



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 Oversight Policies	Date Last Reviewed: January 2023
Responsible Entity: Chief Compliance and Privacy Officer	Date Last Revised: January 2023

I. Purpose

Any individual who believes their rights granted under the federal privacy and security regulations, or any other state or federal laws dealing with privacy, security and confidentiality of protected health information have been violated may file a complaint regarding the alleged privacy violation. Formal complaints should be filed with the chief compliance and privacy officer in the Institutional Compliance and Privacy Office (ICPO).

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 any UT Health San Antonio controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

III. 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.

11.1.2 Complaints Regarding Privacy and Confidentiality of Protected Health Information

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 UT Health San Antonio employee working at an affiliated organization, UT Health San Antonio'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. UT Health San Antonio's Institutional Compliance and Privacy Office will document all complaints received and their disposition.

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 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

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
04/2003	Policy Origination		
04/2010	Policy Revision		
03/2013	Policy Revision		
01/2023	Policy Review, discretionary edits	ICPO	01/05/23