



# TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER

## Operating Policy and Procedure

**HSC OP:** 52.02, **Privacy and Security of Health Information**

**PURPOSE:** The purpose of this Health Sciences Center Operating Policy and Procedure (HSC OP) is to provide a framework for Texas Tech University Health Sciences Center's (TTUHSC) compliance with the provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and state laws and regulations for the privacy and security of health information.

**REVIEW:** This HSC OP will be reviewed on November 1 of each odd-numbered year (ONY) by the TTUHSC Institutional Privacy Officer, the TTUHSC Information Security Officer, and the HIPAA Committee, with recommendations for revisions forwarded to the President by January 1.

### **POLICY/PROCEDURE:**

#### **1. Definitions**

- a. "Health Insurance Portability and Accountability Act of 1996" or "**HIPAA**" is the federal law that establishes national standards for the privacy and security of health information and electronic health care transactions, which are found in 45 CFR Parts 160, 162 and 164.
- b. "HIPAA Privacy and Security Committee, (hereinafter "**HIPAA Committee**") is a committee established by the President to provide oversight of TTUHSC's compliance with HIPAA and applicable state laws governing the use, storage and disclosure of Protected Health Information (PHI).
- c. "**Institutional Privacy Officer**" is the individual responsible for overseeing compliance with the privacy provisions of HIPAA (Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164) and applicable state laws.
- d. "**Institutional Security Officer**" is the individual appointed under HSC OP 56.01 who is responsible for overseeing compliance with the *security* provisions of HIPAA (Security Standards for the Protection of Electronic Protected Information, 45 CFR Parts 160, 162 and 164) and applicable state laws and other related duties.
- e. "**Protected Health Information (PHI)**" is individually identifiable health information created, 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.
- f. "**Electronic PHI**" is individually identifiable health information that is transmitted by or maintained in electronic media. Examples include, but are not limited to internet, extranet, leased lines, dial-up lines, private networks, hard drives, flash drives, magnetic tape/disk, CD, digital memory card, etc.
- g. "**Hybrid Entity**" For purposes of HIPAA, TTUHSC has designated itself a hybrid entity. The HIPAA Committee is responsible for designating and identifying the TTUHSC health care components subject to HIPAA based on performance of covered functions, and these shall be listed in the HIPAA policies.
- h. "**HITECH**" – Health Information Technology for Economic and Clinical Health Act, which is part of the American Recovery and Reinvestment Act of 2009. It is a federal law that

affects the health care industry that provides expanded reach of HIPAA. Section 13400-13423 Subtitle D-Privacy.

- i. **“Workforce Member”** – TTUHSC workforce member means 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. See 45 CFR 160.103.

## 2. **Obligations of Workforce Members**

TTUHSC faculty, staff, students, volunteers and vendors are expected to follow federal and state laws, as well as TTUHSC policies regarding the privacy and security of PHI.

## 3. **Institutional HIPAA Privacy and Security Officers**

- a. Privacy. TTUHSC’s Institutional Privacy Officer (IPO) reports to the Institutional Compliance Officer. The IPO is responsible for developing and implementing HIPAA privacy policies approved by the HIPAA Committee, initial and on-going HIPAA privacy training, monitoring use and disclosure of PHI and investigating HIPAA privacy concerns/complaints.
- b. Security. TTUHSC’s Institutional Security Officer (ISO) is responsible for developing and implementing HIPAA security policies, providing initial and on-going HIPAA Security training, monitoring security of TTUHSC electronic PHI and investigating of HIPAA security breaches, concerns, and complaints.
- c. The IPO and ISO shall work collaboratively to encourage and foster compliance with HIPAA Privacy and Security laws and regulations as well as related TTUHSC policies. This may include working with Schools and regional campuses to appoint regional privacy officers and/or security liaison to assist with HIPAA compliance activities.

## 4. **HIPAA Committee**

- a. Establishment of HIPAA Committee. The President has established an Institutional HIPAA Committee to oversee issues and concerns related to the privacy and security of PHI and electronic PHI. The HIPAA Committee, and any subcommittees established under it, shall each be considered a “medical committee” as defined under Texas Health & Safety Code § 161.031(a), and/or other applicable state and federal statutes. All documents generated by, submitted to, or created for the purposes of fulfilling HIPAA Committee’s duties are confidential and privileged and shall be identified as a “Confidential – Medical Committee Document”.
- b. Membership. The HIPAA Committee shall consist of the following voting members: (Members may serve in more than one capacity.)
  - Institutional Compliance Officer
  - Institutional Privacy Officer
  - Institutional Security Officer
  - Regional Privacy Officers
  - Regional Security Liaison
  - Clinical Research and/or Research Integrity Department Representative
  - Representative from Schools of Medicine Information Application Services Department
  - Human Resources Representative appointed by the Assistant Vice President of Human Resources
  - Representative from each School (Medicine, Nursing, Allied Health Sciences, Biomedical Sciences & Pharmacy) as appointed by the Dean of that School
  - Senior Security Manager
  - Clinical Faculty Representative (SOM, PLFSOM, SON, SOAHS, SOP)

- General Counsel representative appointed by the Senior Associate General Counsel (ex-officio, without vote)

The IPO shall serve as the chair of the HIPAA Committee.

c. Responsibilities. The HIPAA Committee shall:

1. Policies. Recommend, review, and/or approve HIPAA Privacy and Security policies, which shall be incorporated by reference into this policy and posted at the following websites:
  - i. HIPAA Privacy: [http://www.ttuhs.edu/hipaa/policies\\_procedures.aspx](http://www.ttuhs.edu/hipaa/policies_procedures.aspx);
  - ii. HIPAA Security: <http://www.ttuhs.edu/it/policy>
  - iii. Manuals: [http://www.ttuhs.edu/hipaa/policies\\_procedures.aspx](http://www.ttuhs.edu/hipaa/policies_procedures.aspx)
2. Monitoring. Provide guidance and oversight of HIPAA Privacy and Security monitoring activity conducted by the Institutional Privacy Officer and Institutional Security Officer.
3. Investigations/Reports. Review reports of investigations of concerns and/or complaints related to HIPAA 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 HIPAA Committee may recommend further action to persons with authority to implement such recommendations.
4. Communication. Responsible for reporting information back to respective areas to bring awareness and compliance of HIPAA regulations, HITECH law, and HIPAA privacy and security policies.

d. Meetings. The HIPAA Committee shall meet monthly or more often as necessary to deal with HIPAA Privacy and/or HIPAA Security matters.

e. Subcommittees. The HIPAA Committee is specifically authorized to appoint subcommittees consisting of TTUHSC faculty, staff or students to provide guidance on specific HIPAA Privacy and Security matters.

## 5. **Violations**

Violations of HIPAA privacy and security laws or TTUHSC policies shall be reported to the IPO and/or ISO, or in accordance with TTUHSC OP 52.04, Report & TTUHSC Internal Investigation of Alleged Violations; Non-Retaliation. Violations of HIPAA privacy or security policies may be subject to legal or disciplinary action in accordance with applicable civil and criminal laws, rules, and TTUHSC OP 52.14, HIPAA Sanctions Process. Violations, as used here, include, but are not limited to failure to comply with federal or state privacy laws, TTUHSC privacy and security policies, participating, encouraging, aiding or failing to report known breaches of HIPAA privacy and/or security.

## 6. **Right to Change Policy.**

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