Texas Tech University Health Sciences Center
HIPAA Privacy Policies

Complaints, Breaches and Sanctions	**Policy 5.3**
HIPAA Violations – Discipline	**Effective Date: May 15, 2016**
References: http://www.hhs.gov/ocr/hipaa HSC HIPAA website http://www.ttuhsc.edu/hipaa/policies_procedures.aspx	

Policy Statement

The purpose of this Health Sciences Center HIPAA Policy and Procedure (HSC HPP) is to provide for consistent and equitable responses to confirmed HIPAA Privacy and Security violations in accordance with existing Texas Tech University Health Sciences Center (TTUHSC) disciplinary processes. This policy applies to TTUHSC's Workforce members and Business Associates.

HPP 5.3 created from Operating Policy 52.14 *HIPAA Sanctions Process* as part of consolidation of HIPAA guidance to HPP format. OP 52.14 deactivated.

Scope and Distribution

This policy applies to all health care clinical service areas owned and/or operated by TTUHSC. It does not apply to inmates seen or treated by TTUHSC.

Definitions

Refer to HPP 1.1 for Glossary of HIPAA Terms

See *Old/New HIPAA Policy Number Cross Reference Chart*

Procedure

1. **Responsibility to Report**

a. TTUHSC Workforce members and Business Associates have a responsibility to report known HIPAA Violations. See HSC OP 52.03, Compliance Hotline. 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 violations;
   3) The Informational 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 Investigations of Alleged Violations; Non-Retaliation.

2. **Investigation**

a. Upon receipt of an allegation of a HIPAA violation, the Institutional Privacy Office (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 and ISO shall prepare a written report of all HIPAA Privacy and Security breaches to be submitted to the HIPAA Privacy and Security Committee, ICO and the Office for 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 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 and/or restitution in accordance with TTUSHC 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 mistakenly accesses PHI that he/she had no need to know in carrying 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:

- 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.;
- 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 or through negligence 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;
- Leaving PHI in a public area;
- 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;
- 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:
- Intentionally assisting another individual to gain unauthorized access to PHI to cause harm to the patient or for personal and/or financial gain. This includes, but is not limited to, giving another individual your unique user name and password to access electronic PHI that results in personal/financial benefit for the employee and/or individual, and/or harm to the patient;
- Access, disclosures or uses PHI for financial and/or personal benefit to the employee or another individual (i.e., lawsuit, marital dispute, custody dispute);
- 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 and Security Violations**

Tiered disciplinary actions listed here are for general guidance only. Any disciplinary action is at the discretion of the employee's supervisor and/or Human Resources Department. The Office of Institutional Compliance does not determine nor administer disciplinary actions.

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

- **Level 1** violations may 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 may result in a letter of disciplinary reprimand, and may include imposition of disciplinary leave without pay and/or a recommendation for termination. See HSCOP 70.31, Employee Conduct, Discipline and Separation of Employees and/or HSCOP 60.01, Tenure and Promotion Policy.

- **Level 3** violations may result in termination of employment and/or association with TTUHSC. See HSCOP 70.31, Employees Conduct, Discipline and Separation of Employees and/or HSCOP 60.01, Tenure and Promotion Policy.

Parties to contact:

1) *Staff*. When a non-faculty employee is involved, the Human Resources office at the campus may 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.

5) *TTUHSC Volunteers*. Violations by volunteers shall be reported to the Director of Volunteer Services at the campus.

6) *TTUHSC Student*s. 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.

b. TTUHSC Business Associates. Any level of breach by the Business Associate 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.

c. 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 the 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 outlines in this policy do not apply when an individual exercises his/her rights to:

- File a complaint with the Office for Civil Right, 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.

This policy and procedure will be documented and retained for a period of 6 years from the date of its creation or the date when it last was in effect, whichever is later.

Knowledge of a violation or potential violation of this policy must be reported directly to a Regional Privacy Officer, the Institutional Privacy Officer or to the employee Compliance Hotline at (866) 294-9352 or Ethics Point - Texas Tech University under HSC.

Approval Authority

The TTUHSC Privacy and Security Committee has authority for HIPAA policy approval.

Responsibility and Revisions

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

This policy may be amended or terminated at any time.