Operating Policy and Procedure

SON OP: 10.050 Privacy and Security of Health Information

PURPOSE: The purpose of this School of Nursing Operating Policy and Procedure (HSC 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 HSC OP became effective April 14, 2003. It will be reviewed on November 1 annually by the TTUHSC School of Nursing Coordinating Council with recommendations for revisions forwarded to the Dean 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 of health information and electronic health care transactions, which are contained in 45 CFR Parts 160, 162 and 164.
   b. “Health Insurance Portability and Accountability Act Committee” or “HIPAA Committee” is the committee established by the President to provide oversight of TTUHSC compliance HIPAA and applicable state laws governing the use, storage and disclosure of Protected Health Information (PHI).
   c. “Institutional Privacy Officer” means the individual responsible for overseeing compliance with the privacy provisions of HIPAA (Standards for Privacy of Individually Identifiable Health Information/Security Standards, 45 CFR Parts 160 and 164) and applicable state laws.
   d. “Institutional Security Officer” means the individual 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.
   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” means individually identifiable health information that is transmitted by electronic media (i.e., internet, extranet, leased lines, dial-up lines, private networks, flash drives, CD, etc.) or maintained in electronic media (hard drives, magnetic tape/disk, CD, digital memory card, etc.).
   g. For purposes of HIPAA, TTUHSC has designated itself a hybrid entity and the health care components shall be designated by the HIPAA Committee by policy and has the right to add and delete health care components based on the components performance of covered functions under HIPAA.

2. Obligations of School of Nursing Faculty, Staff, and Students
   The School of Nursing adheres to Texas Tech University Health Sciences Center OP 52.02 Privacy and Security Health Information Policy http://www.ttuhsc.edu/hsc/op/op52/op5202.pdf. The School of Nursing 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. **TTUHSC School of Nursing Student Guidelines**  
**Confidentiality/Health Insurance Portability and Accountability Act of 1996 (HIPAA)**

The SCHOOL OF NURSING is dedicated to ensuring each student is current in issues as they relate to nursing practice and research. One such regulation includes the Health Insurance Portability and Accountability Act (HIPAA).

a. Each student is required to provide proof of education in HIPAA training.
b. The training requirements vary by program; the student receives information regarding HIPAA training and is asked to sign a Confidentiality Agreement prior to the beginning of the initial semester of enrollment.
c. Proof of training is kept electronically and only accessible to the School of Nursing Student Affairs Office and the TTUHSC Privacy Officer.
d. Those who cannot show proof are not allowed to attend clinical.
e. Release of confidential information (including verbal communications, written communications or electronic communications with or about patients or involving patient health information to anyone who does not need the information for treatment, payment or health care operation) is a cause for dismissal from the School.
f. Certificates of compliance are not transferable from another institution because HIPAA certification is institution specific. Thus, all students must take the TTUHSC HIPAA training and provide evidence of compliance certification.

4. **TTUHSC HIPAA Privacy and Security Officers**

a. Privacy. TTUHSC has designated an Institutional Privacy Officer who shall have responsibility for development and implementation of HIPAA privacy policies approved by the HIPAA Committee, provision of initial and on-going HIPAA Privacy training, monitoring use and disclosure of PHI and investigation of HIPAA privacy concerns/complaints. Each Regional campus shall designate a Regional Privacy Officer who shall assist the Institutional Privacy Officer in carrying out these responsibilities. The Institutional Privacy Officer shall serve as the Regional Privacy Officer for the Lubbock and Abilene campuses.
b. Security. TTUHSC has designated an Institutional Security Officer who shall have responsibility for development and implementation of HIPAA security policies approved by the HIPAA Committee, provision of initial and on-going HIPAA Security training, monitoring security of TTUHSC electronic PHI and investigation of HIPAA security concerns/complaints.
c. The Institutional Privacy and Security Officers shall work collaboratively to encourage and foster compliance with HIPAA Privacy and Security laws and regulations as well as related TTUHSC policies.

5. **TTUHSC HIPAA Committee**

a. Establishment of HIPAA Committee. The President shall establish and maintain 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 this Policy, shall each be considered a “medical committee” as defined under Texas Health and Safety Code § 161.031(a), and/or other applicable state and federal statutes. All documents generated by the HIPAA Committee, submitted to the HIPAA Committee 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. TTUHSC HIPAA Committee Membership. The HIPAA Committee shall consist of the following voting members:

- Institutional Compliance Officer
- Institutional Privacy Officer
- Institutional Security Officer
- Regional Privacy Officers from each campus
- IDX (Internet Data Exchange) Representative
- Human Resources Representative
- Representative from each Clinical School (Medicine, Nursing, Allied Health, and Pharmacy)
- General Counsel (ex-officio, without vote)

The Institutional Compliance Officer shall serve as the chair of the HIPAA Committee.

c. Responsibilities. The HIPAA Committee shall:

- Review, approve, and maintain HIPAA Privacy and Security policies (these shall be posted on the TTUHSC HIPAA Privacy and Security websites);
- Provide oversight of HIPAA Privacy and Security training;
- Provide guidance and oversight of HIPAA Privacy and Security monitoring activity conducted by the Institutional Privacy Officer and Institutional Security Officer;
- Review reports of investigations of concerns and/or complaints related to HIPAA Privacy and/or Security compliance and confirm that appropriate corrective action has been taken to minimize the risk of similar non-compliance in the future;
- Appoint subcommittees consisting of TTUHSC faculty, staff or students to provide guidance on specific HIPAA Privacy and Security matters.

In order to meet its responsibilities, the Committee may seek input from members of TTUHSC community who have expertise in specific areas.

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

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.