I. 11.1.16 Electronic Health Record Access Monitoring Program

Chapter 11 - Patient Privacy	Original Effective Date: December 2022
Section: 11.1 General and Oversight Policies	Date Last Reviewed: August 2026
Responsible Entity: Chief Compliance and Privacy Officer	Date Last Revised: August 2026

II. Purpose

UT Health San Antonio (UTHSA) is responsible for ensuring that users with authorized access to UTHSA's electronic systems containing protected health information access only the information necessary to perform their job duties. UTHSA reserves the right to monitor and audit access to any electronic system, application, database, electronic health record system and any other UTHSA system or application containing electronic protected health information. This policy establishes the appropriate use, behaviors and expectations for accessing electronic protected health information in any UTHSA electronic system.

III. Scope

This policy applies to all Workforce Members—including faculty, staff, students, healthcare providers, contractors, and researchers—who have direct or indirect access to Protected Health Information (PHI). This includes all PHI maintained by UTHSA and its controlled affiliates, such as clinics, hospitals, and research facilities.

IV. Policy

A. Protecting Electronic Patient Information

Protecting the privacy of patient information is an important consideration for everyone who utilizes UTHSA's electronic systems that contain patient information. UTHSA has a legal and ethical obligation to ensure the confidentiality and security of patient information and individuals granted access to patient information are personally responsible for ensuring that the privacy of our patients is always protected.

B. Individual Responsibilities to Protect Patient Privacy When Accessing Patient Information in Electronic Systems

1. The electronic health record is the property of UTHSA. The information contained within the record, including all forms of electronic patient information, is the property of the patient and cannot be released to unauthorized individuals without

the written consent of the patient, a subpoena, court order or pursuant to state or federal law.

2. Only authorized users with a legitimate business reason (also known as "Need to Know" access) should access the patient health records. Authorized users should access the minimum amount of PHI necessary to complete assigned job responsibilities.
3. Workforce Members who have been granted access to systems containing patient information shall accept personal responsibility for all activities undertaken using their assigned usernames and passwords or devices. Workforce members shall be responsible for any misuse or unauthorized disclosure of confidential patient information made using their assigned usernames and passwords and for the failure to safeguard their assigned usernames and passwords or devices.

C. Right to Perform Access Monitoring and Audits of Electronic Systems

1. UTHSA recognizes that monitoring and auditing is an essential function of safeguarding confidential patient information from inappropriate access or use.
2. Through the use of system tools and technical functionality, UTHSA has the right, without prior notice, to conduct audits of any electronic system, including the electronic health record (EHR), database, file folder or application to ensure that any access to patient information was performed in accordance with the appropriate "Need to Know" access.
3. The Institutional Compliance and Privacy Office shall be responsible for performing access monitoring and audits of electronic systems containing patient health records.

D. Sanctions for Violations

Individuals who have been determined to have accessed patient information without legitimate business reason shall be subject to disciplinary action in accordance with the *Institutional Handbook of Operating Policies* (IHOP) policy 11.1.17 Sanctions for Privacy and Security Violations.

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 compliance@uthscsa.edu.

Code of Federal Regulations (CFR)
45 CFR Part 164 Security and Privacy, Subsection 514: *Other requirements related to uses and disclosures of protected health information, items* (h)(a).

Institutional Handbook of Operating Policies (IHOP)

11.1.0 Privacy Compliance Program
11.1.17 Sanctions for Privacy and Security Violations

VII. Review and Approval History

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

Effective Date	Action Taken	Approved By	Approved Date
12/2022	Policy Origination	Executive Committee	12/2022
08/2026	Policy Review/Discretionary Edits	ICPO	08/24/2026