TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSC OP: 52.13, **HIPAA Business Associate Agreement Policy**

PURPOSE: The purpose of this Health Sciences Center Operating Policy and Procedure (HSC OP) is to provide guidance to identify Business Associates (BAs) and obtain written assurances from those BAs in order for TTUHSC EP to comply with the Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) and their implementing regulations.

REVIEW: This HSC OP will be reviewed in June of each even-numbered year (ENY) by the Office of General Counsel, the Institutional Privacy Officer (IPO), Institutional Security Officer (ISO), and Institutional Compliance Officer (ICO), with recommendations for revisions submitted to the HIPAA Privacy and Security Committee.

POLICY/PROCEDURE:

1. **Defined Terms.** The following terms are defined as:

   a. **Breach** means an unauthorized acquisition, access, Use or Disclosure of Protected Health Information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. 45 CFR 164.402.

   b. **Business Associate (BA)** means a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involves access by the business associate to protected health information. This includes creates, receives, maintains, or transmits protected health information. 45 CFR 160.103.

   c. **Contracts** mean written contracts or agreements which shall be executed whenever TTUHSC EP enters into a binding agreement with another party which involves any material consideration. Contracts are construed to include, but not be limited to agreements, cooperative agreements, memorandums of understanding, interagency contracts, grants, loans, easements, licenses, leases, permits and restrictions on acceptances of gifts and bequest. Other parties include, but are not limited to: federal, state and local agencies, nonprofit organizations, private businesses, partnership and individuals. All contractual arrangements (verbal or written) must be documented and processed for signature in accordance with HSC OP 54.01, Contracting Authority and Policy, and HSC OP 54.02

   d. **Business Associate Agreement (BAA) means a TTUHSC EP approved BAA, or other written agreement reviewed and accepted by the TTUHSC EP IPO.**

   e. **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 164.504

   f. **Covered Entity in the Texas Health and Safety Code 181.001** means any person who:

      1) 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;

2) Comes into possession of protected health information;
3) Obtains or stores protected health information; or
4) Is an employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits protected health information.

g. **Designated Record Set** means a group of records maintained by or for Covered Entity that is used, in whole or part, to make decision about individuals, or that is a provider's medical and billing records about individuals or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems. 45 CFR 164.501.

h. **Disclose** means, with respect to Protected Health Information, the release or transfer of, provision of access to, or divulging in any other manner such information outside the entity holding the information. 45 CFR 160.103.

i. **Electronic Protected Health Information** (hereinafter EPHI) shall have the same meaning as defined in 45 CFR 160.103.

j. **HHS** means the U.S. Department of Health & Human Services.

k. **Individual** means the person who is the subject of protected health information as defined in 45 CFR 160.103, and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g) and applicable Texas law.

l. **Privacy Rule** means the Standards for Privacy of Individually Identifiable Health Information in 45 CFR Parts 160 and 164.

m. **Protected Health Information (PHI)** means any individually identifiable health information in any form, including information related to payment for health services provided by Covered Entity. 45 CFR 160.103.

n. **Required by Law** means a mandate contained in law that compels an entity to make use or disclosure of protected health information (PHI) and that is enforceable in a court of law. 45 CFR 164.103 and/or applicable Texas laws and regulations.

o. **Secretary** means the Secretary of the U.S. Department of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated. 45 CFR 160.103.

p. **Security Incident** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. 45 CFR 164.304.

q. **Security Rule.** The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. 45 CFR Part 160, 162, and Subparts A and C of Part 164.

r. **Subcontractor** means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate. 45 CFR 160.103.

s. **Unsecured Protected Health Information** means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary. 45 CFR 164.402

t. **Use** means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. 45 CFR 160.103

2. **Policy**

a. An approved BAA shall be signed by a BA and an authorized TTUHSC EP official **before** a BA has access to, creates, receives, maintains, transmits or discloses TTUHSC EP's PHI/EPHI. Each TTUHSC EP contract manager is responsible for identifying BAs and obtaining a BAA. See Attachment B, Decision Tree, to determine whether a proposed contractual arrangement creates a BA relationship. If it is not clear whether a Contract creates a BA relationship, refer the Contract for review to the TTUHSC EP Purchasing Department, Contracting Office, or Institutional Privacy Officer.

b. Exceptions to the Requirement for a BAA. A BAA is not required in the following situations:

1) disclosure of PHI/EPHI for treatment purposes;
2) disclosures to a patient's insurer for payment purposes;
3) with members of TTUHSC EP's organized health care arrangements;
4) with members of TTUHSC EP's workforce;
5) private or public couriers (i.e., US Post Office, Fed Ex);
6) disclosures of a Limited Data Set (however a Data Use Agreement is required and should be submitted to the IPO);
7) disclosures to researchers for research purposes, provided that appropriate consent has been obtained from research subjects or a Waiver of Authorization has been obtained from the Institutional Review Board acting as the Privacy Board;
8) disclosures of PHI/EPHI between TTUHSC EP and affiliated training institutions as necessary to carry out training and education programs, as well as to meet the accreditation requirements of each institution;
9) Disclosures to a financial institution for the purpose of processing consumer-conducted financial transactions by debit, credit, or other payment cared, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for payment for health care or health plan premiums.

3. **Business Associate Agreement for Business Associates of TTUHSC EP.**

a. Approved BAA Template. The TTUHSC EP HIPAA Privacy and Security Committee (See HSC OP 52.02) adopted a Business Associate Agreement tem plate (TTUHSC EP BAA template) that meets HIPAA and HITECH requirements. This Committee is responsible for amending and/or updating the TTUHSC EP BAA Template as needed.

b. Use and Completion of TTUHSC EP BAA Template. Each TTUHSC EP Department, division, or operating unit shall utilize the TTUHSC EP BAA Tem plate (Attachment A to this HSC OP) and complete Section II.A. of this Template. If the other party provides a Contract with business associate language imbedded within the Contract, the TTUHSC EP BAA Tem plate shall be presented to the other party in place of the business associate language which shall be removed from the Contract.

c. Negotiation of BAA.

i) *Minor Modifications.* In the event a BA desires to make a minor modification of the terms of the TTUHSC EP BAA Tem plate which would not affect HIPAA compliance, the Purchasing Department and/or Contracting Office has the authority to negotiate with the BA, using discretion in making any such modifications.

ii) *Other Modifications.* If the requested modification is not minor in nature and/or would affect HIPAA compliance, the request will be brought to the IPO, who may seek guidance from the ICO and/or Office of General Counsel.

d. Maintenance of ex ecuted BAAs. The Purchasing Department and Contracting Office shall employ a tracking system to keep a record of the execution of all BAA by uploading all BAAs.

e. Minimum Necessary. Any disclosures of PHI/EPHI to a BA under a BAA must be limited to the minimum necessary to accomplish the intended purpose of the disclosure, use or access. Under a BAA, the BA must request only information that is the "minimum necessary", and therefore TTUHSC EP may reasonably rely on a BA's request as meeting the minimum necessary standards.

f. Authority to Sign BAA on Behalf of TTUHSC EP. Only those individuals with authority delegated in accordance with Texas Tech University System Regents' Rules have authority to sign a BAA or other written contract evidencing a BAA. (See HSC OP 54.01.) All BAA's shall be routed through the TTUHSC EP Contract Office or Purchasing Department for signature.

4. **Breach of Business Associate Agreement by Business Associate**

Any use or disclosure of PHI/EPHI by a BA that is not provided for under a BAA shall immediately be reported to the TTUHSC EP Institutional Privacy Officer (IPO) and/or Information Security Officer (ISO). The IPO and/or ISO, as applicable, will investigate the breach and take all necessary actions to cure the breach or end the violation. If a breach cannot be cured or ended, the following steps apply in any order.

a. Terminate the Contract. The Contract for services or products between TTUHSC EP and a BA shall be terminated through the TTUHSC EP Purchasing Department or Contracting Office. If termination of the Contract is not feasible, this shall be immediately reported to the ICO.

b. Report to ICO. At any time a breach may be referred to the TTUHSC EP ICO for review and action.

c. Mitigate. The IPO and/or ISO, in cooperation with applicable departments, divisions, or operating units shall mitigate, to the extent practicable, any harmful effect known to TTUHSC EP arising from a disclosure of PHI/EPHI in violation of the BAA, TTUHSC EP policies and procedures, or HIPAA and HITECH regulations.

5. **Business Associate Agreement Where TTUHSC EP is the Business Associate.**

a. BAA. BAAs from third parties requesting that TTUHSC EP sign as the BA **shall be** forwarded to the IPO for review before execution of the agreement or Contract.

b. Notification of Breaches by TTUHSC EP. If TTUHSC EP is acting as a BA and has actual knowledge of a breach, or violation by the TTUHSC EP workforce, the TTUHSC EP IPO and/or ISO shall, upon completion of an investigation of credible evidence of violation, notify the other party (Covered Entity) as required by law.

6. **Right to Change Policy.**

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