11.1.16 Electronic Medical Record Access Monitoring Program

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

I. Purpose

It is the responsibility of UT Health San Antonio (UTHSA) to ensure that users who have authorized access to UTHSA's electronic systems containing patient medical information access only the patient medical information necessary to perform their job functions. UTHSA shall have the right to audit accesses into any electronic system, application, database, electronic health record system and any other UTHSA system or application containing patient medical records in electronic format. This policy outlines appropriate behaviors and expectations for access to electronic patient information contained in any UTHSA electronic system.

II. 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 UT Health San Antonio or controlled affiliate.

III. Policy

A. Protecting Electronic Patient Information

Protecting the privacy of patient information is an important consideration for everyone who utilizes UT Health San Antonio's electronic systems that contain patient information. UT Health San Antonio 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 medical record is the property of UT Health San Antonio. 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 records. Authorized users should access the minimum amount of PHI necessary to complete assigned job responsibilities.
3. UTHSA 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 Audits of Electronic Systems

1. UT Health San Antonio recognizes that auditing is an essential function of safeguarding confidential patient data from inappropriate access or use.
2. Through the use of system tools and technical functionality, UT Health San Antonio 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 of 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 audits of electronic systems containing patient medical information.

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 *Institutional Handbook of Operating Policies* (IHOP) policy 11.1.17 Sanctions for Privacy and Security Violations.

IV. 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.*

V. 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

VI. Review and Approval History

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

B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By	Date Approved
12/2022	Policy Origination	Executive Committee	12/2022