



# TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER

## Operating Policy and Procedure

**HSC OP:** 52.05, **Privacy Compliance Plan**

**PURPOSE:** The purpose of this Health Sciences Center Operating Policy and Procedure (HSC OP) is to provide a framework for implementation of an effective information privacy compliance program for Texas Tech University Health Sciences Center (TTUHSC).

**REVIEW:** This HSC OP will be reviewed in July of each even-numbered year (ENY) by the TTUHSC Institutional Privacy Officer, the TTUHSC Information Security Officer, the Associate Provost for Student Affairs, the VP for Information Technology and Chief Information Officer (CIO), and the Office of General Counsel. Any substantive revisions will then be forwarded to the Privacy and Security Committee (PSC).

### **POLICY/PROCEDURE:**

#### **I. Introduction**

Texas Tech University Health Sciences Center (TTUHSC) is subject to many laws, rules and regulations as an academic, research and patient care center. Failure to comply with these laws, rules and regulations can adversely impact TTUHSC's ability to continue these activities. TTUHSC is committed to conducting its activities in an ethical and honest manner and in compliance with applicable laws, regulations, Texas Tech University System (TTUS) Regents rules, and TTUHSC policies.

The goal of the TTUHSC Privacy Compliance Plan is to provide guidelines that promote understanding and compliance with applicable information privacy laws, rules, and regulations, including the Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act of 1999 (GLBA), Payment Card Industry Data Security Standard (PCI DSS) and other applicable information privacy regulations. This Privacy Compliance Plan is designed to help TTUHSC faculty, staff, and students understand how to appropriately handle and safeguard Protected Health Information (PHI), education records and other confidential information as well as the core responsibilities for complying with HIPAA, FERPA and other privacy and security regulations. Confidential Information has the same meaning as set forth in [HSC OP 52.09](#), Confidential Information.

#### **II. Compliance Policies.**

- a. Anyone who has access to Confidential Information regarding TTUHSC employees, Students, patients, affiliates, or any other information made confidential by TTUHSC policies or law will take reasonable and necessary steps to maintain the confidentiality and privacy of such information.
- b. It is illegal for a TTUHSC employee to use confidential information for the personal benefit/gain of himself/herself or another or to harm another person.
- c. Security, access to, and use, and/or disclosure of PHI shall be governed by HIPAA, HITECH and TTUHSC's [HIPAA Privacy Policies](#) and [Information Technology & Security Policies](#).
- d. Security, access to, and use, and/or disclosure of student education records shall be governed by FERPA and [HSC OP 77.13](#), Student Education Records. Access to student educational records is granted on the basis of a legitimate educational interest of the employee, Student or Volunteer.

- e. Security, access to, and use, and/or disclosure of certain financial information that is covered by the Gramm-Leach-Bliley Act of 1999, shall be governed by [HSC OP 52.09](#), Confidential Information, [Attachment A](#) – Information Security Plan for Financial Information.
- f. Any form of credit/bank card processing shall be governed by PCI DSS and [HSC OP 56.34](#), PCI (Credit Card Processing) Data security.
- g. Electronic transformation of Personally Identifiable Information (PII) and PHI shall be governed by HIPAA and [HSC OP 56.04](#), Electronic Transmission of Personally Identifiable Information (PII) and Protected Health Information (PHI).
- h. Security, access to, and use, and/or disclosure of any other Confidential Information shall be governed by [HSC OP 52.09](#), Confidential Information.

### **III. Privacy Compliance Oversight**

- a. Authority. The Privacy and Security Committee (PSC) is responsible for implementing, managing and oversight of this Privacy Compliance Plan. The PSC also serves as the HIPAA Privacy and Security Committee for TTUHSC. The PSC, and any subcommittees established by the PSC, shall each be considered a “medical committee” as defined under Texas Health and Safety Code 5 §161.031(a), and/or other applicable state and federal laws. All documents generated by the PSC, submitted to the PSC or created for the purposes of fulfilling PSC’s duties under this Privacy Compliance Plan, are confidential and privileged and shall be identified as a “Confidential – Medical Committee Document.” The PSC reports to the Institutional Compliance and Risk Committee (ICRC).
- b. Membership. The Institutional Privacy Officer shall serve or appoint a designee to serve as the Chair of PSC. The Chair appoints the committee members. The PSC shall consist of representations from the following areas (Members may serve in more than one capacity):
  - Office of Institutional Compliance (Institutional Compliance Officer & Institutional Privacy Officer)
  - Information Technology (Chief Information Officer & Information Security Officer)
  - School of Medicine Information Application Services
  - Clinical Transformation
  - Medical Records Office
  - Human Resources
  - Student Affairs
  - Finance
  - Managed Care
  - Clinical Research and/or Research Integrity Department
  - School of Medicine
  - School of Nursing
  - School of Health Professions
  - School of Pharmacy
  - Graduate School of Biomedical Sciences
  - Clinical Leadership/Administrator
  - General Counsel (ex-officio, non-voting member)
  - TTU HIPAA Compliance Liaison (ex-officio, non-voting member)

The PSC may also invite independent experts or advisors to meetings as it deems necessary or appropriate, to advise the PSC on specific matters and issues.

- c. Meetings. The PSC shall meet at least quarterly or more often as necessary to meet its responsibilities under this Privacy Compliance Plan. Minutes are maintained in the Office

of Institutional Compliance. A quorum for the conduct of business by the PSC shall consist of a majority of the appointed voting members.

- d. Roles and Responsibilities. The PSC's responsibilities include:
  - i. Oversee and monitor implementation of this Privacy Compliance Plan.
  - ii. Recommend, review, and/or approve policies and procedures related to information privacy and/or security.
  - iii. Provide guidance and oversight of information privacy and security monitoring activities conducted by the Institutional Privacy Officer and Information Security Officer.
  - iv. Review reports of investigations of concerns and/or complaints related to information privacy and/or security compliance and review responsive or corrective action(s) taken to minimize the risk of similar non-compliance in the future. The PSC may recommend further action to persons with authority to implement such recommendations.
  - v. Stay abreast of emerging information privacy and security issues and adjust strategy as necessary.
  - vi. Report information back to respective areas to bring awareness and compliance of HIPAA, HITECH law, FERPA, PCI DSS, and other information privacy and/or security regulations.
  - vii. Periodically assess and report to the ICRC on the effectiveness of the overall privacy compliance program and of individual programs (e.g., HIPAA, FERPA, Gramm-Leach-Bliley, etc.)

#### **IV. Education and Training**

General and topic-specific training modules have been developed for employees, students, and volunteers by the responsible departments/offices. Please refer to the applicable compliance policies identified above for detailed information about the education and training requirement for different topics.

#### **V. Reporting Responsibilities and Resources**

Anyone who knows of or suspects a violation of any information privacy compliance policies identified above shall report that incident promptly to his/her immediate supervisor and/or to individuals in accordance with the applicable privacy compliance policies and [HSC OP 52.04](#), Report & TTUHSC Internal Investigation of Alleged Violations, Non-Retaliation. TTUHSC shall not intimidate, threaten, coerce, terminate, discriminate against or take any retaliatory action against any person who, in good faith, reports suspected non-compliance or violations of law or TTUHSC policies.

#### **VI. Response and Corrective Action**

All reports of suspected violations and non-compliance shall be reviewed and investigated. All information acquired in the investigation and any findings and recommendations shall be kept confidential. Violations of any compliance policies identified above may result in corrective actions as set forth in the applicable policies including, but not limited to [Texas Tech University System Regulation 07.07](#), Employee Conduct, Coaching, Corrective Action, and Termination, [HSC OP 60.01](#), Tenure and Promotion Policy, and the [TTUHSC Students Handbook](#).

#### **VII. Right to Change Policy.**

TTUHSC reserves the right to interpret, change, modify, amend or rescind this policy in whole or in part at any time without the consent of employees.