I. 11.1.6 Confidentiality of Patient Health Information

Chapter 11 - Patient Privacy	Original Effective Date: April 2003
Section: 11.1 General and Oversight Policies	Date Last Reviewed: January 2023
Responsible Entity: Chief Compliance and Privacy Officer	Date Last Revised: January 2023

II. Purpose

UT Health San Antonio strives to maintain the highest level of confidentiality of all patient health information. All patient information is strictly confidential and can be shared only with those who have a "need to access patient information to perform their job" according to their job duties and responsibilities.

III. Scope

This policy applies to all faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other individual (collectively, Workforce Member, including employees and non-employees) who has direct or indirect access to patient protected health information (PHI) created, held, or maintained by any UT Health San Antonio controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

If a workforce member is working at an affiliated organization, that organization's privacy regulations may also apply.

IV. Policy

A. Education and Training

1. UT Health San Antonio requires all new workforce members to complete training on expectations regarding confidentiality and privacy of health information within thirty (30) days of their official hire date.
2. Workforce members are also provided a link to the Code of Ethics and Standards of Conduct which describes UT Health San Antonio's stance on confidentiality and disciplinary measures for non-compliance.
3. Each workforce member who will be exposed to PHI during their tenure at UT Health San Antonio is required to sign a Confidentiality/Security Acknowledgement.

4. Non-employees exposed to PHI as a part of their responsibilities will also be required to attend training. See Institutional Handbook of Operating Policies (IHOP) policy 4.3.8 Non-Employee Service for the definition of a non-employee.

B. Non-Affiliated Reviewers and Visitors

Individuals not affiliated with UT Health San Antonio who are exposed to health information must complete a Confidentiality/Security Acknowledgement.

C. Data Collection

1. The types and amounts of information gathered and recorded about a patient are limited to information needed to provide and facilitate patient care. Supplementary data, which is not required for patient care, but is desirable for education, etc., may be recorded for which the information is requested.
2. The collection of any data relative to a patient, whether by interview, observation, or review of documents, is to be conducted in a setting which provides maximum privacy and protects the information from unauthorized individuals.
3. No information contained in the patient's record will be given, transferred, or in a way relayed to any person or entity not involved in treatment, payment, or healthcare operations or without the patient's authorization. Policies addressing exceptions for allowable disclosure of patient healthcare information without the patient's authorization are outlined in IHOP policy 11.2.1 Use and Disclosure of Protected Health Information Without Authorization.

D. Access

1. Access to confidential information is limited to workforce members with a legitimate need to access patient health information to perform their job within UT Health San Antonio.
2. Areas in which confidential information is stored and/or exchanged verbally are limited to authorized workforce members.
3. Information about the patient which may or may not be recorded in the patient's record should be treated with the same level of confidentiality as the health record. Such discussions should be conducted only in areas where unauthorized individual will not overhear.
4. Workforce members whose positions and duties do not require them to view patient information are restricted from seeking access to these records, whether paper or electronic. See IHOP policy 11.1.5 Patient Health Records for additional guidance.
5. Designated workforce members are responsible for responding to requests for uses and disclosures of health information according to federal and state law and UT Health San Antonio policy. See IHOP Section 11.2 Uses and Disclosures of Protected Health Information.
6. For incidental disclosures, see IHOP policy 11.2.4 Uses and Disclosures of Protected Health Information for Treatment, Payment and Health Care Operations.

E. Security, Safeguards, and Storage

1. All health records, including the legal medical record, components of the designated record set, and any existing case management (shadow) files, should be stored in physically secured areas. See IHOP policy 11.1.5 Patient Health Records.
2. UT Health San Antonio ensures that appropriate administrative, technical, and physical safeguards are in place to protect the privacy of PHI from intentional or unintentional unauthorized use or disclosure.

F. Research

1. All research protocols are reviewed and approved by UT Health San Antonio's Institutional Review Board (IRB) and address confidentiality of individuals involved in a research study and the health information of such individuals. UT Health San Antonio workforce members involved in research activities must strictly adhere to such confidentiality requirements. Health information used in research studies is held to the same level of confidentiality and privacy as all health information used, disclosed, or stored within UT Health San Antonio systems.
2. See IHOP policy 11.2.12 Uses and Disclosures of Protected Information for Research for guidance.

G. De-identification of Protected Health Information

When de-identifying PHI, such as for research studies, only authorized individuals have access to code lists or any device that links de-identified information to specific individuals or patients. When de-identifying PHI, IHOP policy 11.2.9 De- identification of Protected Health Information should be followed unless otherwise directed by the IRB. Caution also must be taken when re-identifying protected health information, using methods approved by IRB protocol.

H. Telephones

1. All workforce members are accountable for using caution in discussing confidential patient information over the telephone. Information may be released for treatment, payment, and healthcare operations, if the workforce member disclosing the information is certain of the identity of the person and/or entity to which they are releasing the information and the purpose of the release.
2. If the workforce member is uncertain as to the identity of the person to who they are speaking, the workforce member should terminate the call and return the call with the requested information and/or confer with a supervisor.
3. The workforce member may release confidential information over the telephone in an emergency situation; however, they should take every precaution to ensure appropriate disclosure.

V. Definitions

Terms used in this document have the meaning set forth in the Patient Privacy Policies Glossary unless a different meaning is required by context.

VI. Related References

For questions regarding this policy, contact the Privacy Program Director at 210-567-2014 or email compliance@uthscsa.edu.

Health Insurance Portability and Accountability Act (HIPAA) of 1996
HIPAA Privacy Rule, 45 CFR Part 160 and Subparts A and E of Part 164
HIPAA Security Rule, 45 CFR Part 160 and Subparts A and C of Part 1644

VII. Review and Approval History

The approving authority of this policy is the University Executive Committee.

Effective Date	Action Taken	Approved By	Approved Date
04/2003	Policy Origination		
04/2010	Policy Revision		
03/2013	Policy Revision		
01/2023	Policy Review	ICPO	01/05/2023