I. 11.1.2 Complaints Regarding Privacy and Confidentiality of Protected Health Information

Chapter 11 - Patient Privacy	Original Effective Date: April 2003
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

Any individual who believes their rights under federal privacy and security regulations, or other applicable state or federal laws governing the privacy, security and confidentiality of protected health information have been violated may file a complaint regarding the alleged violation. Formal complaints must be submitted to UT Health San Antonio's (UTHSA) Chief Compliance and Privacy Officer in the Institutional Compliance and Privacy Office (ICPO).

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. Filing Complaints

1. Any privacy or security related complaint made by patients or workforce members must be reported to the chief compliance and privacy officer.
2. Complaints may be reported anonymously through several methods:
    a. Call the Compliance Hotline (1-877-507-7317);
    b. Complete the online internal Report Form for workforce members; or
    c. Complete the online external Report Form for non-workforce members.

B. Investigation of Complaints

1. The Chief Compliance and Privacy Officer is responsible for investigating all complaints made by patients regarding alleged breaches of their privacy.

2. If a complaint is made by a patient regarding a UTHSA workforce member working at an affiliated organization, UTHSA's Chief Compliance and Privacy Officer will work with that organization's Privacy Officer.
3. The Chief Compliance and Privacy Officer will request assistance from the Chief Information Security Officer with investigations of any information technology or other electronic system to determine if a breach of security has occurred.
4. After an investigation, workforce members who are found to have knowingly violated the privacy and confidentiality of PHI will be subject to disciplinary action, up to and including termination. A description of privacy violation sanctions to be taken based on level of severity is outlined in IHOP policy 11.1.17 Sanctions for Privacy and Security Violations.
5. UTHSA's Institutional Compliance and Privacy Office will document all complaints received and their disposition.

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 at compliance@uthscsa.edu.

Institutional Handbook of Operating Policies (IHOP)
11.1.1 Notification of Privacy and Security Breaches

Health Insurance Portability and Accountability Act (HIPAA) of 1996
HIPAA Privacy Rule, 45 CFR Part 160 and Subparts A and E of Part 164
HIPAA Security Rule, 45 CFR Part 160 and Subparts A and C of Part 164

VII. Review and Approval History

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

Effective Date	Action Taken	Approved By	Approved Date
04/2003	Policy Origination		
04/2010	Policy Revision		
03/2013	Policy Revision		
01/2023	Policy Review, discretionary edits	ICPO	01/05/2023
08/2026	Policy Review/Discretionary Edits	ICPO	08/24/2026