TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

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

PURPOSE: The purpose of this Texas Tech University Health Sciences Center El Paso (TTUHSC EP) Health Sciences Center Operating Policy and Procedure (HSCEP OP) is to provide a framework for 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 HSCEP OP will be reviewed by November 1 of each even numbered year (ENY) by the Institutional Privacy Officer, the Information Security Officer, with recommendations for revisions forwarded to the HIPAA Privacy and Security Committee.

POLICY/PROCEDURE:

1. Definitions:

- **Affiliated Entities-means** covered entities that are legally separate entities but share common ownership (5 percent or more) or control. Entities that share such a relationship may designate themselves as a single entity for purposes of complying with the privacy and security rule. 45 CFR 164.504

- **"Covered Entity"(CE)** means a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction. 45 CFR 160.103

- **"Covered Entity" In the Texas Health and Safety Code 181.001** means any person who:

  A. for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, non-profit, or pro bono basis, engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information;
  B. comes into possession of protected health information;
  C. obtains or stores protected health information; or
  D. is an employee, agent, or contractor of a person described by Paragraph (A), (B), or (C) insofar as the employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits protected health information.

- **"Electronic Protected Health Information" (hereinafter ePHI)** means any electronic individually identifiable health information in any electronic form, including information related to payment for health services provided by the Covered Entity. 45 CFR 160.103.

- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** means a federal law that allows persons to qualify immediately for comparable health insurance coverage when they change their employment relationships. Title 11, Subtitle F of HIPAA gives DHHS the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans) and employers (or sponsors); and to specify the types of measures required to

protect the security and privacy of personally identifiable health care information. 45 CFR Parts 160,162,164

- **HIPAA Committee -** HIPAA Privacy and Security Committee is an Institutional committee established by the President to provide oversight of TTUHSC EP's compliance with HIPAA and applicable state laws governing the use, storage and disclosure of protected health information (PHI). See Section 5.

- **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 an expanded reach of HIPAA. Section 13400 and 13423 Subtitle D-Privacy.

- **Institutional Privacy Officer (IPO)** 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.

- **Information Security Officer (ISO)** is the individual appointed under HSCEP 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.

- **Organized Health Care Arrangement (OHCA)** means a clinically integrated care setting in which individuals typically receive health care from more than one health care provider; and an organized system of health care in which more than one covered entity participates and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement; and participate in joint activities that include at least one of the following: Utilization review, Quality assessment and improvement activities; or payment activities. 45 CFR 160.103. See Section 2.

- **Protected Health Information (hereinafter PHI)** means any individually identifiable health information in any form, including information related to payment for health services provided by the covered entity. 45 CFR 160.103

- **Workforce Member** means employees, residents, students, volunteers, trainees, and other persons whose conduct, in performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate. 45 CFR 160.103

3. Obligations of Workforce Members

TTUHSC EP faculty, staff, residents, students, volunteers, trainees, and temporary employees either internal or external are required to follow federal and state laws, as well as TTUHSC EP policies regarding the privacy and security of PHI.

4. Institutional HIPAA Privacy and Security Officers

a. Privacy. TTUHSC EP's Institutional Privacy Officer (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 and complaints.

b. Security. TTUHSC EP's Information Security Officer (ISO) is responsible for developing and implementing HIPAA security policies, providing initial and on-going HIPAA security training, monitoring the security of TTUHSC EP electronic PHI and investigating 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 EP policies.

5. HIPAA Committee

a. Establishment of HIPAA Committee. The President established the Institutional HIPAA Privacy and Security Committee to oversee issues and concerns related to the privacy and security of PHI and ePHI with reporting obligations to the Institutional Compliance Committee (ICC). The HIPAA Privacy and Security 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 to fulfill HIPAA Privacy and Security Committee's duties are confidential and privileged and shall be identified as a "Confidential – Medical Committee" Document.

b. 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: https://elpaso.ttuhsc.edu/hipaa/policies-procedures.aspx
   ii. HIPAA Security: https://elpaso.ttuhsc.edu/it/policies/default.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 with HIPAA regulations, HITECH law, and HIPAA privacy and security policies.

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

d. Subcommittees. The HIPAA Privacy and Security Committee is specifically authorized to appoint subcommittees consisting of the TTUHSC EP workforce to guide specific HIPAA Privacy and Security matters.

6. Violations

Violations of HIPAA privacy and security laws or TTUHSC EP policies shall be reported to the IPO and/or ISO, or in accordance with TTUHSC EP OP 52.04, Report & TTUHSC EP 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 EP OP 52.14, HIPAA Sanctions Process.

7. Training

All workforce members are required to complete initial and refresher HIPAA privacy and security training and education as set forth by Federal and State law. All new TTUHSC EP workforce members must complete training within the first thirty (30) days of employment. Annual training will be assigned based on a calendar year. Annual training must be completed within ninety (90) days of notification from the Compliance Office. Training not completed within ninety (90) days may be subject to having access removed from the TTUHSC EP network or electronic health record.

a. Training Materials. The IPO and ISO are responsible for developing the HIPAA privacy and security training materials.

b. Training Modalities. Various methods may be used to deliver HIPAA Privacy and Security training, including, but not limited to, live, video-tape, internal/external web-based sessions, email, memorandum, digital signage, newsletters, or any combination thereof.

c. Tracking. The IPO is responsible for tracking the completion of privacy training and the ISO is responsible for tracking security training. The IPO and ISO are responsible for notifying supervisors/directors if required HIPAA and security training has not been timely completed by workforce members under their supervision.

8. Right to Change Policy

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