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:
Responsible Entity: Chief Compliance and Privacy Officer	Date Last Revised:

I. 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 UTHSA Workforce Members understand their rights and obligations with regard to the privacy, security, and integrity of Protected Health Information (PHI).

II. Scope

This policy applies to all UT Health San Antonio faculty, staff, residents, students, researchers, contractors, volunteers, or any other individual who has direct or indirect access to PHI (collectively, Workforce Members) created, held, or maintained by UTHSA or controlled affiliates.

III. Policy

A. Privacy Compliance Program

1. Privacy Compliance Program Oversight

   a. The Institutional Compliance and Privacy Office (ICPO) leads the Privacy Compliance Program for UTHSA. The ICPO is charged with implementing this Policy and overseeing UTHSA's HIPAA Privacy Compliance Program, which includes developing standard procedures, preparing, and disseminating information and training materials, monitoring, and auditing, and responding to reports of suspected noncompliance with this Policy or with HIPAA requirements in order to prevent future similar offenses.

   b. The ICPO will ensure appropriate administrative, technical, and physical safeguards are implemented and adhered to in order to protect PHI from any intentional or unintentional use or disclosure that is in violation of UTHSA privacy policies, the HIPAA Privacy Rule, or HITECH.

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 potential privacy or security incident, or violation of this policy, of which they are notified and will recommend appropriate corrective actions in the event that a breach has occurred. The ICPO may involve the UTHSA Information Security Office, Legal Affairs Office, Human Resources or other UTHSA units as appropriate. In the event any other UTHSA unit receives notification of a potential HIPAA violation or violation of this policy, the unit will promptly notify the ICPO.

b. As part of its investigation of any potential privacy or security incident, or violation of this policy, the ICPO has the authority to access UTHSA email accounts, document storage service, or transmission service 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 will cooperate in such investigations and promptly respond to inquiries from the ICPO and to any other such requests from units assisting with or coordinating the investigation. Failure to cooperate with an investigation concerning a privacy or security breach, or a violation of this policy, may result in disciplinary action by UTHSA, in accordance with applicable policies.

e. Nothing in this Policy precludes the applicability of UTHSA policies that relate to 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).

    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. UTHSA Workforce Members must comply with any applicable standards under *42 CFR Part 2* and the *Standards for Confidentiality of Substance Use Disorder Patient Records* policy.

    b. If PHI involves Patient Identifying Information (as defined in the *Standards of Confidentiality of Substance Use Disorder Patient Records* policy), Workforce Members are directed to consult the *Standards of Confidentiality of Substance Use Disorder Patient Records* policy and must comply with that policy.

    c. If the *Standards of Confidentiality of Substance Use Disorder Patient Records* policy establishes different standards from those under other HIPAA privacy policies relating to individuals who may sign an authorization, or other standards for access, uses or disclosures, where applicable, the facility should not use or disclose information except where permitted by both the *Standards for Confidentiality of Substance Use Disorder Patient Records* policy, and other applicable policies.

B. Policy Review

The Policy will be reviewed periodically by the Institutional Compliance and Privacy Office to ensure compliance with applicable laws and standards. The content of this policy will be modified as necessary or appropriate.

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.

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

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