care component sending a fax for non-TPO purposes, based on an authorization of the individual or based on a request that does not require the consent of the individual, must maintain a copy of the fax transmittal sheet or, if available, the fax confirmation sheet in the individual's record. It must also enter the transmission into the health care component's disclosure accounting database.

### Misdirected Faxes

If a fax is known to have arrived at an incorrect location, the workforce member must obtain the incorrect number from the fax memory and must attempt to contact the party by phone at the remote location to request that the misdirected fax be destroyed in its entirety. If no one is available by phone at the remote location, a form designated by the health care component must be faxed to the incorrect number with a request that the misdirected fax be destroyed in its entirety. The number to which the misdirected fax was sent must be entered into the disclosure accounting database with a notation that the fax was sent erroneously to that location.

### Receipt of Faxes with PHI

Fax machines designated for receiving PHI must not be located in areas accessible to the general public or to workforce members who do not have authorization to access PHI. **The director of the health care component, in conjunction with workforce members responsible for security, shall designate a secure location for fax machines.**

**Incoming fax documents containing PHI must be handled in compliance with this policy and with the health care component's procedures and practices.**

If a fax is received in error, the receiving department shall immediately notify the sending party, and then shall either destroy it in its entirety or shall follow the directions of the sending party.

### Email Transmission of PHI

Electronic mail that is sent, received, or stored on computers that are owned, leased, administered, or otherwise under the custody and control of UNT is the property of UNT and subject to this policy.

### General

- **Email transmission of PHI is only permitted if the email is encrypted.**

- Email containing PHI must be treated with the same degree of privacy and confidentiality as the patient's medical record.
- UNT health care components shall make all email messages sent or received that concern the treatment of an individual part of the individual's record.
- UNT workforce members may not email PHI outside the UNT email network unless specifically authorized by the individual.
- When sending PHI via email UNT workforce members must limit the information transmitted to the minimum necessary to meet the requestor's needs (see Section 4(a)) and must use de-identified PHI (see Section 3(d)) whenever possible.
- All external disclosures of PHI through email must comply with Sections 4(b) and 5(e), which deal with authorizations and accounting of disclosures.

**b) Storage of PHI**

UNT health care components have a duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. All UNT workforce members must strictly observe the following standards for storing PHI:

- Before regular working hours have ended, workforce members must clean desks and working areas so that PHI is properly secured, unless the immediate area can be secured from unauthorized access.
- When not in use, PHI must always be protected from unauthorized access. When left in an unattended room, such information must be appropriately secured.
- If PHI is stored on the hard disk drive or other internal components of a computer workstation, personal computer, or PDA (Personal Digital Assistant), it must be protected by either a password or encryption. Unless encrypted when not in use, computers and their storage units must be secured from unauthorized access.
- If PHI is stored on diskettes, CD-ROMs, ZIP disks, or any other type of removable data storage media, it must be password protected or encrypted and cannot be commingled with other electronic information.
- If backup copies of PHI are moved to a location away from campus to ensure redundancy and integrity of data, the remote location must be secure and the person transporting the copies must have security clearance and documented HIPAA training.
- When PHI is being released through teleconference or video feed, UNT workforce members must treat the protection of the PHI in the same manner as PHI recorded on paper, thereby securing access to the teleconference or video to authorized personnel only. Support staff for the teleconference or video feed must have documented training regarding HIPAA compliance procedures if they will have contact with PHI during the teleconference or video feed.

- PHI stored in medical equipment (EKG, etc.) must be kept secure and disposed of in compliance with this policy.

**Each UNT health care component shall develop the procedures and workforce training necessary to ensure the integrity and confidentiality of stored PHI.**

**c) Printing and Copying of PHI**

All UNT workforce members must strictly observe the following standards relating to the printing and copying of PHI:

- PHI in hardcopy format must be disposed of in accordance with this policy and with records retention schedules.
- Printed versions of PHI should not be copied indiscriminately or left unattended and open to compromise.
- Printers and copiers used for printing and copying PHI should be in a secure, non-public location. If the equipment is in a public location, the information being printed or copied is required to be strictly monitored.
- PHI shall not be downloaded onto personally owned mobile devices, including mobile storage devices (e.g., CD, DVD, flash drive, external hard drive).
- PHI should never be stored on social networking websites or transmitted through peer-to-peer applications.
- Defective copies or printouts of PHI must be secured and immediately disposed of, in compliance with this policy.
- Access controls must be enforced to ensure that workforce members who transport and dispose of PHI have appropriate security clearance and training; and
- PHI printed to a shared printer shall be promptly removed from the printer and secured.

**d) Disposal of PHI**

All UNT workforce members must strictly observe the following standards for disposal of hardcopy and electronic copies of PHI:

- PHI must not be discarded in trash bins, recycle bins (including those with locks), or other locations accessible to the public.
- PHI must be personally shredded or disposed of in any reasonable way that renders documents unreadable.
- Printed material and electronic data containing PHI shall be disposed of in a manner that ensures confidentiality.
- Each individual handling PHI is responsible for ensuring that documents containing PHI are either secured or destroyed. Supervisors are likewise

responsible for ensuring that their employees and volunteers adhere to this policy.

#### *Destruction of Convenience Copies*

- UNT health care component Heads and Directors shall provide workforce members in their health care component with access to shredders for proper disposal of confidential printouts containing PHI.

#### *Electronic Copies*

- Secure methods shall be used to dispose of electronic data and output. Acceptable methods are determined by ITSS to be compliant with Texas law and Department of Information Resources and General Services Commission Regulations.

#### *Destruction of Originals*

- Original documents shall be retained in accordance with records retention schedules, and then shall be destroyed in compliance with this policy.
  - PHI printed material shall be shredded by a workforce member authorized to handle and personally shred the PHI.
  - Microfilm or microfiche must be cut into pieces or chemically destroyed.
- If hardcopy PHI cannot be shredded, it must be incinerated, using a business associate that specializes in the disposal of confidential records.

#### *Documentation of Destruction*

- To ensure that PHI is in fact destroyed and disposed of properly, UNT workforce members or a bonded business associate specializing in this service must carry out the destruction of PHI.
- If UNT workforce members destroy the records, the UNT workforce member must use the records destruction form provided by their health care component or unit to record the date and method of destruction, and a description of the records being destroyed.
- If a bonded business associate destroys the PHI, the bonded business associate must provide the UNT health care component Privacy Officer with a document of destruction that contains the following information:
  - Date of destruction.
  - Method of destruction.
  - Description of the disposed records.
  - Inclusive dates covered.
  - A statement that the records have been destroyed in the normal course of doing business.

- The signatures of the individuals supervising and witnessing the destruction.
- The UNT health care component shall retain destruction documents permanently.

## **7. Administrative Requirements**

### **a) Mitigation of Harmful Effects from Unauthorized Use, 164.530(f)**

To the extent practicable, UNT will mitigate any harmful effect that becomes known to UNT as a consequence of the use or disclosure of PHI that violates federal or Texas laws, or the policies or procedures of UNT or of its health care components.

Mitigation may include, but is not limited to the following:

- Taking corrective measures to remedy the effect of the violation.
- Retraining workforce members responsible for the violation.
- Disciplining workforce members responsible for the violation, following the procedures specified in this policy and in the appropriate sections of the UNT Policy Manual.
- Revising UNT policies or procedure to prevent a recurrence of the violation.
- Addressing problems with business associates, once UNT has been made aware of the problems.

### **b) Reporting Violations of HIPAA, 164.530(d), (h)**

Any individual who believes UNT or any of its health care components has violated HIPAA or any other state or federal laws dealing with privacy and confidentiality may file a complaint regarding the alleged violation. Individuals should file their complaint with the Secretary of the Department of Health and Human Services, with the Privacy Officer of the health care component, or with the UNT HIPAA Compliance Officer.

Each health care component shall develop and implement a set of procedures that enable individuals to file a complaint. These procedures shall specify to whom a complaint shall be delivered and how it will be investigated. If the complainant wishes to make an anonymous complaint, and if the health care component has no provision to accept such a complaint, the complaint can be filed through the anonymous reporting hotline system on the UNT Office of Institutional Compliance website at [compliance.unt.edu](http://compliance.unt.edu). Each health care component must document all complaints received, and their disposition, if any.

Individuals may not be asked or expected to waive their right to file a complaint as a condition of receiving treatment by the health care component.

**c) Sanctions for Breaches, 164.530(e)**

**Each health care component must develop and implement a policy for disciplinary action in the event that a member of the workforce uses or discloses PHI in a manner that violates federal or Texas law or regulations, or UNT policies.**

**Disciplinary Action.** Failure to comply with this policy may be grounds for disciplinary action, including termination of employment. The appropriate level of disciplinary action will be determined on a case by case basis, taking into consideration the specific circumstances and severity of the violation. In cases where disciplinary action is imposed (except for termination), the workforce member shall be required to repeat confidentiality training.

The procedures for disciplinary action will be consistent with UNT Policy 05.033. UNT health care components must document the sanctions that are applied, if any.

**d) Prohibition of Retaliation, 164.530(g)**

UNT shall not intimidate, threaten, coerce, discriminate against, or retaliate against any patient, legally authorized representative, workforce member, association, organization or group that in good faith:

- Discloses or expresses the intention to disclose suspected violations of federal or Texas laws or regulations, or of this policy.
- Provides information to or testifies against the alleged offender or UNT.
- Objects to or refuses to participate in activities that they believe might violate federal or Texas laws or regulations, or this policy.
- Participates in a compliance review, audit, or peer review of health care services.
- Files a legitimate report, complaint, or incident report.

Workforce members who are alleged and found to have filed a malicious complaint may be subject to disciplinary action.

The UNT HIPAA Compliance Officer will review any allegation of retaliation and will ensure that a proper investigation is conducted.

**References and Cross-references:**

UNT Policy 13.004 Use of Human Subjects in Research

Approved: 4/21/2003

Effective: 9/25/2013

Revised: 9/25/2013