

UT Health Science Center: H110 - Confidentiality of Protected Health Information	
Version 2	Publication Date: 07/17/2024

Responsible Office: Institutional Compliance Office	Last Review: 07/17/2024 Next Review: 07/17/2027
Contact: Melanie Burlison, Privacy Officer	Phone: 901.448.8030 Email: institutional.compliance@uthsc.edu
Related Policies: FI0160 - HIPAA Re-designation and General Policy	

Objective

To establish guidelines and provide guidance to UTHSC workforce members by setting forth the basic requirements for protecting the confidentiality of medical information as required by the Privacy Rule.

Scope

The federal Health Insurance Portability and Accountability Act of 1996 established through its Administrative Simplification regulations to assure privacy for individuals receiving health care services in the United States. The Privacy Rule, as it may also be called, establishes a national standard for the minimum level of protection for medical information. The intent of the statute and the regulatory rule is to expand consumer control over their medical information.

The Privacy Rule introduces the term "Protected Health Information", or "PHI". PHI covers information relating to an individual's health, the care received and/or payment for services, including demographic data. It includes all information in any media related to the individual's health care that can be individually identified as belonging to a particular person.

The basic tenet of the Privacy Rule is that providers may use and disclose PHI without the individual's authorization only for treatment, payment, and health care operations, as well as certain public interest related purposes such as public health reporting. Other uses and disclosures of PHI generally require the written authorization of the individual.

The Privacy Rule also introduces the concept of "minimum necessary". This requirement mandates that when using or disclosing PHI, or when requesting PHI from external providers or entities, providers will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose. The Privacy Rule does recognize that providers may need to use all an individual's health information in the provision of patient care. However, access to PHI by the workforce must be limited based on job scope and the need for the information.

UTHSC 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.

Definitions

- Confidential Patient Health Information - verbal, written, pictorial images, or electronic information that includes information generated by UTHSC or information received from other

UT Health Science Center:	
H110 - Confidentiality of Protected Health Information	
Version 2	Publication Date: 07/17/2024

health care providers, that identifies the individual patient, includes medical, diagnostic, treatment, and prognosis information on the patient, including data related to research studies.

- Workforce Members - include all UTHSC employees, faculty, staff, students, residents, and volunteers.

Procedure

I. 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.

II. Access

Access to confidential information is limited to persons with a legitimate "need to know" to perform their jobs within UTHSC. 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. Faculty, staff, 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. Designated staff are responsible for responding to requests for uses and disclosures of health information according to federal and state law and UTHSC procedures.

III. Security, Safeguards, And Storage

All health records, including the legal medical record, components of the designated record set, should be stored in physically secured areas. UTHSC 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.

IV. De-Identification of Protected Health Information

When de-identifying protected health information, only authorized individuals have access to code lists or any device that links de-identified information to specific individuals or patients.

UT Health Science Center: H110 - Confidentiality of Protected Health Information	
Version 2	Publication Date: 07/17/2024

V. Telephones

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