Complaints, Breaches and Sanctions	**Policy 5.2**
Breach Risk Assessment and Notification	**Effective Date: December 23, 2015** **Revised: June 1, 2016**
References: http://www.hhs.gov/ocr/hippa;	

Policy Statement

This HIPAA Privacy Policy and Procedure is to establish a standard of how to handle breach notification of sensitive data according to HIPAA federal (§ 45 CFR 164) and state privacy laws (TEX BC. Code § 521).

Definitions

Refer to HPP 1.1 for Glossary of HIPAA Terms

See *Old/New HIPAA Policy Number Cross Reference Chart*

Procedure

1. **Definitions.**

a. Breach means the acquisition, access, use or disclosure of Protected Health Information (PHI) in a manner not permitted under the HIPAA Privacy Rules which compromises the security or privacy of the PHI. (§ 45 CFR 164.402.) The following shall not constitute a Breach:

(1) Any unintentional acquisitions, access or use of PHI by a Workforce Member or Business Associate if it was made in good faith, within the scope of such individual's authority and does not result in further unauthorized use or disclosure of the PHI;

(2) Any inadvertent disclosure by a person authorized to access PHI by TTUHSC to another person authorized to access PHI within TTUHSC and/or organized health care arrangements in which TTUHSC participates, provided there is no further unauthorized use or disclosure of the PHI; and

(3) A disclosure of PHI in which TTUHSC has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the PHI.

b. Breach of System Security means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt data. TEX BC. Code § 521.053.

c. Health Insurance Portability and Accountability Act of 1996 (HIPAA) is 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.

d. Health Information including Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) (§ 45 CFR 160.103) means information, including demographic information, that:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse;

(2) Relates to the past, present, or future physical or mental condition of a patient, the provision of health care to a patient, or the past, present, or future payment for the provision of health care to a patient; and

(3) Identifies the patient (or there is a reasonable basis to believe the information can be used to identify the patient).

e. Unsecured PHI is PHI in any medium that is not maintained in a form which has been identified by HHS as a method for rendering the PHI unusable, unreadable or indecipherable to unauthorized individuals though the use of a technology or methodology specified in guidance issued by HHS. (§ 45 CFR 164.402) As of the effective date of this Policy, PHI will be deemed unusable, unreadable, or indecipherable if the PHI is either:

(1) Encrypted using a process identified and tested by the National Institute of Standards and Technology ("NIST") to meet this standard. For data at rest, such process shall be consistent with NIST Special Publication 800-11. For data in motion, such process shall be consistent with NIST Special Publication 800-52, 800-77, or 800-113, or other processes which are Federal Information Processing Standards 140-2 validated; or

(2) Destroyed such that the PHI cannot be read or reconstructed. For PHI maintained in an electronic form, the PHI must be destroyed in a manner consistent with NIST Special Publication 800-88. (Note: Redaction is not an acceptable method for destroying PHI.)

f. Personal Identifying Information means information that alone or in conjunction with other information identifies an individual (TEX BC. Code § 521.002.), including an individual's:

(1) Name, Social security number, date of birth, or government-issues identification number;
(2) Mother's maiden name;
(3) Unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
(4) Unique electronic identification number, address, or routing code;
(5) Telecommunication access device as defined by Section 32.51, TX Penal Code.

g. Sensitive Personal Information (TEX BC. Code § 521.002) means:

a. An Individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

(i) Social security number;
(ii) Driver's license number or government-issued identification number; or
(iii) Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or

b. Information that identifies an individual and relates to:

(i) The physical or mental health or condition of the individual;
(ii) The provision of health care to the individual; or
(iii) Payment for the provision of health care to the individual.

h. 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.

2. **Reporting an Actual or Suspected Impermissable Use and Disclosure of PHI.**

a. The TTUHSC Institutional Privacy Officer (IPO) shall be notified of all potential unlawful or unauthorized access to, use of, or disclosure of potentially identifiable patient medical information as soon as detected.

b. If a breach of unsecured PHI occurs at or by a BA or its subcontractor, the BA is obligated to notify HSC within the specified time frame and fulfill other obligations per the BAA.

c. If Privacy Officer determines a "Data Breach Team" is needed, it shall

consist of, at minimum:

(1) Privacy Officer(s) and/or his/her designees.
(2) Security Officer and/or his/her designees.
(3) Human Resources Director or representative.
(4) Office of General Counsel or representative.
(5) Marketing and Communication representative.
(6) Members of the HSC Privacy and Security Committee.
(7) Others as determined necessary by the Privacy and Security Committee.

3. **Determining Whether a Breach of Unsecured PHI Occurred.**

Upon receiving a report of any actual or suspected unauthorized use or disclosure of PHI as defined in Section 1, the Privacy Officer shall immediately investigate the incident to determine if the incident resulted in a Breach of Unsecured PHI. This investigation shall include completion of the Breach Risk Assessment form. This assessment will include:

1. In what form was the PHI disclosed?
2. Nature and Extent: What type of PHI was disclosed?
3. The unauthorized person who used the PHI or to whom the disclosure was made?
4. Circumstances of Breach or Disclosure;
5. Disposition: What happened to the information after the initial disclosure; was PHI acquired or viewed?
6. Additional controls to mitigate risk to the PHI

Based on the risk assessment, if it is determined the disclosed information was not compromised, TTUHSC through its Privacy Officer, in consultation with the Data Breach Team, shall conclude that no Breach of Unsecured PHI has occurred and that no notification is required under this operating policy.

4. **Procedure if No Breach of Unsecured PHI Occurred.**

If, based on the steps above, TTUHSC determines that the incident did not constitute a Breach of Unsecured PHI; the TTUHSC Privacy Officer shall document such conclusion and the rationale for such conclusion and shall maintain such documentation and any additional supporting documents for a period of at least six (6) years from the determination.

5. **Procedure If a Breach of Unsecured PHI Occurred.**

If TTUHSC determines that a Breach of Unsecured PHI occurred, TTUHSC shall provide notice of the Breach and maintain documentation of such notice as follows:

c. Notice to Individual(s). Unless contrary instructions from law enforcement are received (see Section 5.(d) below), the Privacy Officer will provide written

notice of the Breach to each individual whose Unsecured PHI has been Breached, or is reasonably believed to have been Breached, as follows:

a. *Content of Notice*. The notice shall be written in plain language and shall contain the following information (Attachment A):
b. Brief description of the incident, including the date of the Breach and the date of the discovery of the Breach, if known,
c. Description of the types of Unsecured PHI involved in the Breach (rather than a description of the specific PHI),
d. Any steps the patient should take to protect himself or herself from harm resulting from the Breach,
e. Brief description of what TTUHSC is doing to investigate the Breach, to mitigate the harm to individuals and to protect against future occurrences, and
f. Contact procedures for the individual to ask questions or learn additional information, which may include a toll-free telephone number, an e-mail address, website or postal address.
g. Attachment B Sample notification letter

2. *Substitute Notice*. If there is insufficient or out-of-date contact information for an individual, as soon as reasonably possible after the determination of a Breach, TTUHSC shall provide notice reasonably calculated to reach individuals as described below:

   a. If there is insufficient or out-of-date contact information for fewer than ten (10) individuals, notice may be provided by e-mail, telephone, or other means.
   b. If there is insufficient or out-of-date contact information for ten (10) or more individuals, notice shall (1) be in the form of either a conspicuous posting for ninety (90) days on TTUHSC website home page or conspicuous notice in major print or broadcast media in geographic areas where the affected individuals are likely reside, and (2) include a toll-free number that remains active for at least ninety (90) days so that the individual can learn whether his or her Unsecured PHI was included in the Breach.
   c. Substitute notice need not be provided if the affected individual is deceased and TTUHSC has insufficient or out-of-date contact information for the next-of-kin or personal representative for the individual.

3. *Law Enforcement Delay*. If a law enforcement official informs TTUHSC that the notice to individuals, HHS or the media described above would impede a criminal investigation or cause damage to national security, TTUHSC shall:

   a. If the statement is in writing and specifies the time for which a delay is required, delay the notification for the specified time; or
   b. If the statement is made orally, document the statement, including

the identity of the official, and delay the notification for no longer than thirty (30) days from the date of the oral statement, unless during that thirty (30) day time period, the official provides a written statement requiring a different notification timeframe.

d. Timing of Notice. The notice shall be provided promptly and **no later than sixty (60) days** after TTUHSC discovers the Breach. The Breach is considered to be discovered on the first day on which the Breach is known, or would have been known by exercising reasonable diligence to any person who is a Workforce Member or agent of TTUHSC (other than the person committing the Breach.)

e. Manner of Notice. The notice shall be sent by first-class mail addressed to the patient's last known address. Notice may be sent electronically if the individual has agreed to receive electronic notice and the agreement has not been withdrawn. If TTUHSC knows that the individual is deceased, TTUHSC shall provide written notice to the next-of-kin or personal representative of such individual if TTUHSC has addressed for them. Notice may be provided in one or more mailings as additional information becomes available. If TTUHSC determines there is potential for imminent misuse of Unsecured PHI in connection with a breach, TTUHSC may provide information regarding the breach to individuals by telephone or other means, as TTUHSC determines to be appropriate, in addition to provide the required written notice as described above.

6. **Notice to Secretary of HHS.**

Unless contrary instructions from law enforcement are received, in addition to notifying individuals as described above, TTUHSC Institutional Privacy Officer shall notify HHS, i.e. "Secretary" of the Breach of Unsecured PHI. Such notification shall be provided as follows:

a. If the Breach involves 500 or more individuals, TTUHSC shall notify HHS of the Breach contemporaneously with providing the notice to the individual and in a manner specified by HHS on its website.

b. If the Breach involves less than 500 individuals, TTUHSC shall maintain a log or similar documentation of the Breach and shall provide the required documentation to HHS **no later than sixty (60) days** after the end of each calendar year in the manner specified by HHS on its website.

7. **Notice to Media.**

Unless contrary instructions from law enforcement are received, if a Breach involves more than 500 residents of a state or jurisdiction, in addition to notifying the individuals and HHS, TTUHSC also shall notify prominent media outlets serving the state or jurisdiction. Such notice shall be provided promptly and in no case later than sixty (60) calendar days after discovery of the Breach. The

notice shall contain the same information included in the notice to the patient.

8. Notice to Consumer Reporting Agency (Texas Only).

If an entity is required to notify at one time more than 10,000 persons of a breach of system security, the entity shall also notify each consumer reporting agency, as defined by 15 U.S.C. Section 1681a, that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices. The person shall provide the notice required by this subsection without unreasonable delay. § TEX BC. Code 521.053.

9. Documentation of Breach Notice.

TTUHSC shall maintain the documentation related to the provision of notice to patients, HHS, the media, risk assessment, if applicable, and any communication from law enforcement related to the delayed notification, if applicable, for at least six (6) years from the date notice was provided.

Knowledge of a violation or potential violation of this policy must be reported directly to a Regional Privacy Officer, the Institutional Privacy Officer or to the employee Compliance Hotline at (866) 294-9352 or www.ethicspoint.com under HSC.

Approval Authority

Questions regarding this policy may be addressed to the Regional Privacy Officer (Amarillo, Permian Basin Lubbock), the Institutional Privacy Officer, or the Institutional Compliance Officer.

Responsibility and Revisions

This policy will be reviewed on each even-numbered year by the (ENY) by the Institutional Privacy Officer, and the HIPAA Privacy and Security Committee, but may be amended or terminated at any time

TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER™
Office *of* Institutional Compliance

Attachment A
3601 4th Street, MS 8165
Lubbock, Texas 79430
(806) 743-3949

SAMPLE BREACH NOTIFICATION LETTER

DATE

NAME
ADDRESS
CITY, STATE ZIP

Dear Mr./Mrs./Ms.

This letter is to inform you of a recent breach of your personal information from Texas Tech University Health Sciences Center (TTUHSC). We became aware of this breach on DATE which occurred on or about DATE. The breach occurred as follows:

A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

B. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).

C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.

D. A brief description of what TTUHSC is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.

E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, website, or postal address.]

Other Optional Considerations:

To help avoid your information being used inappropriately, TTUHSC will cover the cost for one year for you to receive credit monitoring. To take advantage of this offer, we also recommend that you immediately take the following steps:

- Call the toll-free numbers of anyone of the three major credit bureaus (below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge.
    - **Equifax**: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241.
    - **Experian**: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013.
    - **TransUnion**: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

- Order your credit reports. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.
- Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information.

TTUHSC is committed to safeguarding your personal information and using it in an appropriate manner, and is taking steps to rectify the situation.

You may call us toll-free number at 1-877-272-0570 during regular business hours with questions about the breach of your personal information.

Also, there is a section on the TTUHSC website (www.ttuhsc.edu) with updated information and links to websites that offer information on what to do if your personal information has been compromised.

Sincerely,

Institutional Privacy Officer

cc: Secretary of Health and Human Services