I. 11.1.0 Privacy Compliance 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

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Title XIII, Subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH), hereafter collectively referred to as HIPAA, and associated regulations (see Code of Federal Regulations (CFR) 45 Parts 160, 162, and 164) were enacted in part to establish rights for patients and responsibilities for Covered Entities and Business Associates of Covered Entities with regard to the confidentiality, availability, and integrity of Protected Health Information (PHI). UT Health San Antonio (UTHSA) meets the definition of a "Covered Entity", as defined by 45 CFR §160.103.

The purpose of this policy is to:

1. Establish UTHSA's commitment to maintaining a broad operational framework for the Privacy Compliance Program in accordance with the Privacy, Security, and Breach Notification Rules found in HIPAA; and
2. Ensure all Workforce Members understand their rights and obligations with regard to the privacy, security, and integrity of Protected Health Information (PHI).

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. Privacy Compliance Program

1. Privacy Compliance Program Oversight

    a. The Institutional Compliance and Privacy Office (ICPO) leads the UT Health San Antonio Privacy Compliance Program and is responsible for implementing

this Policy and overseeing UTHSA's compliance with applicable federal and state privacy laws and regulations, including HIPAA, HITECH, and other applicable privacy requirements. The ICPO develops, implements, and periodically reviews privacy policies; provides privacy education and guidance to the workforce; monitors compliance through audits, risk assessments, and other oversight activities; investigates reports of suspected privacy violations; coordinates breach risk assessments and required notifications; and implements corrective actions to mitigate risk and prevent recurrence.

b. The ICPO also oversees privacy compliance for research involving PHI by providing guidance on applicable HIPAA research requirements in collaboration with the Institutional Review Board (IRB), Research Administration, and other institutional stakeholders.

c. The ICPO supports institutional governance of artificial intelligence (AI) and other emerging technologies by advising on the appropriate use of PHI and sensitive data, evaluating privacy risks, and collaborating with institutional governance bodies to ensure compliance with applicable privacy laws, regulations, and UTHSA policies.

d. The ICPO shall oversee the implementation and maintenance of appropriate administrative, technical, and physical safeguards to protect PHI from unauthorized use or disclosure and, in collaboration with Information Security and other institutional stakeholders, monitor the effectiveness of those safeguards and recommend improvements to address evolving privacy, research, and technology-related risks.

2. Reporting Privacy Violations

a. If any UTHSA Workforce Member becomes aware of an actual or alleged violation of HIPAA requirements or this Policy, including but not limited to a privacy incident or unauthorized access, use, or disclosure of PHI, the individual is required to report the actual or alleged violation to the ICPO.

b. The ICPO will provide information on its website to enable the reporting of actual or alleged violations and will develop procedures to ensure the prompt and timely response to reports received.

c. UTHSA will take appropriate steps to mitigate, as required by applicable law, any violation of this Policy or applicable HIPAA requirements.

d. UTHSA Workforce Members found to have violated this Policy may be subject to disciplinary action, up to and including termination, in accordance with *Institutional Handbook of Operating Policies (IHOP)* policy 11.1.17 Sanctions for Privacy and Security Violations. Students in violation of this policy may be subject to additional disciplinary action under the applicable student policies and procedures.

3. Privacy Violation Investigations

a. The ICPO will promptly investigate any reported privacy incident or potential violation of this policy and recommend appropriate corrective actions if a breach has occurred. The ICPO may involve the Information Security Office, Legal

Affairs Office, Human Resources or other UTHSA units as appropriate. Any UTHSA unit that becomes aware of a potential HIPAA or Policy violation must promptly notify the ICPO.

b. As part of its investigation of any potential privacy incident or policy violation, the ICPO has the authority to access UTHSA email accounts, document storage service, and transmission services without the permission of the account or service owner when there is a reasonable basis to suspect the email account or service was involved in the incident.

c. Investigations may include interviews of complainant, patients or staff, review of work schedules, auditing electronic information systems, medical information reviews, and other related processes or documents.

d. All UTHSA Workforce Members must cooperate with investigations and promptly respond to inquiries from the ICPO and any units assisting or coordinating the investigation. Failure to cooperate in an investigation concerning a privacy breach, or a violation of this policy, may result in disciplinary action in accordance with applicable policies.

e. Nothing in this Policy limits the applicability of UTHSA policies governing the investigation of cyber-security incidents.

4. Monitoring Program

The ICPO will define and implement a process to routinely monitor compliance with UTHSA privacy policies and procedures, the HIPAA Privacy Standards, and HITECH that includes the following minimum requirements:

a. The performance of privacy rounds (e.g., walking throughout UTHSA facilities and interviewing Workforce Members to identify potential areas of noncompliance);

b. Auditing Workforce Member privacy training completion;

c. Audit appropriate access to systems containing PHI in accordance with IHOP policy 11.1.16 Electronic Access Monitoring Surveillance; and

d. Report all monitoring findings to the Compliance and Ethics Committee.

5. Prior Notification of Intent to Conduct HIPAA Standard Transactions or Engage in HIPAA Covered Activity

a. All UTHSA Workforce Members must notify the ICPO of their intent to engage in HIPAA Standard Transactions or to send, receive, and/or maintain PHI in connection with the provision of health care services (see *45 CFR §160.103*).

b. Notification must be as soon as possible prior to proposed initiation of such transmissions or activity, but no later than ninety (90) days prior to the planned date of implementation to enable the ICPO to conduct an analysis and recommend appropriate HIPAA compliance measures.

6. Student Health Information

a. Student health information obtained or created as part of the student's academic career is normally covered under the privacy provisions of the Family

Educational Rights and Privacy Act (FERPA). See Institutional Handbook of Operating Procedures (IHOP) policy 2.2.3 Family Educational Rights and Privacy

b. This Policy in no way affects the applicability of FERPA regulations to student records, including student health records created as a result of health care services provided by UTHSA clinical programs for students.

7. Substance Use Disorder Patient Information

a. Workforce members working in a substance use disorder program shall comply with all applicable provisions of 42 CFR Part 2.

i. 42 CFR Part 2 defines a "program" as:

(1) An individual or organization that provides substance use disorder (SUD) diagnosis, treatment, or referral for treatment, and
(2) Receives federal assistance (such as Medicare/Medicaid funding, grants, or federal support of any kind)

b. In instances where 42 CFR Part 2 establishes requirements that differ from HIPAA, including but not limited to authorization standards or conditions governing access, use, or disclosure, workforce members shall comply with 42 CFR Part 2. Information may only be used or disclosed as permitted under 42 CFR Part 2 and applicable institutional policies.

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.

Health Insurance Portability and Accountability Act (HIPAA)

Code of Federal Regulations Title 45, Part 160 and subparts A and E of Part 164

Institutional Handbook of Operating Policies (IHOP)
IHOP 11.1.17 Sanctions for Privacy and Security Violations
IHOP 11.1.16 Electronic Access Monitoring Surveillance

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 Revision	Executive Committee	08/2026