Chapter 11	Patient Privacy Policies	Effective:	April 2003
Section 11.1	General Oversight Policies	Revised:	July 2017
Policy 11.1.6	**Confidentiality of Patient Health Information**	Responsibility:	Chief Compliance Officer for Regulatory Affairs & Compliance

CONFIDENTIALITY OF PATIENT HEALTH INFORMATION

Policy

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 know" according to their job duties and responsibilities.

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

Definitions

CONFIDENTIAL PATIENT HEALTH INFORMATION: Verbal, written, pictorial images, or electronic information that includes information generated by UT Health San Antonio or information received from other health care providers, that identifies the individual patient, includes medical, diagnostic, treatment, and prognosis information on the patient, including data related to research studies.

Education and Training

UT Health San Antonio requires all new employees, faculty, students, or residents to take an on-line course regarding UT Health San Antonio's expectations regarding confidentiality and privacy of health information within thirty (30) days of employment, and they will be provided this link to the "Institutional Compliance Program and Standards of Conduct" which describes UT Health San Antonio's stance on confidentiality and on disciplinary measures for non-compliance. Each new employee, faculty, student, or resident who will be exposed to patient health information during his/her tenure at UT Health San Antonio is required to sign a Confidentiality/Security Acknowledgement statement. Non-employees exposed to protected health information as part of their responsibilities will also be required to attend training. See Section 4.3.8 of the *Handbook of Operating Procedures* (HOP), "Non-Employee Service" for the definition of non-employees.

Non-Affiliated Reviewers & Visitors

Individuals non-affiliated with the institution and are exposed to health information, must complete a Confidentiality/Security Acknowledgement statement.

Chapter 11	Patient Privacy Policies	Effective:	April 2003
Section 11.1	General Oversight Policies	Revised:	July 2017
Policy 11.1.6	**Confidentiality of Patient Health Information**	Responsibility:	Chief Compliance Officer for Regulatory Affairs & Compliance

Data Collection

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 with the permission of the patient, following an explanation of the purpose for which the information is requested.

The collection of any data relative to a patient, whether by interview, observation, or review of documents, is conducted in a setting which provides maximum privacy and protects the information from unauthorized individuals.

No information contained in the patient's record will be given, transferred, or in any 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 located in Section 11.2.1 of the HOP, "Use and Disclosure of Protected Health Information Without Authorization".

Access

Access to confidential information is limited to persons with a legitimate "need to know" to perform their jobs within UT Health San Antonio. Areas in which confidential information is stored and/or exchanged verbally are limited to authorized staff. 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 individuals will not overhear. Employees, faculty, students, and residents 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 "Patient Health Records" in Section 11.1.5 of the HOP.

Designated staff are responsible for responding to requests for uses and disclosures of health information according to federal and state law and UT Health San Antonio policies. See Section 11.2 "Uses and Disclosures of Protected Health Information" of the HOP.

For incidental disclosures, see Section 11.2.4 of the HOP, "For Treatment, Payment, and Healthcare Operations".

Security, Safeguards, and Storage

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 "Patient Health Records" in Section 11.1.5 of the HOP.

UT Health San Antonio ensures that appropriate administrative, technical, and physical safeguards are in place to protect the privacy of protected health information from intentional or unintentional unauthorized use or disclosure.

Research

All research protocols are reviewed and approved by UT Health San Antonio's Institutional Review Board (IRB) and address confidentiality of individuals involved in the research study and the health information of such individuals. UT Health San Antonio employees, faculty, students, or residents 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.

De-identification of Protected Health Information

When de-identifying protected health information, 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 protected health information, the policy of "De-identification of Protected Health Information" in Section 11.2.9 of the HOP 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.

Telephones

All employees are accountable for using extreme caution in discussing confidential patient information over the telephone. Information may be released for treatment, payment, and healthcare operations, if the

employee disclosing the information is certain of the identity of the person and/or entity to which he/she is releasing the information and the purpose of the release. If the employee is uncertain as to the identity of the person to whom he/she is speaking, the employee should terminate the call and return the call with the requested information and/or confer with a supervisor. The employee may release confidential information over the telephone in an emergency situation; however, he/she should take every precaution to ensure appropriate disclosure.