| Administration | Policy 1.5 |
|---|---|
| HIPAA Sanctions | Effective Date: July 22, 2011 |
| **References:** 45 U.S.C. §1320d; HITECH Act, Title XIII, Part D; 45 CFR Parts 160, 162 and 164. | |

## Policy Statement

This policy endeavors to provide for consistent and equitable responses to confirmed HIPAA Privacy violations regardless of an individual's or entity's status with TTUHSC. This policy supports, but does not replace or supersede existing Texas Tech University Health Sciences Center (TTUHSC) disciplinary processes for employees and students.

## Scope and Distribution

This policy applies to members of TTUHSC's Workforce as that term is defined below and Business Associates of Texas Tech University Health Sciences Center.

## Definitions

1. **Authorized Access, Use or Disclosure of PHI** means access, use or disclosure of PHI that is necessary to support treatment, payment or TTUHSC healthcare operations, or is otherwise authorized by the patient or his/her personal representative or required or allowed by law.

2. **Business Associate** has the same definition as stated in HSC OP 52.13, HIPAA Business Associate Agreements.

3. **HIPAA Violation** means access, use or disclosure of paper or electronic PHI that is not authorized access, use or disclosure of PHI.

4. **HIPAA Breach** is defined at 45 CFR 164.402 and generally means the acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA laws and regulations which compromises the security or privacy of the PHI that poses a significant risk of financial, reputational, or other harm to the individual.

5. **Individually Identifiable Health Information** means health information collected from an individual that is created or received by a health care provider, a health plan, or health care clearing house that:

    - Involves the past, present, or future physical or mental health, or condition of an individual; the providing of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and
    - Identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.

6. **Protected Health Information (PHI)** is individually identifiable health information maintained or transmitted by TTUHSC or any other covered entity in any form or

medium, including information transmitted orally, or in written or electronic form. PHI does not include individually identifiable health information in employment records held by TTUHSC in its role as employer.

7. **TTUHSC's Workforce Members** means faculty, employees, residents, students, volunteers and other persons whose conduct, in performance of work for TTUHSC, is under the direct control of TTUHSC, whether or not they are paid by TTUHSC. It does not include Business Associates or their employees and agents.

## Procedure

1. Responsibility to Report

   a. Workforce members and Business Associates have a responsibility to report known HIPAA Violations. See HSC OP 52.04, Report & TTUHSC Internal Investigation of Alleged Violations; Non-Retaliation. Reports may be made to one of the following:

      1) The Regional Privacy Officer for HIPAA Privacy violations;
      2) The Institutional Privacy Officer for HIPAA Privacy violation;
      3) The Information Security Officer for HIPAA Security violations;
      4) The Institutional Compliance Officer; or
      5) The Compliance Hotline, 1-866-294-9352 or https://secure.ethicspoint.com/domain/en/report_company.asp?clientid=12414re

   b. Failure to report a known HIPAA Violation may result in disciplinary action in accordance with TTUHSC policies.

   c. No one shall be retaliated against for making a report in good faith under this policy. See HSC OP 52.04, Report & TTUHSC Internal Investigation of Alleged Violations; Non-Retaliation.

2. Investigation

   a. Upon receipt of an allegation of a HIPAA Violation, the Institutional Privacy Officer (IPO) and/or Institutional Security Officer (ISO) or their designees, depending on the type of HIPAA Violation reported, shall conduct a confidential and timely investigation of the matter in accordance with TTUHSC policies. If necessary, advice may be sought from the Office of General Counsel at any point during the investigation.

   b. In the event of an alleged HIPAA Violation involving PHI of TTUHSC and an affiliated entity, the investigation shall be coordinated between the entities.

   c. All investigations shall be tracked. Each year, the IPO shall prepare a written report of all HIPAA Privacy breaches to be submitted to the HIPAA Committee,

ICO and the Office of Civil Rights no later than the last day of February. The ICO shall include this information in the annual compliance report to the Institutional Compliance Committee.

3. Levels of HIPAA Violations

The level of HIPAA Violation is determined based on the severity of the violation, whether it was intentional or unintentional, and whether the violation indicates a pattern of improper use, disclosure or release of PHI and/or misuse of computing resources. The degree of discipline may range from a verbal warning up to and including termination of relationship with TTUHSC and/or restitution in accordance with TTUHSC policies. The following three (3) levels of violations will be utilized in recommending the disciplinary action and/or corrective action to apply:

a. **Level 1:** An individual inadvertently or mistakenly accesses PHI that **he/she had no need to know** in order to carry out his/her responsibilities for TTUHSC, or carelessly accesses or discloses information to which he/she has authorized access. Examples of level 1 HIPAA violations include, but are not limited to, the following:

- Leaving PHI in a public area;
- Mistakenly sending e-mails or faxes containing PHI to the wrong recipient;
- Discussing PHI in public areas where it can be overhead, such as elevators, cafeteria, restaurants, hallways, etc.;
- Leaving a computer accessible and unattended with unsecured PHI;
- Loss of an unencrypted electronic device containing unsecured PHI;
- Improperly disposes of PHI in violation of TTUHSC policy;
- An individual fails to report that his/her password has been potentially compromised (i.e., has responded to e-mail spam and given out their password);

b. **Level 2:** An individual **intentionally** accesses, uses and/or discloses PHI **without appropriate authorization**. Examples of level 2 HIPAA violations include, but are not limited to, the following:

- Intentional, unauthorized access to your own, friends, relatives, co-workers, public personality's, or other individual's PHI (including searching for an address or phone number);
- Intentionally assisting another individual to gain unauthorized access to PHI. This includes, but is not limited to, giving another individual your unique user name and password to access electronic PHI;
- Disclosing patient condition, status or other PHI obtained as a TTUHSC workforce member to another TTUHSC workforce member who does not have a legitimate need to know;
- Fails to properly verify the identity of individuals requesting PHI which results in inappropriate disclosure, access or use of PHI;

- Logs into the TTUHSC network resources (including EMRs) and allows another individual to access PHI;
- Connects devices to the network and/or uploads software without having received authority from IT;
- Second occurrence of any Level 1 violation (it does not have to be the same offense).

c. **Level 3**: An individual **intentionally** uses, accesses and/or discloses PHI **without any authorization and causes personal or financial gain; causes physical or emotional harm to another person; or causes reputational or financial harm to the institution.** Examples of level 3 HIPAA violations include, but are not limited to, the following:

- Unauthorized intentional disclosure and/or delivery of PHI to anyone;
- Intentionally assisting another individual to gain unauthorized access to PHI to cause harm. This includes, but is not limited to, giving another individual your unique user name and password to access electronic PHI;
- Access or uses PHI for personal gain (i.e., lawsuit, marital dispute, custody dispute);
- Discloses PHI for financial or other personal gain;
- Uses, accesses or discloses PHI that results in personal, financial or reputational harm or embarrassment to the patient;
- Utilizes TTUHSC computing resources, including the network, that are either related to or result in events that are reportable to the FBI;
- Attempts to penetrate or gain access to the TTUHSC network and/or its resources without appropriate authorization;
- Second occurrence of any Level 2 violation (it does not have to be the same offense) or multiple occurrences of any Level 1 violation.

4. Response to Confirmed HIPAA Privacy Violations

ALTHOUGH RESPONSES TO CONFIRMED HIPAA PRIVACY VIOLATIONS ARE SPECIFIED BELOW IN THIS SECTION, DISCIPLINARY ACTION MAY TAKE PLACE AT ANY TIME, UP TO AND INCLUDING TERMINATION IN ACCORDANCE WITH APPLICABLE POLICIES.

a. TTUHSC Employees (Faculty, Residents, Staff, and Post-doctoral Fellows).

- Level 1 violations shall result in an informal talk, oral warning and/or letter of disciplinary reprimand in accordance with HSC OP 70.31, Employee Conduct, Discipline and Separation of Employees.

- Level 2 violations shall result in a letter of disciplinary reprimand, and may include imposition of disciplinary leave without pay and/or a recommendation for termination. See HSC OP 70.31, Employee Conduct, Discipline and Separation of Employees and/or HSC OP 60.01, Tenure and Promotion Policy.

- Level 3 violations, in most cases, shall result in termination of employment and/or association with TTUHSC. See HSC OP 70.31, Employee Conduct, Discipline and Separation of Employees and/or HSC OP 60.01, Tenure and Promotion Policy.

1) *Staff.* When a non-faculty employee is involved, the Human Resources office at the campus shall be consulted before taking disciplinary action.

2) *Faculty.* When faculty is involved, the faculty member's Chair shall be consulted, and the faculty shall have the rights outlined in relevant faculty policies.

3) *Residents.* When a resident is involved, the resident's supervising Residency Director, Department Chair, and the Associate Dean or designee shall be consulted in addition to Human Resources office at the campus.

4) *Post-Doctoral Fellows.* When post-doctoral fellows are involved, his/her Faculty Supervisor shall be notified.

b. TTUHSC volunteers. Violations by volunteers shall be reported to the Director of Volunteer Services at the campus and will result in the volunteer's termination from the program if recommended, regardless of the level of violation.

c. TTUHSC students. Any level of HIPAA violation is considered unprofessional conduct and subject to discipline as outlined in the Student Handbook, Code of Professional and Academic Conduct applicable to that student's School.

d. TTUHSC Business Associates. Any level of breach by the BA and/or its employees or agents shall be addressed by TTUHSC in accordance with the terms of the BA Agreement currently in effect at the time of the breach.

e. Individuals Participating in TTUHSC Programs under an Affiliation Agreements (i.e., non-TTUHSC students, externs, residents).

Any level of violation by an individual participating in TTUHSC programs under an Affiliation Agreement shall be reported to applicable TTUHSC Dean of the School or his/her designee and the affiliated entity for appropriate action, which may include, but is not limited to, suspension of individual's access to PHI and/or termination of the individual from participation in the TTUHSC program.

5. Notification of State or Federal Agencies. In the discretion of the ICO, in consultation with the Office of General Counsel, the President and/or the Institutional Compliance Committee, certain violations may be reported to law enforcement officials and/or regulatory, accrediting and/or licensure organizations.

6. Access, Use or Disclosures that Do Not Constitute HIPAA Violations. The policy and procedures outlined in this policy do not apply when an individual exercises his/her right to:

    - File a complaint with the Office of Civil Rights, U.S. Department of Health and Human Services pursuant to the HIPAA regulations;
    - Testify, assist or participate in an investigation, compliance review, proceeding, or hearing under Part C of Title XI of the Social Security Act (42 U.S.C. §1320d);
    - Oppose any act made unlawful by the HIPAA Privacy or Security rules; provided the individual has a good faith belief that the act opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of the HIPAA Privacy and Security rules;
    - Disclose PHI as a whistleblower and the disclosure is to a health oversight agency; public health authority; or an attorney retained by the individual for purposes of determining the individual's legal options with regard to the whistleblower activity provided the individual in good faith believes TTUHSC has acted unlawfully; or
    - The individual is the victim of a crime and discloses PHI to a law enforcement official, provided that the PHI is about a suspected perpetrator of the criminal act; and is limited to the information allowed under federal law.

**NOTE:** *References to other TTUHSC Operating Policies are general and do not exclude application of any appropriate TTUHSC policy.*

## Approval Authority

Questions regarding this policy may be addressed to the Regional Privacy Officer (Amarillo, El Paso, Permian Basin), the Institutional Privacy Officer, Institutional Security Officer, or the Institutional Compliance Officer.

## Responsibility and Revisions

This policy may be amended or terminated at any time to address changes in law or processes at TTUHSC.