TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 52.13, HIPAA Business Associate Agreement Policy

PURPOSE: The purpose of this Texas Tech University Health Sciences Center El Paso (TTUHSC El Paso) Operating Policy and Procedure (HSCEP OP) is to provide guidance to identify Business Associates (BAs) and obtain written assurances from those BAs in order for TTUHSC El Paso 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 HSCEP 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:

I. Defined Terms. The following terms are defined as:

A. **Breach** means an unauthorized acquisition, access, use, or disclosure of protected health information (PHI) 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 PHI. This includes creating, receiving, maintaining, or transmitting PHI. 45 CFR 160.103.

C. **Contracts** mean written documents or agreements which shall be executed whenever TTUHSC El Paso enters into a binding agreement with another party that 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 acceptance of gifts and bequests. Other parties include, but are not limited to: federal, state and local agencies, nonprofit organizations, private businesses, partnerships and individuals. All contractual arrangements (verbal or written) must be documented and processed for signature in accordance with HSCEP OP 54.01, Contracting Authority and Policy, and HSCEP OP 54.02

D. **Business Associate Agreement (BAA)** means a TTUHSC El Paso business associate agreement (BAA). A Contract between a covered entity and an individual or organization that will receive access to, transmit, or store Protected Health Information as part of its services for the covered entity.

E. **Covered Entity (CE)** means a health plan, a health care clearinghouse, or a healthcare 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 PHI;
2) Comes into possession of PHI;
3) Obtains or stores PHI; or
4) Is an employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits PHI.

G. **Designated Record Set** means a group of records maintained by or for a CE that is used, in whole or part, to make decisions about individuals, or that is a provider's medical and billing record 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 PHI, 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 PHI 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 a 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 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' EPHI 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 EPHI. 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

II. Policy

A. An approved BAA shall be signed by a BA and an authorized TTUHSC El Paso official **before** a BA has access to, creates, receives, maintains, transmits or discloses TTUHSC El Paso's PHI/EPHI. Each TTUHSC El Paso 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 El Paso Purchasing Department, Contracting Office, or IPO.

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 El Paso's organized health care arrangements;
4) with members of TTUHSC El Paso'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 through the contracting system);
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 El Paso 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 card, clearing checks, initiating or processing electronic funds transfers, or conducting any other activity that directly facilitates or effects the transfer of funds for payment for health care or health plan premiums.

III. Business Associate Agreement for Business Associates of TTUHSC EP.

A. Approved BAA Template. The TTUHSC El Paso HIPAA Privacy and Security Committee (See HSCEP OP 52.02) adopted a BAA template (TTUHSC El Paso BAA template) that meets HIPAA and HITECH requirements. This Committee is responsible for amending and/or updating the TTUHSC El Paso BAA Template as needed.

B. Use and Completion of TTUHSC El Paso BAA Template. Each TTUHSC El Paso department, division, or operating unit shall utilize the TTUHSC El Paso BAA Template (Attachment A to this HSCEP OP) and complete Section II.A. of this template when a BA will have access to, create, receive, maintain, store, transmit, or disclose TTUHSC El Paso's PHI/EPHI. If the other party provides a contract with BA language embedded within the contract, the TTUHSC El Paso BAA Template shall be presented to the other party in place of the BA language, which shall be removed from the contract.

C. Negotiation of BAA.

1) *Minor Modifications.* In the event a BA desires to make a minor modification of the terms of the TTUHSC EP BAA Template which would not affect HIPAA compliance, the Purchasing Department and/or Contracting Office will submit the agreement (utilizing the contracting system) to Institutional Compliance and the Legal Department to approve or reject any such modifications.

2) *Other Modifications*. If the requested modification is not minor in nature and/or would affect HIPAA compliance, the request (utilizing the Contracting System) will be brought to the ICO, and/or the Office of General Counsel

D. Maintenance of executed BAAs. The Purchasing Department and Contracting Office shall utilize the contracting system to keep a record of the execution of all BAAs by uploading all BAAs into the contracting system.

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 El Paso may reasonably rely on a BA's request as meeting the minimum necessary standards.

F. Authority to Sign BAA on Behalf of TTUHSC El Paso. 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 HSCEP OP 54.01.) All BAA's shall be routed through the TTUHSC El Paso Contract Office or Purchasing Department for signature.

IV. 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 El Paso IPO and/or 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 El Paso and a BA shall be terminated through the TTUHSC El Paso 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 El Paso 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 El Paso arising from disclosure of PHI/EPHI in violation of the BAA, TTUHSC El Paso policies and procedures, or HIPAA and HITECH regulations.

V. Business Associate Agreement Where TTUHSC El Paso is the Business Associate.

A. BAA. BAAs from third parties requesting that TTUHSC El Paso 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 El Paso. If TTUHSC El Paso is acting as a BA and has actual knowledge of a breach, or violation by the TTUHSC El Paso workforce, the TTUHSC El Paso IPO and/or ISO shall, upon completion of an investigation of credible evidence of the violation, notify the other party (covered entity) as required by law.

VI. Right to Change Policy.

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