11.1.17 Sanctions for Privacy and Security Violations

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

UT Health San Antonio (UTHSA) has a duty to protect the confidentiality and integrity of Protected Health Information (PHI) as required by law, professional ethics, and accreditation requirements. This Policy is designed to ensure the consistent application of appropriate sanctions against Workforce Members (as defined herein) who fail to comply with the privacy and security policies and procedures of UTHSA, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule), the Security Standards for the Protection of Electronic Protected Health Information (HIPAA Security Rule), and the HITECH Act of 2009.

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 may create, receive, maintain, use, disclose, or have access to PHI maintained by UTHSA.

III. Policy

A. Addressing Violations

1. UTHSA is strongly committed to the protection of PHI of all patients. A Workforce Member's failure to comply with the privacy and security policies and procedures of UTHSA, unauthorized release and/or access of PHI in any form, or other violations(s) of the Privacy Compliance Program or Information Security Program requirements (Privacy Violation(s)), may result in disciplinary action as described in this Policy, subject to The Rules and Regulations of the Board of Regents of The University of Texas System.
2. Allegations of privacy violations will be investigated by the Institutional Compliance and Privacy Office (ICPO) in accordance with the applicable Privacy

Compliance Program policy and preliminary findings will be shared with departmental leadership.

3. Sanctions for privacy violations as described in this Policy will be based on ICPO's findings and will be applied consistently, considering the totality of the circumstances. Department leadership, in consultation with the Office of Human Resources, will be responsible for determining appropriate sanctions based on this Policy.

4. UTHSA may apply progressive discipline policies; however, depending on the circumstances and the severity of the violation, a Workforce Member may be disciplined at any level of the disciplinary process up to and including dismissal or termination, subject to The Rules and Regulations of the Board of Regents of The University of Texas System.

B. Privacy Violation Sanctions by Severity Level

Privacy Violations will/may result in appropriate sanctions to be determined based on the totality of circumstances, including but not limited to the severity, intentionality, and pattern/practice of the Workforce Member's behavior.

To assist in determining the significance and impact of a violation, four (4) categories of severity, including hypothetical examples of violations and appropriate disciplinary actions for each category, are identified below. This is not an exhaustive list.

1. Severity Level I:

A Level I Privacy Violation is likely an unintentional violation that may be caused by carelessness, lack of knowledge/training, or other human error. Examples of a Level I Privacy Violation may include, but are not limited to:

a. Inadvertently leaving documents containing PHI in public areas (e.g., cafeteria or breakroom locations, restrooms, etc.);

b. Leaving a computer screen unattended with unsecured PHI in an accessible area;

c. Discussing a patient's PHI in a public area with colleagues, for treatment, payment or health care operations, and speaking in a high volume without considering the surroundings (e.g., elevators, cafeteria locations, hallways, etc.);

d. Transmitting PHI via electronic mail without encrypting the transmission to a non-UTHSA email address;

e. Disclosing PHI that has not been properly redacted or de-identified in accordance with Institutional Handbook of Operating Policies (IHOP) policy 11.2.9 De-identification of Protected Health Information;

f. Leaving detailed PHI on a patient's answering machine without consent;

g. Improper disposal of PHI;

h. Transmitting PHI via mail, facsimile or electronic mail (e-mail) to the incorrect location or recipient (e.g., inadvertent fax of PHI to the incorrect recipient by misdialing or mistyping the fax number);

i. Accidental electronic transfer (e.g., e-mail) of patient data to unintended individuals or external parties that are not contracted as Business Associates of UTHSA;

j. Entering PHI into the wrong patient's medical record account that results in an unauthorized party (e.g., individual, provider's office, business associate, etc.) receiving the incorrect patient information;

k. Inadvertent Disclosure of PHI to the incorrect patient by not double-checking each page and/or using patient identifiers (e.g., discharge instruction);

l. Discussing PHI with colleagues or vendors that do not have a business need to know;

m. Discussing PHI with family or visitors of the patient without first allowing the patient the opportunity to exercise their right to consent or object to their information being disclosed;

n. Workforce Member use of user credentials to access, view or retrieve their own PHI (e.g., self-look up in an electronic medical record system); or

o. Any other violation with similar scope that may result from unintentional error or oversight.

Suggested Sanctions: Verbal or written counseling/coaching, documentation on a performance improvement plan, and/or required completion of HIPAA Privacy re-training.

2. Severity Level II:

A Level II Privacy Violation may be caused by a lack of performance improvement or failure to follow established policies and procedures. Examples of a Level II Privacy Violation may include, but are not limited to:

a. Allowing a co-worker to utilize user credentials to access PHI, or sharing passwords or other log-in credentials to circumvent information security standards;

b. Loss of paper records, information assets (e.g., laptop, cell phone, flash drive, etc.) or any electronic device that contains PHI;

c. Avoiding or bypassing security measures to photograph and/or transmit PHI to an authorized party (e.g., attending provider);

d. Any other violation with similar scope that may involve access to or release of PHI; or

e. A repeated Level I Privacy Violation.

Suggested Sanctions: Written counseling/coaching, documentation on a performance improvement plan, and/or required completion of HIPAA Privacy re-training.

3. Severity Level III:

A Level III Privacy Violation is likely a deliberate or purposeful violation without harmful intent. Examples of a Level III Privacy Violation may include, but are not limited to:

a. Workforce member accessing an electronic medical record and/or PHI of a patient (e.g., family, friend, co-worker or VIP patient) without an operational business purpose for the access (e.g., snooping);

b. Releasing PHI, in any form, to unauthorized individuals;

c. Removing and/or transporting PHI off the premises of the facility without prior approval;

d. Posting and/or transmitting patient information, images, or PHI on social media web sites;

e. Workforce member accessing paper or electronic medical record of a family member or friend, at the request of the patient, to view information or print their results for them instead of the patient signing a Release of Information (ROI) Authorization Form;

f. Any other violation with similar scope that may involve access to or release of PHI; or

g. A repeated Level II Privacy Violation.

Suggested Sanctions: Final written warning and/or a suspension; dismissal or termination based on level of severity; and/or required completion of HIPAA Privacy re-training.

4. Severity Level IV:

A Level IV Privacy Violation is likely a willful or malicious violation with harmful intent. Examples of a Level IV Privacy Violation may include but are not limited to:

a. Selling, releasing, disclosing, accessing and/or compiling patient information for personal gain, or with malicious intent;

b. Misappropriating information assets for personal use or to sell or theft of any Information Asset(s) that contains PHI;

c. Any other violation with similar scope that may involve access to or release of PHI; or

d. A repeated Level III Privacy Violation.

Suggested Sanctions: Immediate and final written warning and/or a suspension; dismissal or termination based on level of severity; may result required reporting to external entities.

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.

Institutional Handbook of Operating Policies (IHOP)
11.1.0 Privacy Compliance Program
11.2.9 De-identification of Protected Health Information

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