TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 52.14, **HIPAA Sanctions Process**

PURPOSE: The purpose of this Texas Tech University Health Sciences Center El Paso (TTUHSC El Paso) Operating Policy and Procedure (HSCEP OP) is to provide consistent and equitable responses to confirmed HIPAA Privacy and Security violations in accordance with existing TTUHSC El Paso disciplinary processes. This policy applies to TTUHSC El Paso's workforce members

REVIEW: This HSCEP OP will be reviewed in March of each even-numbered year by the TTUHSC El Paso Privacy and Security Committee, with recommendations for revisions forwarded to the Institutional Compliance Committee for the April meeting.

POLICY/PROCEDURE:

I. Definitions

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

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

C. **HIPAA Violation** means unauthorized access, use, or disclosure of paper or electronic PHI.

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

E. **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 clearinghouse 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.

F. **Protected Health Information (PHI)** is individually identifiable health information maintained or transmitted by TTUHSC El Paso or any other covered entity in any form or medium, including information transmitted orally or in written or electronic form.

G. **TTUHSC El Paso Workforce Members** means faculty, employees, residents, students, volunteers, and other persons whose conduct, in performance of work for TTUHSC El Paso, is under the direct control of TTUHSC El Paso, whether or not they are paid by

TTUHSC El Paso. It does not include business associates or their employees and agents.

II. Responsibility to Report

A. TTUHSC El Paso workforce members and business associates have a responsibility to report known HIPAA Violations. See HSCEP OP 52.03, Fraud and Misconduct Hotline. Reports may be made to one of the following:

1. The institutional privacy officer (IPO) for HIPAA privacy violations;

2. The informational security officer (ISO) for HIPAA Security violations;

3. The institutional compliance officer; or

4. The Fraud and Misconduct Hotline, 1-866-294-9352, 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 El Paso policies.

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

III. Investigation

A. Upon receipt of an allegation of a HIPAA violation, the IPO and/or ISO or their designees, depending on the type of HIPAA Violation reported, will conduct a confidential and timely investigation of the matter in accordance with TTUHSC El Paso 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 the PHI of TTUHSC El Paso and an affiliated entity, the investigation will be coordinated between the entities.

C. All investigations will be tracked. Each year, the IPO, in coordination with the institutional compliance officer and the ISO, will prepare a written report of all HIPAA privacy and security breaches to be submitted to the HIPAA Committee, ICO, and the Office for Civil Rights no later than the last day of February. The ICO will include this information in the annual compliance report to the Institutional Compliance Committee.

IV. Levels of HIPAA Violation

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 El Paso and/or restitution in accordance with TTUHSC El Paso policies. The following three violation levels will be used in recommending the applicable disciplinary action and/or corrective action.

The Privacy Disciplinary Recommendation Guide (Attachment A) will be utilized to assist in determining the violation level.

A. **Level 1:** An individual inadvertently or mistakenly accesses PHI that **he/she had no need to access** in order to carry out his/her responsibilities for TTUHSC El Paso, 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 overheard, 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 El Paso policy;
- An individual fails to report that his/her password has been potentially compromised (i.e., has responded to e-mail spam giving 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, 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 username and password to access electronic PHI;
- Disclosing patient condition, status or other PHI obtained as a TTUHSC El Paso workforce member to another TTUHSC El Paso workforce member who does not have a legitimate need to know;
- Failing to properly verify the identity of individuals requesting PHI which results in inappropriate disclosure, access, or use of PHI;
- Logging into the TTUHSC El Paso network resources (including EMRs) and allowing another individual to access PHI;
- Connecting devices to the network and/or uploading 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 username and password to access electronic PHI;
- Accessing or using PHI for personal gain (i.e., lawsuit, marital dispute, custody dispute);
- Disclosing PHI for financial or other personal gain;
- Using, accessing, or disclosing PHI that results in personal, financial, or reputational harm or embarrassment to the patient;
- Utilizing TTUHSC El Paso computing resources, including the network, that are either related to or result in events that are reportable to the FBI;
- Attempting to penetrate or gain access to the TTUHSC El Paso 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.

V. Response to Confirmed HIPAA Privacy and Security Violations

ALTHOUGH RESPONSES TO CONFIRMED HIPAA PRIVACY AND SECURITY 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 El Paso Employees (Faculty, Residents, Staff, and Post-Doctoral Fellows).

- Level 1 violations will result in an informal discussion, oral warning and/or letter of disciplinary reprimand in accordance with HSCEP OP 70.31, Employee Conduct, Coaching, Corrective Action and Termination of Employees.

- Level 2 violations, in most cases, will result in a letter of disciplinary reprimand, and may include imposition of disciplinary leave without pay and/or a recommendation for termination. See HSCEP OP 70.31, Employee Conduct, Coaching, Corrective Action and Termination of Employees and/or HSCEP OP 60.01, Tenure and Promotion Policy.

- Level 3 violations, in most cases, will result in termination of employment and/or association with TTUHSC El Paso. See HSCEP OP 70.31, Employees Conduct, Coaching, Corrective Action and Termination of Employees and/or HSCEP OP 60.01, Tenure and Promotion Policy.

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

2. *Faculty.* When faculty is involved, the faculty member's Chair will be consulted, and the faculty will 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 will be consulted in addition to Human Resources.

4. *Post-Doctoral Fellows*. When post-doctoral fellows are involved, their faculty supervisor will be notified.

B. TTUHSC El Paso Volunteers. Violations by volunteers will be reported to the director of Volunteer Services and will result in the volunteer's termination from the program if recommended, regardless of the level of violation.

C. TTUHSC El Paso 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 El Paso Business Associates. Any level of breach by the Business Associate and/or its employees or agents will be addressed by TTUHSC El Paso in accordance with the terms of the Business Associate's Agreement currently in effect at the time of the breach.

E. Individuals Participating in TTUHSC El Paso Programs under Affiliation Agreements (i.e., non-TTU students, externs, residents). Any level of violation by an individual participating in TTUHSC El Paso programs under an Affiliation Agreement will be reported to the

applicable TTUHSC El Paso dean of the School or their designee and the affiliated entity for appropriate action, which may include, but is not limited to, suspension of the individual's access to PHI and/or termination of the individual from participation in the TTUHSC El Paso program.

VI. **Notification of State or Federal Agencies.** At 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.

VII. Access, Use, or Disclosures that Do Not Constitute HIPAA Violations

The policy and procedures outlined in this policy do not apply when an individual exercise their rights to:

- File a complaint with the Office for 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 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 about the whistleblower activity provided the individual in good faith believes TTUHSC El Paso 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 HSCEP OPs are general and do not exclude the application of any appropriate TTUHSC El Paso policy.*

VIII. Right to Change Policy.

TTUHSC El Paso reserves the right to interpret, change, modify, amend or rescind any policy in whole or in part at any time.