Texas A&M School of Public Health
HIPAA Privacy Compliance Manual
For Researchers

Final: Approved by the SPH Executive Committee, 01/12/2016
Table of Contents

INTRODUCTION ...................................................................................................................................... 3
PURPOSE ..................................................................................................................................................... 4
LEGAL STATUS OF TEXAS A&M SCHOOL OF PUBLIC HEALTH ........................................................... 4
HIPAA COMPLIANCE FOR RESEARCH PURPOSES ............................................................................ 4
HIPAA’S 18 PHI IDENTIFIERS ............................................................................................................... 5
LIMITED & DE-IDENTIFIED DATA SETS, WAIVER OF HIPAA AUTHORIZATION .................................... 6
HIPAA COMPLIANCE FLOWCHART........................................................................................................ 7
SPH MONITORING OF PROTOCOLS FOR HIPAA COMPLIANCE: ....................................................... 8
UTILIZATION OF CLOUD SERVERS FOR STORAGE AND FILE SHARING: ....................................... 8
UTILIZATION OF PHI IN RESEARCH BY AUTHORIZATION: ................................................................. 8
UTILIZATION OF PHI IN RESEARCH WITH A WAIVER OF AUTHORIZATION ....................................... 9
DATA ANALYSIS PREPARATORY TO RESEARCH ............................................................................... 10
PHI OF DECEDEANTS ............................................................................................................................ 10
TRACKING OF PHI DISCLOSURES ........................................................................................................ 10
REVOCAITION OF PHI OR IRB AUTHORIZATION BY PARTICIPANT .................................................. 11
STORAGE AND SECURITY FOR DATA CONTAINING PHI .................................................................. 12
RESEARCH COMMENCED PRIOR TO HIPAA’S EFFECTIVE DATE APRIL 14, 2003 ............................ 12
WAIVER OF CONSENT REQUIREMENT BY IRB FOR RESEARCH PRIOR TO APRIL 14, 2003 ........ 13
FORMS FOR RESEARCHERS ................................................................................................................. 14
TAMHSC BUSINESS ASSOCIATE AGREEMENT ................................................................................ 15
TAMHSC DATA USE AND CONFIDENTIALITY AGREEMENT ............................................................... 25
CASE STUDY AUTHORIZATION FORM ................................................................................................. 27
DATA USE PREPARATORY-TO-RESEARCH ............................................................................................ 29
CERTIFICATION & GUIDANCE .............................................................................................................. 29
NOTICE OF PRIVACY PRACTICES ACKNOWLEDGEMENT ................................................................ 31
POLICIES & STANDARD OPERATING PROCEDURES ........................................................................ 32
PRIVACY OFFICER OPERATING PROCEDURE .................................................................................. 33
HIPAA COMPLIANCE AND PRIVACY OFFICER JOB DESCRIPTION ................................................ 35
COMPLAINT OPERATING PROCEDURE ............................................................................................. 37
HIPAA PRIVACY & COMPLIANCE COMPLAINT FORM .................................................................. 38
WORKFORCE TRAINING OPERATING PROCEDURE FOR HIPAA .................................................... 39
HIPAA EMPLOYEE TRAINING RECORD ............................................................................................. 40
OPERATING PROCEDURE FOR DISCIPLINARY ACTION RELATING TO ............................................... 41
SANCTIONS RECORD ........................................................................................................................... 44
OPERATING PROCEDURE FOR BUSINESS ASSOCIATES ................................................................ 45
OPERATING PROCEDURE FOR CHANGES TO POLICIES AND PROCEDURES ................................ 48
OPERATING PROCEDURE FOR CONFIDENTIALITY OF PHI ............................................................... 49
CONFIDENTIALITY AGREEMENT ......................................................................................................... 52
BREACH NOTIFICATION OPERATING PROCEDURE ........................................................................ 53
FURTHER INFORMATION ........................................................................................................................ 59
INTRODUCTION:

This TEXAS A&M SCHOOL OF PUBLIC HEALTH HIPAA PRIVACY COMPLIANCE POLICY MANUAL is designed to assist A&M School of Public Health Researchers in complying with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") privacy standards and the Health Information Technology for Economic and Clinical Health Act OF 2009 ("HITECH") (collectively referred to as “HIPAA” in this Manual) and the Texas Medical Privacy Act, (HB 300). TEXAS A&M SCHOOL OF PUBLIC HEALTH firmly believes that any SPH faculty member, student, employee or Business Associate entrusted with Protected Health Information ("PHI") must treat the PHI with the utmost confidentiality.

Please note: If you, your employees, your students, or your program are providing actual services or interventions to persons, including, but not limited to, services such as counseling, health coaching, behavior training, or self-management education, then you may be covered under the full TAMHSC HIPAA regulations which may be found at http://sph.tamhsc.edu/research/hipaa/. To determine if you are covered under HIPAA please see HIPAA Flow Chart, page 7, and/or contact the SPH HIPAA Privacy Officer.

This Manual does not provide guidance as to the HIPAA security and transaction standards which may be found at http://it.tamhsc.edu/systems-security/it-security.html. Security standards are mentioned only to the extent that they overlap with the privacy standards. The following HIPAA Compliance for Researchers Manual provides policies and procedures pertaining only to research.

Emphasis is placed on:

- Distinguishing HIPAA compliance for research purposes as opposed to patient services
- Data and documentation management
- SPH audit and tracking of data used by researchers
- Allowable disclosure of PHI
- Business Associate Agreements, DUAs, and other frequently used documents
- HIPAA Training Requirements
- Operating Procedures and Procedure Documentation

Please be aware that regardless of HIPAA and state law retention of records requirements discussed in this manual, if you have any notice of a health care liability claim, you should never destroy any records or related data. If you have any questions or concerns at any time, please feel free to contact me directly at jbolin@sph.tamhsc.edu

Sincerely,

JANE N. BOLIN, RN, JD, PhD
SPH-HIPAA Compliance & Privacy Officer
PURPOSE:

HIPAA places on the Texas A&M School of Public Health a duty to protect the confidentiality and integrity of an individual's health information, including all information designated as PHI. Protecting the confidentiality of PHI is not only required by federal HIPAA and HITECH laws, but it is also required by the Texas Medical Privacy Act (Texas HB 300), as well as professional ethics, and A&M SPH accreditation requirements. HIPAA governs how health information is protected, used and disclosed, including use and disclosure for research purposes. The purpose of this manual is to set forth the policies and procedures that will be applicable to data used for evaluation and research.

LEGAL STATUS OF TEXAS A&M SCHOOL OF PUBLIC HEALTH:

Texas A&M University is an entity that has chosen hybrid status, meaning it is a single legal entity with some components, including SPH that are covered under HIPAA. The Texas A&M Health Science Center and the School of Public Health are HIPAA covered components that must comply with HIPAA.

HIPAA Affected Components and Operations are those units at Texas A&M University that have access to, or keep or maintain PHI, as defined by HIPAA, because the component falls under one of the following definitions:

- Is either a covered healthcare component (healthcare provider or a health plan),
- provides services to covered components and as such receives PHI to perform those tasks, or
- uses PHI for education or research purposes. (emphasis supplied)

HIPAA COMPLIANCE FOR RESEARCH PURPOSES

Any study or evaluation that involves health information about a human subject obtained for purposes of evaluation or research invokes some level of obligation to comply with HIPAA. HIPAA privacy and security laws are designed to protect individually identifiable health information known as protected health information (PHI), when this information is in the possession of entities subject to HIPAA, including SPH.

A full list of the 18 PHI identifiers may be found on the next page.
HIPAA’s 18 PHI Identifiers

HIPAA compliance duties apply to protected health information (PHI), falling within any of the following 18 PHI identifiers:

1. Names
2. Addresses
3. Dates
4. Telephone numbers
5. Fax numbers
6. Email addresses;
7. Social Security numbers
8. Medical record numbers
9. Health plan numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code

---

1 **Addresses** - All geographical subdivisions smaller than a state, including street address, city county, precinct, zip code, their equivalent geocodes, except for the initial three digits of the zip codes, if according to the current publicly available data from the Bureau of the Censes: (1) geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of the zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

2 **Dates** - All elements of dates (except year) for the dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.

3 **Other unique number, characteristic, or code** -- (which may identify a person),
Limited & De-Identified Data Sets, Waiver of HIPAA Authorization

If your study involves a limited data set or de-identified data, and you are not providing advice, treatment or intervention then you do not need to comply with the full set of HIPAA obligations.

**Limited Data Set:** A researcher may choose to use a limited data set, which is less restrictive and excludes mostly direct subject identifiers. For use of a limited data set, the researcher must complete a formal data use agreement, (DUA) that sets forth permitted uses and disclosures of the limited data set information with the data source.

**De-identified data** contains none of the 18 PHI identifiers. If the data does not contain any of the 18 identifiers it is considered de-identified and the data is exempt from HIPAA's requirements. However, SPH will still require researchers to provide the Office of Research with a yearly data inventory. To be completely de-identified, the data must be stripped of all direct and indirect subject identifiers.

**Waiver of HIPAA Authorization:** A&M's IRB, however, may permit the disclosure of PHI subject to HIPAA without a subject's specific prior consent or authorization, (1) if the research cannot be practically conducted without access to the PHI, and (2) the disclosure involves no more than minimal risk to the privacy of the subject. If you are requesting such a Waiver of Authorization, then you must complete the Texas A&M's Waiver of Authorization application form and submit to the IRB.

If you plan to share or disclose a subject's PHI in connection with a research study that is determined to be subject to HIPAA then the full provisions of HIPAA apply and you must first obtain the written permission of the subject prior to sharing. This permission, called an Authorization for Release of Protected Health Information, and must specify precisely what information will be released, why it is being released, and from and to whom it is being released. A template for this form is provided in the Forms and Templates section of this website, which can be accessed from the main menu. This form must be appended to the informed consent form and completed by the subject at the same time the subject completes the informed consent form. A subject cannot participate in the research if he or she does not complete the Authorization. Additionally, the investigator must maintain a detailed record of each release of health information, and this record must be accessible under certain circumstances to the subject.

Failure to comply with the SPH yearly HIPAA data audit inventory and/or HIPAA policies will result in immediate suspension of your research study and withholding of your paychecks or salary until the required inventory is filed. Repeated failure to comply will result in disciplinary action by the Dean of the School of Public Health and may result in termination of employment and/or faculty appointment.

A more detailed description of the HIPAA Privacy Rule requirements may be found at [http://sph.tamhsc.edu/research/hipaa/certification.html](http://sph.tamhsc.edu/research/hipaa/certification.html)

If HIPAA applies to your research study, any failure to comply with HIPAA will result not only in termination of your study and suspension of related research grants, but also potentially in criminal and/or civil penalties to you and A&M SPH (for an individual, penalties may be as severe as $1,500,000 or 10 years imprisonment.).
HIPAA Compliance Flowchart. The following flow-chart will help you determine if your research requires full HIPAA Compliance or whether it may be subject to exceptions.⁴

Credit: adapted from: https://www.umaryland.edu/media/umb/oaa/hrp/documents/study-tools-docs/hipaaflowchart.pdf
SPH MONITORING OF PROTOCOLS FOR HIPAA COMPLIANCE:

All research protocols must be submitted to the A&M Division of Research Institutional Review Board (IRB) for review and approval prior to commencing any study or evaluation of data containing PHI. SPH Office of Research monitors all active IRB protocols through the Office of Shared Research Services (SRS).

UTILIZATION OF CLOUD SERVERS FOR STORAGE AND FILE SHARING:

All data containing PHI must be stored on a HIPAA compliant server. This mandate includes “cloud” servers. Many researchers are not aware that very few commercial cloud servers offer HIPAA compliance assurances and many companies are not willing to sign a Business Associate Agreement (BAA), (e.g., iCloud, Dropbox and Amazon). The TAMHSC Office of Information Technology now offers a secure cloud server and file sharing software called Syncplicity. This TAMHSC Cloud server can be accessed per the following:

**Access and Use:** TAMHSC Cloud (Syncplicity), can be accessed at [cloud.tamhsc.edu](http://cloud.tamhsc.edu). It allows you to...

- Share most file types and folders with others from any device — Syncplicity keeps everyone in sync, automatically.
- Create, edit, and share Microsoft Office documents using any platform, including mobile devices.
- Break out of the box — Syncplicity lets you share any file or folder on your computer without copying them to a designated folder, like Dropbox.
- Send large files — there are no file-size limits, and no FTP hassles.

UTILIZATION OF PHI IN RESEARCH BY AUTHORIZATION:

Data that contains PHI must strictly comply with HIPAA. In order to utilize PHI in connection with research, researchers must (a) obtain written authorization from the individual who is participating as a research subject in accordance with HIPAA standards for authorization, or (b) obtain a waiver of the authorization requirement from the Institutional Review Board (IRB) in accordance with HIPAA standards for such waivers, or (c) obtain approval for such use as preparatory to research, or d) notify the IRB of such use as research on decedents’ information.

PHI obtained in accordance with this policy may be used only by and disclosed only to the principal investigator and other members of the research team identified in the research protocol application, except that further disclosure may be made (a) as specified in the authorization granted by individual from whom PHI has been obtained or allowed under a BAA or DUA; or (b) as required or permitted by the HIPAA rules or other law. Approval of the IRB is required for any disclosure request that is not within the scope of an authorization granted by the individual participating in research or as required or permitted by HIPAA rules and other law. If an authorization is required in order to utilize PHI in connection with research, the content of the authorization must comply with HIPAA rules.

Authorization may be obtained by the use of a separate authorization form, which is reviewed with and signed by the individual participating in the research protocol. A template authorization form is available at the Office for Research Protections and should be completed by the principal investigator and submitted for review and approval by the IRB.

Authorization may also be obtained by including the requisite information in an Informed Consent Form to be used with the protocol. Model provisions for inclusion of an authorization
with the Consent Form are available at http://rcb.tamu.edu/humansubjects/forms/humansubjectsforms The IRB will review the authorization provisions as part of its review of the Informed Consent Form.

Copies of the authorization must be signed by the individual participating in the research protocol and must be retained by the principal investigator for a minimum of three (3) years following completion of the study. (Ref. 45 CFR 46.115(b)). Other time limits may apply and the IRB office should be consulted in the event there are any questions.

In the event a principal investigator leaves the University during the study or prior to the end of the time period required by contract or policy, for retaining consents and waivers, the investigator will notify the SPH Office of Research and IRB and make arrangements for ongoing retention of required research documents at the University.

UTILIZATION OF PHI IN RESEARCH WITH A WAIVER OF AUTHORIZATION:

If a research protocol proposes to obtain and use PHI in research without an authorization, the principal investigator must submit a request for a waiver of the authorization requirement to the A&M IRB. In addition, depending upon the policies of individual health care providers, it may be necessary to obtain approval of the waiver from another IRB or privacy board.

An application must be in writing and be submitted with the protocol to be reviewed by the IRB. An application form for this purpose is available at http://rcb.tamu.edu/humansubjects/forms/humansubjectsforms.

A request for waiver of authorization will be reviewed by the full IRB at a regularly scheduled monthly meeting.

An application for waiver will be approved only if the IRB concludes that the criteria in the HIPAA rules have been satisfied. These include:

1. The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
   i. an adequate plan to protect the identifiers from improper use and disclosure;
   ii. an adequate plan to destroy the identifiers at the earliest opportunity consistent with the protocol, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
   iii. adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted under the HIPAA Privacy Rule.

2. The research could not practicably be conducted without the waiver or alteration; and
3. The research could not practicably be conducted without access to and use of the protected health information.

DATA ANALYSIS PREPARATORY TO RESEARCH:

Because it may be necessary for a researcher to obtain access to and review PHI in order to prepare a research protocol, HIPAA rules allow such review upon compliance with specified criteria. This provision might be used, for example, to design a research study or to assess the feasibility of conducting a study, or to identify potential participants for a study. An application for review of PHI preparatory to research must be submitted to the A&M IRB. An application form is available at the A&M Research Compliance Office web site at http://rcb.tamu.edu/humansubjects/forms

HIPAA allows data analysis preparatory to research under the following conditions:

1. The use or disclosure of the protected health information is solely to prepare a research protocol or for similar purposes preparatory to research;

2. No PHI will be removed in any manner, including by means of copying or notes, from the original source of the PHI; and

3. The PHI for which access is sought is necessary for the research purpose.

PHI OF DECEDENTS:

Principal Investigators will also need to submit an IRB application prior to engaging in research with the PHI of decedents. In order to gain access to the PHI maintained by a covered entity, principal investigators will need to demonstrate:

1. Use or disclosure sought is solely for research on the PHI of decedents;

2. Adequate documentation of the death of such individuals; and

3. PHI for which use or disclosure is sought is necessary for the purposes of the proposed research.

TRACKING OF PHI DISCLOSURES:

HIPAA rules require that a record be made of a disclosure of any personally identifiable information that is made without an authorization by the research participant. Therefore, tracking of disclosures will have to be undertaken for all disclosures if a waiver of authorization, an approval for review preparatory to research or an approval for the use of a decedent's PHI is obtained for purposes of research, and for any disclosures not previously specified in a signed authorization document. For purposes of this policy, "disclosure" means the release, transfer, provision of access to, or divulging in any other manner of PHI to any person, whether or not employed by PSU, who is not participating in carrying out the research protocol.

The following information about any disclosure must be recorded and made available upon request to the individual who is the subject of the PHI:

1. Date of disclosure;

2. Name of person/entity that received the PHI;
3. Description of what PHI was disclosed; and
4. Brief statement regarding the purpose of the disclosure.

If a research protocol requires multiple disclosures to the same outside party over a period of time, the following information is adequate:

1. For the first disclosure, all of the above must be recorded.
2. For subsequent disclosures, tracking can refer to the initial record of disclosure and should include the frequency, periodicity or the number of disclosures that will be made.
3. The date of the last disclosure must be documented.

**Large Studies with Waiver:** HIPAA rules allow a modified tracking method for research that involves the disclosure of PHI from more than 50 people and for which authorization has been waived. In this instance it is unnecessary to maintain a list of the specific persons about whom PHI has been disclosed, but the following information must be available upon the request of any individual whose information may have been included.

1. The name and description of all protocols involving 50 or more people for which authorization has been waived, including the purpose of these and criteria for selecting records, if the individual's information may have been included;
2. Brief descriptions of types of PHI disclosed;
3. Dates or time periods during which disclosures occurred;
4. Contact information (name, address, telephone number) for sponsors and recipient researchers; and
5. Statement that a specific individual's PHI may or may not have been disclosed for a particular protocol or research activity.

In addition, the researcher must also assist in contacting the sponsor and recipient researcher if it is reasonably likely that an individual's PHI was disclosed to them.

The principal investigator must submit all tracking of disclosure information to the IRB, and the principal investigator must retain the tracking information for no less than three (3) years.

**REVOCATION OF PHI or IRB AUTHORIZATION BY PARTICIPANT:**

HIPAA rules allow a subject to revoke a prior authorization to use or disclose PHI for purposes of research. Participant requests for the revocation of authorization must be requested in writing to the principal investigator. Researchers must honor this request, except to the extent the researcher has already relied on the authorization. Researchers may continue utilizing PHI that was obtained prior to the time the individual revoked his or her authorization, as necessary to maintain the integrity of the research study. In addition, use or disclosure of identifiable information previously obtained is permitted for purposes such as accounting for the participant's withdrawal, reporting adverse events, or complying with investigations.
STORAGE AND SECURITY FOR DATA CONTAINING PHI:
The following apply to storage and security for data, including surveys, focus group notes, or other “hard copy” documents, containing any of the 18 PHI identifiers:

Researchers are responsible for ensuring that all data containing PHI is securely protected from unauthorized disclosures. Researchers must take precautions to securely maintain and dispose of PHI, as described in Policy AD22. (See related policies AD20 and AD23.)

Researchers are responsible for ensuring secure transfer of data containing PHI.

If transmitting data electronically, or transferring data by portable device, researchers should ensure that a) the data is securely encrypted; b) that the receiver of the data is the individual for whom it is intended; and b) the data remains secure until it is received by the intended receiver. Questions about the security of electronic data transfers may be directed to the Office of Information Technology at 1-800-799-7472 or helpdesk@tamhsc.edu

When sending or transferring data containing PHI via ground mail or delivery services, researchers must also assure the security of the information until it arrives in the hands of the intended receiver.

Hard copy documents containing PHI should be sent 1) using an insured carrier; 2) with a receiving signature required; and 3) by a carrier with package tracking services.

See also page 8 pertaining to use of “Cloud” servers.

RESEARCH COMMENCED PRIOR TO HIPAA’S EFFECTIVE DATE APRIL 14, 2003

Research that is/was ongoing before the applicable HIPPA compliance date (April 14, 2003) is covered by the Privacy Rule’s transition provisions if the research participant’s informed consent, other legal permission for the research use and disclosure, or an IRB’s waiver of informed consent was obtained by the covered entity before the applicable compliance date for the Privacy Rule.

A transition provision was included in the HIPAA Privacy Rule that allows the research community to “grandfather” certain research studies that were underway at the compliance date mandated for the Privacy Rule.

The Privacy Rule allows for use and disclosure of PHI created or received for research, either before or after April 14, 2003, if one of the following was obtained prior to that date:

- An authorization or other express legal permission from the individual to use or disclose his or her information for research,
- The legally effective informed consent of the individual to participate in the research, OR
- A valid waiver of informed consent from the IRB

However, if a subject is asked for informed consent (or asked to re-consent) for the use of PHI in research on or after April 14, 2003, an authorization must be obtained at that time.

An authorization is not required under the HIPAA rule for participants who were enrolled in a research protocol before April 14, 2003 and who have signed a Common Rule-compliant informed consent form. Even if participants enrolled before April 14th have follow-up visits after that date, authorization will not be required.
However, an authorization will be required for any participant enrolled in a study on or after April 14, 2003, even if the study was approved by the IRB prior to that date.

Therefore, if all participants were enrolled prior to April 14, 2003, there is no need for an authorization for those participants. However, authorization will be required for any new participants after April 14, 2003, either in the form of a separate authorization document or a modified informed consent form, which includes the required authorization language.

WAIVER OF CONSENT REQUIREMENT BY IRB FOR RESEARCH COMMENCED PRIOR TO APRIL 14, 2003

If researchers are conducting a medical records study under an IRB-approved waiver of consent they should continue protecting the privacy of participants’ information, but do not need to re-apply to the IRB. Ongoing studies for which the IRB approved a waiver of informed consent are grandfathered under the HIPAA rule. Although a new waiver is not required, it is important to note that the individual rights provided by the Privacy Rule went into effect as of April 14, 2003. As a result, any disclosure of PHI made pursuant to a waiver of authorization must be tracked as noted above.
FORMS FOR RESEARCHERS
TAMHSC BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT (“Agreement”) dated ________________, 2013 (the “Effective Date”), is entered into by and between ____________________ (“Covered Entity”) and ____________________ (“Business Associate”), each a “Party” and collectively, the “Parties.”

Covered Entity and Business Associate have entered into, are entering into, or may subsequently enter into, agreements or other documented arrangements (collectively, the “Business Arrangements”) pursuant to which Business Associate may provide products and/or services for Covered Entity that require Business Associate to access, create, maintain, and use health information that is protected by state and/or federal law.

Pursuant to the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), the U.S. Department of Health & Human Services (“HHS”) promulgated the Standards for Privacy of Individually Identifiable Health Information (the “Privacy Standards”), at 45 C.F.R. Parts 160 and 164, requiring certain individuals and entities subject to the Privacy Standards (each a “Covered Entity”, or collectively, “Covered Entities”) to protect the privacy of certain individually identifiable health information (“Protected Health Information” or “PHI”).

Pursuant to HIPAA, HHS issued the Security Standards (the “Security Standards”), at 45 C.F.R. Parts 160, 162 and 164, for the protection of electronic protected health information (“EPHI”).

In order to protect the privacy and security of PHI, including EPHI, created or maintained by or on behalf of the Covered Entity, the Privacy Standards and Security Standards require a Covered Entity to enter into a “business associate agreement” with certain individuals and entities providing services for or on behalf of the Covered Entity if such services require the use or disclosure of PHI or EPHI.

On February 17, 2009, the federal Health Information Technology for Economic and Clinical Health Act was signed into law (the “HITECH Act”), and the HITECH Act imposes certain privacy and security obligations on Covered Entities in addition to the obligations created by the Privacy Standards and Security Standards.

The HITECH Act revises many of the requirements of the Privacy Standards and Security Standards concerning the confidentiality of PHI and EPHI, including extending certain HIPAA and HITECH Act requirements directly to Business Associates.

The HITECH Act requires that certain of its provisions be included in business associate agreements, and that certain requirements of the Privacy Standards be imposed contractually upon Covered Entities as well as Business Associates.

The Texas Legislature has adopted certain privacy and security requirements that are more restrictive than those required by HIPAA and HITECH, and such requirements are applicable to Business Associates as “Covered Entities” as defined by Texas law; and
Because Business Associate and Covered Entity desire to enter into this Business Associate Agreement, in consideration of the mutual promises set forth in this Agreement and the applicable Business Arrangements, and other good and valuable consideration, the sufficiency and receipt of which are hereby acknowledged, the Parties agree as follows:

I. Definitions

a. Except as otherwise defined in this Agreement, all capitalized terms used in this Agreement shall have the meanings set forth in HIPAA.

b. “Business Associate” shall have the same meaning to the term “Associate” under the Privacy Rule, including, but not limited to, 45 CFR Section 160.103.

c. “Breach” shall mean the acquisition, access, use or disclosure of Protected Health Information in a manner not permitted by the HIPAA Privacy Rule that compromises the security or privacy of the Protected Health Information as defined, and subject to the exceptions set forth, in 45 CFR § 164.402.

d. “Covered Entity” shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR Section 160.103.

e. “Data Aggregation Services” shall mean the combining of PHI or EPHI by Business Associate with the PHI or EPHI received by Business Associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of, payment to, and treatment of patients by the respective covered entities.

f. “Electronic Protected Health Information” shall mean Protected Health Information that is transmitted or maintained in Electronic Media.

g. “HIPAA” shall mean the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, as amended and supplemented by the HITECH Act and its implementing regulations, as each is amended from time to time.

h. “HIPAA Breach Notification Rule” shall mean the federal breach notification regulations, as amended from time to time, issued under HIPAA and set forth in 45 CFR Part 164 (Subpart D).

i. “HIPAA Privacy Rule” shall mean the federal privacy regulations, as amended from time to time, issued under HIPAA and set forth in 45 CFR Parts 160 and 164 (Subparts A & E).

j. “HIPAA Security Rule” shall mean the federal security regulations, as amended from time to time, issued under HIPAA and set forth in 45 CFR Parts 160 and 164 (Subparts A & C).

k. “HITECH Act” shall mean Subtitle D of the Health Information Technology for Economic and Clinical Health Act provisions of the American recovery and Reinvestment Act of 2009, 42 U.S.C. §§ 17921-17954, and all its implementing regulations, when and as each is effective and compliance is required.
I. “Protected Health Information of PHI” shall mean Protected Health Information, as defined in 45 CFR § 160.103, and is limited to the Protected Health Information received, maintained, created or transmitted on behalf of, Covered Entity by Business Associate in performance of the Underlying Services.

m. “Underlying Services” shall mean, to the extent and only to the extent they involve the creation, maintenance, use, disclosure or transmission of Protected Health Information, the services performed by Business Associate for Covered Entity pursuant to the Underlying Services Agreement.

n. “Underlying Services Agreement” shall mean the written agreement(s) (other than this Agreement) by and between the parties as amended as set forth in the attached schedule by and between the Parties pursuant to which Business Associate access to, receives, maintains, creates or transmits PHI for or on behalf of Covered Entity in connection with the provision of the services described in that agreement(s) by Business Associate to Covered Entity or in performance of Business Associate’s obligations under such agreement(s).

II. Business Associate Obligations.

Business Associate may receive from Covered Entity, or create or receive or maintain on behalf of Covered Entity, health information that is protected under applicable state and/or federal law, including without limitation, PHI and EPHI. All references to PHI herein shall be construed to include EPHI. Business Associate agrees not to use or disclose (or permit the use or disclosure of) PHI in a manner that would violate the Privacy Standards, Security Standards the HITECH Act, or Texas law, including without limitation the provisions of Texas Health and Safety Code Chapters 181 and 182 as amended by HB 300 (82nd Legislature), effective September 1, 2012, in each case including any implementing regulations as applicable (collectively referred to hereinafter as the “Confidentiality Requirements”) if the PHI were used or disclosed by Covered Entity in the same manner.

III. Use of Protected Health Information

Except as otherwise required by law, Business Associate shall use PHI in compliance with 45 C.F.R. § 164.504(e). Furthermore, Business Associate shall use PHI (i) solely for Covered Entity’s benefit and only for the purpose of performing services for Covered Entity as such services are defined in Business Arrangements, (ii) for Data Aggregation Services (as hereinafter defined), and (iii) as necessary for the proper management and administration of the Business Associate or to carry out its legal responsibilities, provided that such uses are permitted under federal and state law. For avoidance of doubt, under no circumstances may Business Associate sell PHI in such a way as to violate Texas Health and Safety Code, Chapter 181.153, as amended by HB 300 (82nd Legislature), effective September 1, 2012, nor shall Business Associate use PHI for marketing purposes in such as manner as to violate Texas Health and Safety Code Section 181.152, or attempt to re-identify any information in violation of Texas Health and Safety Code Section 181.151, regardless of whether such action is on behalf of or permitted by the Covered Entity. To the extent not otherwise prohibited in the Business Arrangements or by applicable
law, use, creation and disclosure of de-identified health information, as that term is defined in 45 CFR § 164.514, by Business Associate is permitted.

IV. Disclosure of Protected Health Information

Subject to any limitations in this Agreement, Business Associate may disclose PHI to any third party persons or entities as necessary to perform its obligations under the Business Arrangement and as permitted or required by applicable federal or state law. Business Associate recognizes that under the HIPAA/HITECH Omnibus Final Rule, Business Associates may not disclose PHI in a way that would be prohibited if Covered Entity made such a disclosure. Any disclosures made by Business Associate will comply with minimum necessary requirements under the Privacy Rule and related regulations.

Business Associate shall not [and shall provide that its directors, officers, employees, subcontractors, and agents, do not] disclose PHI to any other person (other than members of their respective workforce as specified in subsection 0 below), unless disclosure is required by law or authorized by the person whose PHI is to be disclosed. Any such disclosure other than as specifically permitted in the immediately preceding sentences shall be made only if such disclosee has previously signed a written agreement that:

a.) Binds the disclosee to the provisions of this Agreement pertaining to PHI, for the express benefit of Covered Entity, Business Associate and, if disclosee is other than Business Associate, the disclosee;

b.) Contains reasonable assurances from disclosee that the PHI will be held confidential as provided in this Agreement, and only disclosed as required by law for the purposes for which it was disclosed to disclosee; and,

c.) Obligates disclosee to immediately notify Business Associate of any breaches of the confidentiality of the PHI, to the extent disclosee has obtained knowledge of such breach.

Business Associate shall not disclose PHI to any member of its workforce and shall provide that its subcontractors and agents do not disclose PHI to any member of their respective workforces, unless Business Associate or such subcontractor or agent has advised such person of Business Associate’s obligations under this Agreement, and of the consequences for such person and for Business Associate or such subcontractor or agent of violating them as memorialized in a business associate agreement pursuant to the HIPAA/HITECH Omnibus Final Rule. Business Associate shall take and shall provide that each of its subcontractors and agents take appropriate disciplinary action against any member of its respective workforce who uses or discloses PHI in contravention of this Agreement.

In addition to Business Associate’s obligations under Section 9, Business Associate agrees to mitigate, to the extent commercially practical, harmful effects that are
known to Business Associate and is the result of a use or disclosure of PHI by Business Associate or Recipients in violation of this Agreement.

V. Access to and Amendment of Protected Health Information

Business Associate shall (i) provide access to, and permit inspection and copying of, PHI by Covered Entity; and (ii) amend PHI maintained by Business Associate as requested by Covered Entity. Any such amendments shall be made in such a way as to record the time and date of the change, if feasible, and in accordance with any subsequent requirements promulgated by the Texas Medical Board with respect to amendment of electronic medical records by HIEs. Business Associate shall respond to any request from Covered Entity for access by an individual within seven (7) days of such request and shall make any amendment requested by Covered Entity within twenty (20) days of the later of (a) such request by Covered Entity or (b) the date as of which Covered Entity has provided Business Associate with all information necessary to make such amendment. Business Associate may charge a reasonable fee based upon the Business Associate’s labor costs in responding to a request for electronic information (or the fee approved by the Texas Medical Board for the production of non-electronic media copies). Business Associate shall notify Covered Entity within five (5) days of receipt of any request for access or amendment by an individual. Covered Entity shall determine whether to grant or deny any access or amendment requested by the individual. Business Associate shall have a process in place for requests for amendments and for appending such requests and statements in response to denials of such requests to the Designated Record Set, as requested by Covered Entity.

VI. Accounting of Disclosures

Business Associate shall make available to Covered Entity in response to a request from an individual, information required for an accounting of disclosures of PHI with respect to the individual in accordance with 45 CFR § 164.528, as amended by Section 13405(c) of the HITECH Act and any related regulations or guidance issued by HHS in accordance with such provision.

VII. Records and Audits

Business Associate shall make available to the United States Department of Health and Human Services or its agents, its internal practices, books, and records relating to the use and disclosure of PHI received from, created, or received by Business Associate on behalf of Covered Entity for the purpose of determining Covered Entity’s compliance with the Confidentiality Requirements or the requirements of any other health oversight agency, in a time and manner designated by the Secretary.

VIII. Implementation of Security Standards; Notice of Security Incidents

Business Associate will use appropriate safeguards to prevent the use or disclosure of PHI other than as expressly permitted under this Agreement. Business Associate will implement administrative, physical and technical safeguards that reasonably and
appropriately protect the confidentiality, integrity and availability of the PHI that it creates, receives, maintains or transmits on behalf of Covered Entity. Business Associate acknowledges that the HITECH Act requires Business Associate to comply with 45 C.F.R. §§164.308, 164.310, 164.312 and 164.316 as if Business Associate were a Covered Entity, and Business Associate agrees to comply with these provisions of the Security Standards and all additional security provisions of the HITECH Act.

Furthermore, to the extent feasible, Business Associate will use commercially reasonable efforts to secure PHI through technology safeguards that render such PHI unusable, unreadable and indecipherable to individuals unauthorized to acquire or otherwise have access to such PHI in accordance with HHS Guidance published at 74 Federal Register 19006 (April 17, 2009), or such later regulations or guidance promulgated by HHS or issued by the National Institute for Standards and Technology ("NIST") concerning the protection of identifiable data such as PHI. Lastly, Business Associate will promptly report to Covered Entity any successful Security Incident of which it becomes aware. At the request of Covered Entity, Business Associate shall identify: the date of the Security Incident, the scope of the Security Incident, the Business Associate’s response to the Security Incident and the identification of the party responsible for causing the Security Incident, if known.

IX. Data Breach Notification and Mitigation

HIPAA Data Breach Notification and Mitigation. Business Associate agrees to implement reasonable systems for the discovery and prompt reporting to Covered Entity of any “breach” of “unsecured PHI” as those terms are defined by 45 C.F.R. §164.402. Specifically, a breach is an unauthorized acquisition, access, use or disclosure of unsecured PHI, including ePHI, which compromises the security or privacy of the PHI/ePHI. A breach is presumed to have occurred unless there is a low probability that the PHI has been compromised based on a risk assessment of at least the factors listed in 45 C.F.R. § 164.402(2)(i)-(iv) (hereinafter a “HIPAA Breach”). The parties acknowledge and agree that 45 C.F.R. § 164.404, as described below in this Section 8.1, governs the determination of the date of discovery of a HIPAA Breach. In addition to the foregoing and notwithstanding anything to the contrary herein, Business Associate will also comply with applicable state law, including without limitation, Section 521 Texas Business and Commerce Code, as amended by HB 300 (82nd Legislature), or such other laws or regulations as may later be amended or adopted. In the event of any conflict between this Section 8.1, the Confidentiality Requirements, Section 521 of the Texas Business and Commerce Code, and any other later amended or adopted laws or regulations, the most stringent requirements shall govern.

Discovery of Breach. Business Associate will, following the discovery of a HIPAA Breach, notify Covered Entity without unreasonable delay and in no event later than the earlier of the maximum of time allowable under applicable law or three (3) business days after Business Associate discovers such HIPAA Breach, unless Business Associate is prevented from doing so by 45 C.F.R. §164.412 concerning law enforcement investigations. For purposes of reporting a HIPAA Breach to
Covered Entity, the discovery of a HIPAA Breach shall occur as of the first day on which such HIPAA Breach is known to the Business Associate or, by exercising reasonable diligence, would have been known to the Business Associate. Business Associate will be considered to have had knowledge of a HIPAA Breach if the HIPAA Breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the HIPAA Breach) who is an employee, officer or other agent of the Business Associate.

Reporting a Breach. Without unreasonable delay and no later than the earlier of the maximum of time allowable under applicable law or five (5) business days following a HIPAA Breach, Business Associate shall provide Covered Entity with sufficient information to permit Covered Entity to comply with the HIPAA Breach notification requirements set forth at 45 C.F.R. § 164.400 et seq. Specifically, if the following information is known to (or can be reasonably obtained by) the Business Associate, Business Associate will provide Covered Entity with:

a.) contact information for individuals who were or who may have been impacted by the HIPAA Breach (e.g., first and last name, mailing address, street address, phone number, email address);

b.) a brief description of the circumstances of the HIPAA Breach, including the date of the HIPAA Breach and date of discovery;

c.) a description of the types of unsecured PHI involved in the HIPAA Breach (e.g., names, social security number, date of birth, addressees, account numbers of any type, disability codes, diagnostic and/or billing codes and similar information);

d.) a brief description of what the Business Associate has done or is doing to investigate the HIPAA Breach, mitigate harm to the individual impacted by the HIPAA Breach, and protect against future HIPAA Breaches; and,

e.) appoint a liaison and provide contact information for same so that Covered Entity may ask questions or learn additional information concerning the HIPAA Breach.

Following a HIPAA Breach, Business Associate will have a continuing duty to inform Covered Entity of new information learned by Business Associate regarding the HIPAA Breach, including but not limited to the information described in items (i) through (v), above.

X. Termination

This Agreement shall commence on the Effective Date.

Upon the termination of the applicable Business Arrangement, either Party may terminate this Agreement by providing written notice to the other Party.

Upon termination of this Agreement for any reason, Business Associate agrees:
a.) to return to Covered Entity or to destroy all PHI received from Covered Entity or otherwise through the performance of services for Covered Entity, that is in the possession or control of Business Associate or its agents. Business Associate agrees that all paper, film, or other hard copy media shall be shredded or destroyed such that it may not be reconstructed, and EPHI shall be purged or destroyed concurrent with NIST Guidelines for media sanitization at http://www.csrc.nist.gov/; or,

b.) in the case of PHI which is not feasible to “return or destroy,” to extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI. Business Associate further agrees to comply with other applicable state or federal law, which may require a specific period of retention, redaction, or other treatment of such PHI.

XI. Miscellaneous
Notice. All notices, requests, demands and other communications required or permitted to be given or made under this Agreement shall be in writing, shall be effective upon receipt or attempted delivery, and shall be sent by (i) personal delivery; (ii) certified or registered United States mail, return receipt requested; (iii) overnight delivery service with proof of delivery; or (iv) facsimile with return facsimile acknowledging receipt. Notices shall be sent to the addresses below. Neither party shall refuse delivery of any notice hereunder.

Business Associate:  
Covered Entity:  

Waiver. No provision of this Agreement or any breach thereof shall be deemed waived unless such waiver is in writing and signed by the Party claimed to have waived such provision or breach. No waiver of a breach shall constitute a waiver of or excuse any different or subsequent breach.

Assignment. Neither Party may assign (whether by operation or law or otherwise) any of its rights or delegate or subcontract any of its obligations under this Agreement without the prior written consent of the other Party.

Notwithstanding the foregoing, Covered Entity shall have the right to assign its rights and obligations hereunder to any entity that is an affiliate or successor of Covered Entity, without the prior approval of Business Associate.

Severability. Any provision of this Agreement that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without
invalidating the remaining provisions of this Agreement or affecting the validity or enforceability of such remaining provisions.

**Entire Agreement.** This Agreement constitutes the complete agreement between Business Associate and Covered Entity relating to the matters specified in this Agreement, and supersedes all prior representations or agreements, whether oral or written, with respect to such matters. In the event of any conflict between the terms of this Agreement and the terms of the Business Arrangements or any such later agreement(s), the terms of this Agreement shall control unless the terms of such Business Arrangements are more strict with respect to PHI and comply with the Confidentiality Requirements, or the parties specifically otherwise agree in writing. No oral modification or waiver of any of the provisions of this Agreement shall be binding on either Party; provided, however, that upon the enactment of any law, regulation, court decision or relevant government publication and/or interpretive guidance or policy that the Covered Entity believes in good faith will adversely impact the use or disclosure of PHI under this Agreement, Covered Entity may amend the Agreement to comply with such law, regulation, court decision or government publication, guidance or policy by delivering a written amendment to Business Associate which shall be effective thirty (30) days after receipt. No obligation on either Party to enter into any transaction is to be implied from the execution or delivery of this Agreement. This Agreement is for the benefit of, and shall be binding upon the parties, their affiliates and respective successors and assigns. No third party shall be considered a third-party beneficiary under this Agreement, nor shall any third party have any rights as a result of this Agreement.

**Governing Law.** This Agreement shall be governed by and interpreted in accordance with the laws of the state of Texas. Venue for any dispute relating to this Agreement shall be in Brazos County, Texas.

**Nature of Agreement; Independent Contractor.** Nothing in this Agreement shall be construed to create (i) a partnership, joint venture or other joint business relationship between the parties or any of their affiliates, or (ii) a relationship of employer and employee between the parties. Business Associate is an independent contractor, and not an agent of Covered Entity. This Agreement does not express or imply any commitment to purchase or sell goods or services.

**Counterparts.** This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same document. In making proof of this Agreement, it shall not be necessary to produce or account for more than one such counterpart executed by the party against whom enforcement of this Agreement is sought. Signatures to this Agreement transmitted by facsimile transmission, by electronic mail in portable document format (“.pdf”) form, or by any other electronic means intended to preserve the original graphic and pictorial appearance of a document, will have the same force and effect as physical execution and delivery of the paper document bearing the original signature.

**IN WITNESS WHEREOF,** the parties have executed this Agreement as of the Effective Date.
**BUSINESS ASSOCIATE:**

**COVERED ENTITY:**

**TEXAS A&M HEALTH SCIENCE CENTER**

---

**Departmental Approval**

<table>
<thead>
<tr>
<th>Department:</th>
<th>Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td>Title:</td>
</tr>
<tr>
<td>Title:</td>
<td></td>
</tr>
<tr>
<td>Signature:</td>
<td>Signature:</td>
</tr>
<tr>
<td>Date:</td>
<td>Date:</td>
</tr>
</tbody>
</table>

---

**Dean Approval**

<table>
<thead>
<tr>
<th>Component:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Title:</td>
</tr>
<tr>
<td>Signature:</td>
</tr>
<tr>
<td>Date:</td>
</tr>
</tbody>
</table>

---

**Vice President for Finance and Administration Approval**

| Name:       |
| Title:     |
| Signature: |
| Date:      |
TAMHSC Data Use and Confidentiality Agreement

Access to Technology and Information Resources

Access to Texas A&M Health Science Center data and information, and access to IT accounts, systems, and applications, is based on your need for access and your assent to use that access appropriately. These services are integral to the operation of the university, and security and privacy laws and other institutional policies protect much of the information.

Therefore, before you can be granted access, you must read and agree to follow these acceptable usage standards, and must accept responsibility to preserve the security and confidentiality of information that you access, in any form, including oral, print, or electronic formats.

Although these general provisions apply to all Health Science Center information and IT accounts, systems, and applications, please be aware that managers of certain services or information types may require you to complete additional agreements and/or training.

Usage responsibilities:

The following points detail your responsibilities as you access, use, or handle information or information technology (IT) at Texas A&M Health Science Center.

Secure Usage.

You agree to:

- **Never share your account password(s) or passphrase(s) with anyone.**
- Select strong password(s) and passphrase(s).
- Be mindful that different computer systems and applications provide different levels of protection for information, and seek advice on supplemental security measures, if necessary. For example, a mobile laptop provides inherently less protection than a desktop computer in a locked office. Therefore, the level of protection provided to information accessed or stored using a laptop is to be supplemented by using additional safeguards such as encryption technology, enhancing physical security, restricting file permissions, etc.
- Respect the university's information and system security procedures (i.e., never attempt to circumvent or "go around" security processes).
- Maintain information in a secure manner to prevent access, viewing, or printing by unauthorized individuals.
- Secure unattended devices (e.g., log off, lock, or otherwise make inaccessible), even if you will only be away from the computer or device for a moment.
- Store Restricted and Critical data securely (e.g., on secure servers, in locked file cabinets, etc.).
- Securely dispose of Restricted and Critical information (e.g., by shredding, disk wiping, physical destruction, etc.).
- Never copy and/or store Restricted or Critical data outside of institutional systems (e.g., on desktop workstations, laptops, USB drives, personally owned computers, etc.) without proper approval from the senior executive officer of the department and only in cases where it is absolutely necessary for the operation of the department.
- Take appropriate steps to secure information (e.g., password protection, encryption, etc.) on mobile storage devices (e.g., laptops, USB drives, cell phones, etc.).
• Ensure, in the rare cases where Critical data has been approved for use and storage outside of institutional systems, that the data are appropriately encrypted, especially on mobile storage devices (e.g., laptops, cell phones, USB drives, CD-ROMs).
• Ensure, in the rare cases where it is necessary to email Critical or Confidential data, that the data are sent to the correct recipient and only via encrypted email methods.
• All PHI stored on electronic devices will be de-identified where applicable.

Legal Usage
You agree to:
• Use information and resources for legal purposes only.
• Respect and comply with all copyrights and license agreements.
• Never use your access to information or devices to harass, libel, or defame others.
• Never damage equipment, software, or data belonging to others.
• Never make unauthorized use of computer accounts, access codes, or devices.
• Never monitor or disrupt the communications of others, except in the legitimate scope of your assigned duties.
• Abide by applicable laws and policies with respect to access to, use, disclosure, and/or disposal of information. Applicable laws and policies include but are not limited to:
  ○ Health Insurance Portability and Accountability Act (HIPAA)
  ○ Family Educational Rights and Privacy Act (FERPA)
  ○ TAMHSC rules and policies (http://www.tamhsc.edu/facultystaff/rules/)

Ethical Usage
You agree to:
• Access institutional information only in the conduct of business and in ways consistent with furthering the mission of education, research, and public service.
• Use only the information needed to perform assigned or authorized duties.
• Never access any institutional information to satisfy your personal curiosity.
• Use information and IT in ways that foster the high ethical standards of the university.
• Never use information or IT to engage in academic, personal, or research misconduct.
• Never access or use institutional information (including public directory information) for your own personal gain or profit, or the personal gain or profit of others, without appropriate authorization.
• Respect the confidentiality and privacy of individuals whose records you may access.
• Preserve and protect the confidentiality of all internal, restricted, or Critical information as a matter of ongoing responsibility.
• Never disclose internal, Restricted, or Critical data (as defined by policy; see above) or distribute such data to a third party in any medium (including oral, paper, or electronic) without proper approval, and in the case of Restricted or Critical data, without a contract processed through or waived by the Health Science Center Purchasing Department.

To be entrusted with access to Texas A&M Health Science Center data and information, and access to IT accounts, systems, and applications, new or continuing faculty, staff, students, visiting scholars, volunteers and all other authorized individuals must accept these responsibilities and standards of acceptable use. By accepting these terms, you agree to follow these rules in all of your interactions.

I have read, understand, and agree to abide by the practices outlined in this agreement.

Signature _______________________________ Date _______________________________
CASE STUDY AUTHORIZATION FORM  
SIGNED BY RESEARCH PARTICIPANT

CASE REPORT:  Case description of [Name of disease or condition]

AUTHOR/CO-AUTHOR:  [Researcher Name1]  
[Researcher Name 2]

The case report named above may be performed only by using personal information  
relating to your health. National data protection regulations give you the right to control  
the use and disclosure of your medical information. Therefore, by signing this form, you  
specifically authorize your medical information to be used or disclosed as described  
down below.

Use of your personal information

The following personal information, considered “Protected Health Information” (PHI) is  
needed to conduct this case report and may include, but is not limited to: [name,  
address, telephone number, date of birth, government-issued identification number, and  
medical records and charts, including the results of all tests and procedures performed.]  
Additionally, PHI may be shared with individuals designated to assist in conducting this  
case study as well as with accreditation bodies. PHI may also be reviewed to ensure  
that the case study meets legal and institutional standards.

Disclosure of your personal information

The main reason for sharing this information is to be able to conduct a case study and  
present or publish the results. The results of the case study may be published in one or  
more publications. Although information obtained from your medical record and chart  
will be disclosed in the publication, we will not publish identifiers such as your name,  
address, telephone number or government-issued identification number. Identifiers may  
be used, however, for sharing information with an agency authorized to receive reports  
on adverse events or situations that may help prevent placing other individuals at risk.

I hereby give authorization for the use or disclosure of my personal information for the  
case report based on my understanding of the following.

I understand that you may use my personal information to prepare this report. The  
scope of the report, however, is limited to the case description indicated above.
I understand that medical information that includes direct identifiers may be shared for the purpose of legal and institutional review as well as for the purpose of review by an accreditation body.

I understand that the authorization to use my personal information to conduct this case report will expire at the end of the study. However, I understand that following publication, full articles or abstracts of or from the initial report may be published and continue to be published for an indefinite period of time.

I understand that this authorization does not authorize the use or disclosure of personal information created or obtained after initial publication.

I understand that I do not need to sign this authorization in order to receive health care.

I understand that I may revoke this authorization at any time. However, the revocation will not apply to information that has already been released in response to this authorization.

I agree that my personal health information may be used for the purposes described in this form.

Name of patient: ________________________________

Signature of patient: ________________________________

Date/time: ________________________________
Data Use Preparatory-to-Research Certification & Guidance

Provisions for review of patient records prior to design of research study ("Preparatory to Research"): 

Under the HIPAA Privacy Rule, the activity covered by this guidance is NOT yet considered research. The purpose is to allow investigators to review as many records as necessary (using the minimum necessary standard) in order to design or determine the feasibility of a research study, but may only record data from 25 records per LLU policy. No more information than is allowed in a Limited Data Set may be recorded from these 25 records. This means that no direct identifiers (name, medical record number, etc.) may be recorded from this information. No attempt may be made to identify or contact research participants using this information.

By signing the certification below, you are agreeing to these terms. IRB approval must be obtained for recording data from more than 25 records or for recording any information about the patient other than what is allowed in a Limited Data Set.

Instructions:
1. Download and complete a Data Request Form (see also instructions) for the Certified Data Release Department (CDRD) responsible for the data to be reviewed. Thus, where the Data Request Form asks about Purpose, check "Other" and write in "Preparatory to Research." (Do not check "Research.") Refer to the Data Request Form instructions with any questions.

2. Complete, sign, and date the Certification below and attach to the back of the Data Request Form.

3. Make copies of both forms and submit to the Office of Sponsored Research (558-4531, or extension 44531). Submit the original forms to the appropriate Certified Data Release Department in order to obtain access to the data needed preparatory to research.

Certification:

I hereby certify:

The use or disclosure of the data requested on the attached Data Request Form is solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

No protected health information is to be removed from the covered entity by me or those under my direction in the course of the review; and

The protected health information for which use or access is sought is necessary for the research purposes.
Title of Proposed Research Project

_______________________________________________________

Signed ________________________________ Date

____________________________

Print name of person requesting data

_______________________________________________________
Notice of Privacy Practices ACKNOWLEDGEMENT

Patient Name: ________________________________

Date of Birth: ________________________________

Social Security Number: ________________________

I acknowledge that Texas A&M Health Sciences Center provided me with a written copy of his/her Notice of Privacy Practices.

I also acknowledge that I have been afforded the opportunity to read the Notice of Privacy Practices and ask questions.

__________________________________________  __________________________
Patient Signature                              Date

__________________________________________  __________________________
Personal Representative Signature (if applicable)  Relationship to Patient
POLICIES & STANDARD OPERATING PROCEDURES
PERTAINING TO HIPAA PRIVACY
PRIVACY OFFICER OPERATING PROCEDURE

PURPOSE: To maintain accountability for privacy within TEXAS A&M SCHOOL OF PUBLIC HEALTH.

OPERATING PROCEDURE:

TEXAS A&M SCHOOL OF PUBLIC HEALTH designates Jane Bolin as the Privacy Officer. The Privacy Officer may be contacted at (979)/436-9468 and all correspondence may be mailed to:

The Privacy Officer will oversee TEXAS A&M SCHOOL OF PUBLIC HEALTH Privacy Program, including:

- Developing and implementing privacy policies, in accordance with federal and Texas privacy requirements.
- Receiving and processing authorizations.
- Receiving and processing revocation of authorizations.
- Overseeing that all members of the workforce who come into contact with PHI are properly trained.
- Approving all disclosures that do not require authorization or opportunity to agree/object from the patient.
- Providing information in relation to the Notice of Privacy Practices.
- Mitigating the effects of all disclosures that are not compliant with federal or Texas law or that are contrary to TEXAS A&M SCHOOL OF PUBLIC HEALTH Privacy Policies and Procedures.
- Conducting, at least annually, a review of the implementation of the minimum necessary requirements.
- Conducting, at least annually, a review of TEXAS A&M SCHOOL OF PUBLIC HEALTH access procedures and relevant records.
- Guiding and assisting in the identification, implementation, and maintenance of privacy policies and procedures in coordination with TEXAS A&M SCHOOL OF PUBLIC HEALTH management and legal counsel.
- Reviewing all system-related information security plans in order to align security and privacy practices.

- Performing initial and periodic risk assessments or “privacy audits” and conducting ongoing compliance monitoring activities.

- Overseeing that TEXAS A&M SCHOOL OF PUBLIC HEALTHS maintains appropriate consent, authorization forms, and information notices and materials reflecting current organization and legal practices and requirements.

- Overseeing compliance with privacy practices and application of sanctions for failure to comply with privacy policies.

This list provides an overview of Privacy Officer duties and is not meant to serve as an all-inclusive list.
HIPAA COMPLIANCE AND PRIVACY OFFICER JOB DESCRIPTION

Position Title: HIPAA Compliance & Privacy Officer

Immediate Supervisor: Dean, School of Public Health

General Purpose: The Privacy Officer oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to policies and procedures covering the privacy of, and access to, all patient’s PHI in compliance with federal and Texas laws and information privacy practices.

Responsibilities:

- Provides development guidance and assists in the identification, implementation, and maintenance of privacy policies and procedures in coordination with management, administration, and legal counsel.

- Reviews all system-related information security plans to oversee alignment between security and privacy practices.

- Develops, reviews, and publishes TEXAS A&M SCHOOL OF PUBLIC HEALTH’s privacy notice to general public as required under federal and Texas law.

- Establishes a mechanism to track access to Protected Health Information as required by law.

- Establishes and administers a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization’s privacy policies and procedures.

- Conducts or coordinates initial privacy training and orientation to all employees, volunteers, medical and professional staff.

- Performs or assists in performing initial and periodic risk assessments or “privacy audits” and conducts related ongoing compliance monitoring activities.

- Oversees that TEXAS A&M SCHOOL OF PUBLIC HEALTH has and maintains appropriate privacy and confidentiality consent, authorization forms, and information notices and materials reflecting current legal practices and requirements.

- Oversees compliance with privacy practices and application of sanctions for failure to comply with privacy policies.

- Maintains current knowledge of applicable federal and Texas privacy laws and accreditation standards and monitors advancements in information privacy technologies.
• Cooperates with the HHS Office for Civil Rights and other legal entities in any compliance reviews or investigations.

Qualifications:

**Education:**

Graduate Degree Preferred. At a minimum, completion of undergraduate college with major in administration, business, or human resources, or other educational level relative to the size and scope of the practice.

**Experience:**

Knowledge and experience in information privacy laws, access, release of information, and release control technologies.

Demonstrated organizational, communication, and presentation skills.
COMPLAINT OPERATING PROCEDURE

PURPOSE:

To implement a procedure for receiving, documenting, and taking appropriate action with respect to privacy complaints.

OPERATING PROCEDURE:

All Privacy Complaints must be submitted to the Privacy Officer or his/her designees.

Privacy Complaints must include a statement that describes the basis of the complaint.

The Privacy Officer will determine what health care information the patient claims was misused or improperly disclosed. If the health care information at issue was created or maintained by a business associate, the complaint will be forwarded to the business associate.

RESPONSIBILITIES OF THE PRIVACY OFFICER:

The Privacy Officer shall determine:

1. Whether there has been a violation of the privacy regulations or TEXAS A&M SCHOOL OF PUBLIC HEALTH privacy policies.
2. What, if any, internal privacy practices need to be changed.
3. What, if any, additional policies need to be developed.
4. What additional training will be provided to the person who violated the privacy regulations or policies.

If the Privacy Officer determines that a violation has occurred, he/she in consultation with _____________ determines what appropriate sanctions must be taken against the employee/provider.

The Privacy Officer shall document all complaints received by TEXAS A&M SCHOOL OF PUBLIC HEALTH and the action taken in response to the complaint in a separately and confidentially maintained patient complaint file. Documentation of each complaint will be retained in written or electronic form for seven (7) years from the date of creation or the last effective date, whichever is later.
HIPAA PRIVACY & COMPLIANCE COMPLAINT FORM

Patient Name: ____________________________________________________________

Date of Birth: ________________ Patient File Number: _______________________

Patient Address: __________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

Please describe the basis of your complaint.

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

On what date did this event occur? __________________________

What health care information was allegedly illegally used and/or disclosed?

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

Signature of patient or legal representative: _________________________________

Date: _____________________
WORKFORCE TRAINING OPERATING PROCEDURE FOR HIPAA

PURPOSE:

To establish an OPERATING PROCEDURE for privacy training.

OPERATING PROCEDURE:

The establishment of privacy training courses will be the responsibility of the Privacy Officer.

All members of TEXAS A&M SCHOOL OF PUBLIC HEALTH workforce who come into contact with PHI in performing their job function will be trained on the privacy laws, policies, and procedures regarding PHI. The following workforce members will be trained:

- All current members.
- Members whose duties are affected by a material change in privacy policies will be re-trained within two months after the change becomes effective.
- Members who have violated privacy laws, policies, or procedures shall be re-trained within 30 days of the determination.

The Privacy Officer shall ensure that TEXAS A&M SCHOOL OF PUBLIC HEALTH documents each training session and the names of the workforce members who completed training. Such documentation will be maintained in TEXAS A&M SCHOOL OF PUBLIC HEALTH privacy records for at least seven (7) years from the date of training.

NOTE: The term “workforce” includes employees, non-physician practitioners, physicians, surgeons who perform surgery at TEXAS A&M SCHOOL OF PUBLIC HEALTH (if applicable), volunteers, and any other individual performing work for TEXAS A&M SCHOOL OF PUBLIC HEALTH who is under the direct control of TEXAS A&M SCHOOL OF PUBLIC HEALTH, regardless of whether paid or not.
## HIPAA EMPLOYEE TRAINING RECORD

<table>
<thead>
<tr>
<th>WORKFORCE MEMBER’S IDENTIFICATION</th>
<th>Last Name: ____________________________</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>First Name: ____________________________</td>
</tr>
<tr>
<td></td>
<td>Social Security Number: ________________</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>INDIVIDUAL MAKING ENTRY</th>
<th>Last Name: ____________________________</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>First Name: ____________________________</td>
</tr>
<tr>
<td></td>
<td>Entity: ________________________________</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>INDIVIDUAL CONDUCTING TRAINING</th>
<th>Last Name: ____________________________</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>First Name: ____________________________</td>
</tr>
<tr>
<td></td>
<td>Entity: ________________________________</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DATE OF TRAINING</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DESCRIPTION OF TRAINING RECEIVED</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PLACE OF TRAINING</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>COMMENTS</td>
<td></td>
</tr>
</tbody>
</table>
OPERATING PROCEDURE FOR DISCIPLINARY ACTION RELATING TO HIPAA VIOLATIONS

[NOTE: You may wish to incorporate these provisions in your personnel policies and procedures or cross-reference those policies here.]

TEXAS A&M SCHOOL OF PUBLIC HEALTH recognizes the importance of safeguarding PHI. Consequently, all workforce members will be trained as to TEXAS A&M SCHOOL OF PUBLIC HEALTH policies and procedures regarding PHI. It is the responsibility of each workforce member to comply with these policies, procedures, and applicable Texas and federal confidentiality laws and regulations. Any concerns or questions regarding this OPERATING PROCEDURE should be directed to the Privacy Officer.

Workforce Member’s Duty to Report Violations of Policies.

Any workforce member who observes or is aware of a PHI OPERATING PROCEDURE violation must report the violation to his/her supervisor or to the Privacy Officer.

Any workforce member who believes in good faith that a violation of PHI OPERATING PROCEDURE has occurred, may report such violation to TEXAS A&M SCHOOL OF PUBLIC HEALTH without violating this OPERATING PROCEDURE. TEXAS A&M SCHOOL OF PUBLIC HEALTH will not intimidate, threaten, coerce, discriminate against, or take retaliatory action against any individual who reasonably exercises his/her rights under this OPERATING PROCEDURE.

Failure to report a violation of TEXAS A&M SCHOOL OF PUBLIC HEALTH PHI policies is a violation of this OPERATING PROCEDURE and may lead to disciplinary action, up to and including termination.

Disciplinary Action. Failure to comply with PHI policies may be grounds for disciplinary action, including termination of employment. The appropriate level of disciplinary action will be determined on a case by case basis, taking into consideration the specific circumstances and severity of the violation. In cases where disciplinary action is imposed (except termination), the workforce member shall be required to repeat confidentiality training.

The following is a partial list of workforce member conduct that will constitute a violation of the PHI policies and thus lead to disciplinary action, up to and including termination. There may be other conduct that is not listed which would also constitute OPERATING PROCEDURE violations.

Workforce member demonstrates a pattern or practice of discussing patient information in a public area;

Workforce member demonstrates a pattern or practice of leaving a record in a public area;

Workforce member demonstrates a pattern or practice of leaving a computer containing PHI unsecured;
Workforce member looks up a patient’s address or relative’s address for personal rather than legitimate and authorized business and claim purposes;

Workforce member accesses patient records out of curiosity;

Workforce member compiles a mailing list with the intent to sell or use for personal purposes;

Workforce member reviews a patient’s record in order to use information in a personal relationship; and

Workforce member reviews or discloses PHI in order to advance a personal cause of action.

Explanation of Disciplinary Actions. TEXAS A&M SCHOOL OF PUBLIC HEALTH generally will follow a progressive discipline OPERATING PROCEDURE as set forth below in imposing discipline for violations of this OPERATING PROCEDURE. However, TEXAS A&M SCHOOL OF PUBLIC HEALTH reserves the right, in appropriate circumstances, to immediately terminate or otherwise discipline an employee without notice and/or without following the progressive discipline steps.

Oral Counseling:

Though the counseling is oral, the counseling should be documented.

The record should indicate that it is a verbal counseling.

The workforce member should sign the form.

A refusal to sign should be indicated on the form.

Written Counseling:

This counseling is to be documented.

The workforce member should sign the form.

A refusal to sign should be indicated on the form.

Termination: The reasons for discharge should be documented and discussed with the workforce member.

Mitigation. In an effort to protect all PHI, TEXAS A&M SCHOOL OF PUBLIC HEALTH will mitigate, to the extent practicable, any harmful effect that results from a known use or disclosure of PHI in violation of the PHI policies.

No Retaliation. Individuals shall be protected from retaliation if they act in good faith in believing that the practice opposed is unlawful, the manner of the opposition is reasonable and does not involve the disclosure of PHI in violation of the rule. Further, TEXAS A&M SCHOOL OF PUBLIC HEALTH shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for filing a complaint; testifying, assisting, or participating in an investigation or compliance review;
or opposing any act or practice made unlawful by TEXAS A&M SCHOOL OF PUBLIC HEALTH privacy policies or by Texas and federal laws.
### SANCTIONS RECORD

<table>
<thead>
<tr>
<th>IDENTIFICATION</th>
<th>Last Name: ______________________</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>First Name: ____________________</td>
</tr>
<tr>
<td></td>
<td>Social Security Number:__________</td>
</tr>
<tr>
<td></td>
<td>Title: _________________________</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>INDIVIDUAL MAKING ENTRY</th>
<th>Last Name: ______________________</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>First Name: ____________________</td>
</tr>
<tr>
<td></td>
<td>Title: _________________________</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>INDIVIDUAL TO WHOM THE REPORT WAS MADE</th>
<th>Last Name: ______________________</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>First Name: ____________________</td>
</tr>
<tr>
<td></td>
<td>Title: _________________________</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DATE OF SANCTION</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>DESCRIPTION OF OPERATING PROCEDURE VIOLATED</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>DATE REPORTED</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>DESCRIPTION OF SANCTION</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>REFERENCES TO ANY CORRESPONDENCE</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>COMMENTS</th>
</tr>
</thead>
</table>

**RECORD MUST REMAIN CONFIDENTIAL AND SHOULD BE FILED SEPARATELY IN THE WORKFORCE MEMBER’S PERSONNEL FILE.**
OPERATING PROCEDURE FOR BUSINESS ASSOCIATES

PURPOSE:
Comply with the business associate contract rules under HIPAA.

DEFINITION:
A “Business Associate” is a person who performs a function on behalf of TEXAS A&M SCHOOL OF PUBLIC HEALTH involving individual health information for TEXAS A&M SCHOOL OF PUBLIC HEALTH, other than as a member of the workforce.

OPERATING PROCEDURE:
TEXAS A&M SCHOOL OF PUBLIC HEALTH must obtain satisfactory assurances that a business associate will appropriately safeguard PHI.

The business associate contract must establish the permitted and required uses and disclosures of business associates. A business associate can only use or disclose a covered entity’s PHI as the covered entity can under HIPAA. Therefore, TEXAS A&M SCHOOL OF PUBLIC HEALTH may not authorize business associates to use or further disclose PHI in any manner that would violate HIPAA if the use or disclosure were made by TEXAS A&M SCHOOL OF PUBLIC HEALTH.

A business associate may use and disclose PHI for the proper management and administration of the business associate and to provide data aggregation services relating to the health care operations of TEXAS A&M SCHOOL OF PUBLIC HEALTH.

All business associates must contractually agree:

- Not to use or further disclose the information other than as permitted or required by the contract or as required by law;
- Use appropriate safeguards to prevent use or disclosure of the information other than as provided by the contract;
- Report to TEXAS A&M SCHOOL OF PUBLIC HEALTH any use or disclosure of the information not provided for by his/her contract of which it becomes aware;
- That agents and subcontractors agree to the same restrictions and conditions that apply to the business associate in respect to PHI the agent or subcontractor receives or creates on the behalf of the business associate;
- Make available PHI in accordance with the requirements imposed on TEXAS A&M SCHOOL OF PUBLIC HEALTH;
- Make available PHI for amendment and incorporate any amendments to PHI in accordance with the same requirements imposed on TEXAS A&M SCHOOL OF PUBLIC HEALTH;
- Make available the information required to provide an accounting of disclosures in accordance with the same requirements imposed on TEXAS A&M SCHOOL OF PUBLIC HEALTH;
• Provide the Secretary of HHS and TEXAS A&M SCHOOL OF PUBLIC HEALTH with access to all internal practices and records relating to PHI in order to determine whether TEXAS A&M SCHOOL OF PUBLIC HEALTH is in compliance; and

• To allow TEXAS A&M SCHOOL OF PUBLIC HEALTH, if it is determined that the business associate has violated a material term of the contract, to terminate the relationship.

At termination, the business associate must:
Return or destroy all PHI;
Not retain copies of the information; and
If the business associate cannot return or destroy the PHI, extend the protections of the contract to the information and limit further disclosures.

Satisfactory assurances required of a business associate must be documented through a written contract or other written agreement with the business associate that meets the applicable requirements. The party who enters into the agreement on behalf of TEXAS A&M SCHOOL OF PUBLIC HEALTH is responsible for determining that the agreement contains the necessary business associate provisions.

TEXAS A&M SCHOOL OF PUBLIC HEALTH must take reasonable steps to cure business associate breaches or violations. Failure to cure violations may lead to privacy violations. Sanctions may be imposed against TEXAS A&M SCHOOL OF PUBLIC HEALTH as a result of a failure to cure any action in which there was knowledge of a pattern of activity or practice conducted by the business associate that constituted a material breach or violation of the business associate’s obligations under the contract or other arrangement.

If steps to cure a business associate’s violation of the privacy rules are unsuccessful, TEXAS A&M SCHOOL OF PUBLIC HEALTH must:
Terminate the contract or arrangement, if feasible; or
If termination is not feasible, report the problem to the Secretary of HHS; and

➢  **Practical Tip:** In instances where termination of the contract is not feasible and a business associate has violated the privacy rules, TEXAS A&M SCHOOL OF PUBLIC HEALTH should consult with his/her attorney and determine whether a protective order is appropriate.

The business associate standard does not apply:
With respect to disclosures to a health care provider concerning the treatment of the individual;
With respect to disclosures to health plans for payment purposes; or
To vendors who have only incidental access to PHI. Instead, a Confidentiality Agreement is used for such vendors. (See Section 0 of this Manual.)
OPERATING PROCEDURE FOR CHANGES TO POLICIES AND PROCEDURES

PURPOSE:
To implement a procedure for changing policies and procedures and corresponding forms, records, and agreements.

OPERATING PROCEDURE:
The Privacy Officer is responsible for developing and maintaining all appropriate policies and procedures, prior to implementation.

Policies and procedures may be maintained in written or electronic form.

Any changes to the policies and procedures must be approved by the:

- Privacy Officer; and
- The MSRDP Compliance and Ethics and Executive Committees.

Any changes to an OPERATING PROCEDURE or procedure cannot be implemented until the Privacy Officer makes appropriate changes to the documentation and notifies the appropriate individuals of this change. The Privacy Officer may notify the appropriate individuals of the changes in OPERATING PROCEDURE or procedure in any written form delivered to each individual.

If there are material changes in policies and procedures, the affected workforce must be trained on the amended policies and procedures prior to implementation.

Privacy Officer must retain documentation for seven (7) years from when the documentation is created, unless a longer period applies.
OPERATING PROCEDURE FOR CONFIDENTIALITY OF PROTECTED HEALTH INFORMATION

PURPOSE:
To implement procedures to protect a patient’s PHI.

OPERATING PROCEDURE:

Protection of PHI: All workforce members, directors, officers, contractors, and agents of TEXAS A&M SCHOOL OF PUBLIC HEALTH are responsible for protecting the privacy and security of all PHI that is received, whether orally or recorded, in the course of their work. A patient’s PHI shall be protected from the moment it is received, used, stored, and eventually destroyed.

Verification of Patient Identity: At check-in, all patient identification will be verified. The procedure for verifying patient identity is as follows:

- Employees shall request a patient’s driver’s license and verify the name on the license with the picture. If the patient does not have a driver's license, employee shall verify his/her identity through other appropriate means, such as a Social Security card or personal check with name and address.
- In all cases, the method of verification is to be noted in the patient’s record.
- Employee may assign a personal identification number to the patient to facilitate patient communications. Subsequently, if the patient wishes to access information by phone, TEXAS A&M SCHOOL OF PUBLIC HEALTH may disclose PHI if the patient verifies his/her identity through the use of the personal identifier.

Verification of Personal Representative Authority: It is necessary to verify a personal representative’s identification and authority. The procedure for verifying the identity of a representative is the same as for a patient. The authority of the representative will be verified as follows:

When an adult claims to represent an adult patient, employee shall request a copy of the court document authorizing the person to represent the patient.

When an adult claims to represent an unemancipated minor patient, the fact that the parent or guardian accompanies the child is usually sufficient evidence.

When TEXAS A&M SCHOOL OF PUBLIC HEALTH is aware that parents of minor patients are divorced, a copy of the divorce decree shall be requested and made a part of the patient’s record. The divorce decree shall be complied with in determining which parent has legal authority to consent to surgery on behalf of the minor.

In all cases, the name of the representative and the method of verification are to be noted in the patient’s record.

Verification of Individuals Who Are Not Patients: All disclosures made by workforce members, to individuals other than the patient, shall be directed to the appropriate individual. Therefore, workforce members must identify the person or class of persons
requesting the disclosure and the category or categories of PHI that may be appropriately disclosed.

Prior to making any disclosure, TEXAS A&M SCHOOL OF PUBLIC HEALTH shall make good faith efforts to verify the identity and authority of any person requesting protected information.

The identity or authority of an individual/entity shall be verified by obtaining any oral or written documentation, statement, or representation from the requesting individual.

The presentation of an agency identification badge, other official credential, or other proof of government status, if made in person, shall be sufficient to verify a public official’s identity.

In all cases, the name of the individual and the method of verification are to be noted in the record.

**Confidentiality Agreement:** Each workforce member, full-time employee, temporary employee, consultant, contracted employee, subcontractor, vendor, and business associate shall be required to sign a confidentiality agreement or, where applicable, a business associate agreement, upon commencing work or entering into a contractual relationship with TEXAS A&M SCHOOL OF PUBLIC HEALTH.

All workforce members, as a condition of employment, are required to sign the confidentiality agreement.

Copies of the agreement shall be maintained in the workforce member’s personnel file.

Where required by HIPAA or Texas law, contractors who meet the definition of a business associate shall be required to execute a business associate or chain of trust partner agreement. All other contractors must sign a confidentiality agreement if the service involves the incidental use or disclosure of PHI.

**Protection of Protected Health Information – Hard Copies:** All PHI shall be maintained in a confidential manner that prevents unauthorized disclosure, either internally or to third parties. TEXAS A&M SCHOOL OF PUBLIC HEALTH shall make all reasonable efforts to secure records containing PHI.

All PHI in hard copy form shall be kept in locked files with the number of keys limited to workforce members whose work requires regular access to the information.

Documents shall be destroyed in a method that induces complete destruction of the information when the information is no longer needed.

**Procedure if a Breach is Alleged:** All breaches of confidentiality shall be reported to any supervisor, or the Privacy Officer.

Any workforce member receiving an allegation of a breach of confidentiality or having knowledge or a reasonable belief that a breach of confidentiality of PHI may have occurred shall immediately notify the Privacy Officer.
If it is determined that a breach of confidentiality of PHI has occurred, disciplinary action shall be taken in accordance with TEXAS A&M SCHOOL OF PUBLIC HEALTH disciplinary OPERATING PROCEDURE.

The Privacy Officer shall retain documentation of all allegations that have been made and any action taken in a master employee HIPAA complaint file and in the workforce member’s personnel file. A separate, secure file shall be maintained for documentation concerning violations by non-employees.
CONFIDENTIALITY AGREEMENT

I have read and understand [Name of Physician ("TEXAS A&M SCHOOL OF PUBLIC HEALTH")]) Confidentiality OPERATING PROCEDURE on the use, collection, disclosure, storage, and destruction of Protected Health Information ("PHI").

I agree to follow the Confidentiality OPERATING PROCEDURE and all related policies. I agree that while I am employed or have privileges at TEXAS A&M SCHOOL OF PUBLIC HEALTH, I will not reveal or disclose PHI to any person except as authorized by this OPERATING PROCEDURE and Texas and federal law.

I further understand that my obligations to maintain the confidentiality of PHI will continue after my employment or association with TEXAS A&M SCHOOL OF PUBLIC HEALTH ends.

Finally, I understand that unauthorized use or disclosure of PHI may result in disciplinary action, which may include termination of employment or contract, the imposition of civil and criminal fines pursuant to Texas and federal laws, and reporting to any appropriate professional licensing board.

______________________________
Employee Signature

______________________________
Employee Name

______________________________
Date

I have discussed TEXAS A&M SCHOOL OF PUBLIC HEALTH Confidentiality OPERATING PROCEDURE and the appropriate use, collection, disclosure, storage, and destruction of PHI with named employee or workforce member. I have also discussed the consequences of a breach and provided an opportunity for questions.

______________________________
Privacy Officer’s Signature
BREACH NOTIFICATION OPERATING PROCEDURE

PURPOSE:
To establish a breach notification process applicable to Unsecured PHI.

APPLICABILITY:
This OPERATING PROCEDURE applies to TEXAS A&M SCHOOL OF PUBLIC HEALTH and his/her business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use or disclose Unsecured PHI.

DEFINITIONS:

Breach: means the unauthorized acquisition, access, use or disclosure of 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.

Data Disposed: includes discarded paper records or recycled electronic media.

Data in Motion: includes data that is moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange.

Data at Rest: includes data that resides in databases, file systems, flash drives, memory, and any other structured storage method.

Data in Use: includes data in the process of being created, retrieved, updated, or deleted.

Law Enforcement Official: means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, empowered by law to: (1) Investigate or conduct an official inquiry into a potential violation of law; (2) Prosecute or otherwise conduct an official inquiry into a potential violation of law; or (3) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Unsecured Protected Health Information: means PHI that is not secured through the use of a technology or methodology specified by the Secretary of HHS (“Secretary”) guidance.
BREACH NOTIFICATION OPERATING PROCEDURE

General Duty.

In the event TEXAS A&M SCHOOL OF PUBLIC HEALTH discovers a breach of Unsecured PHI (i.e., PHI that is not secured through the use of a technology or methodology specified by the Secretary of HHS), TEXAS A&M SCHOOL OF PUBLIC HEALTH will notify each individual whose Unsecured PHI has been, or is reasonably believed by TEXAS A&M SCHOOL OF PUBLIC HEALTH to have been, inappropriately accessed, acquired, or disclosed as a result of such breach, as outlined below.

The notification requirements of the OPERATING PROCEDURE apply to breaches committed by TEXAS A&M SCHOOL OF PUBLIC HEALTH Business Associates. Following discovery of a breach, business associates must: (1) notify TEXAS A&M SCHOOL OF PUBLIC HEALTH of the breach and identify those individuals whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been breached; and (2) upon receiving TEXAS A&M SCHOOL OF PUBLIC HEALTH prior written approval, notify individuals whose unsecured PHI has been, or is reasonably believed by Business Associate (upon conferring with TEXAS A&M SCHOOL OF PUBLIC HEALTH Privacy Officer) to have been breached as outlined below.

Determination of a Breach.

A “breach” includes the unauthorized acquisition, access, use, or disclosure of PHI which compromises, (i.e., poses a significant risk of financial, reputational, or other harm to the individual, 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.

In the event TEXAS A&M SCHOOL OF PUBLIC HEALTH or one of TEXAS A&M SCHOOL OF PUBLIC HEALTH business associates discovers a breach, TEXAS A&M SCHOOL OF PUBLIC HEALTH Privacy Officer shall: (1) review such breach; (2) perform a risk assessment, and (3) unless otherwise provided in the Business Associate between TEXAS A&M SCHOOL OF PUBLIC HEALTH and his/her Business Associate determine whether the breach requires providing notice, who must be notified and who must provide the notice.

PERFORMANCE OF RISK ASSESSMENT:

In order to determine whether a breach of PHI, requires notice, the Privacy Officer shall:

Step 1: Determine Whether a Breach of the HIPAA Privacy Rule Occurred. For an acquisition, access, use, or disclosure of PHI to constitute a breach, it must constitute a violation of the HIPAA Privacy Rule.

Step 2: Determine whether the Improper Acquisition, Use or Disclosure Constitutes a “Breach” for Purposes of HITECH. Under HITECH, the term “breach” does not include:
1. Unintentional acquisitions, access, or uses of PHI by an employee or individual acting under the authority of TEXAS A&M SCHOOL OF PUBLIC HEALTH or a Business Associate of TEXAS A&M SCHOOL OF PUBLIC HEALTH if:

   (a) The acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of a workforce member while working under the authority of TEXAS A&M SCHOOL OF PUBLIC HEALTH or TEXAS A&M SCHOOL OF PUBLIC HEALTH Business Associate; and

   (b) The information is not further acquired, accessed, used, or disclosed by any person.

2. Inadvertent disclosures from an individual otherwise authorized to access PHI at a clinic or other facility operated by TEXAS A&M SCHOOL OF PUBLIC HEALTH or a TEXAS A&M SCHOOL OF PUBLIC HEALTH Business Associate if:

   (a) The disclosure is to another similarly situated individual at the same clinic/facility; and

   (b) The information is not further acquired, accessed, used or disclosed by any person without patient authorization.

3. A disclosure of PHI where TEXAS A&M SCHOOL OF PUBLIC HEALTH or a TEXAS A&M SCHOOL OF PUBLIC HEALTH Business Associate (upon conferring with TEXAS A&M SCHOOL OF PUBLIC HEALTH Privacy Officer) has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. TEXAS A&M SCHOOL OF PUBLIC HEALTH Privacy Officer should complete the analysis on Step 4 below in making this determination.

4. If information is de-identified in accordance with 45 C.F.R. §165.514, it is not PHI and thus any inadvertent or unauthorized disclosure of such information will not be considered a breach.

To the extent an acquisition, use or disclosure falls into one of the above four (4) categories, Privacy Officer need not provide notice to individual or continue with subsequent steps. However, Privacy Officer should document the acquisition, use or disclosure in the individuals Accounting Log in accordance with 45 C.F.R. §165.528.

**Step 3: Determine the Nature of Data Elements Breached.** A use or disclosure of PHI that does not include the following identifiers does not compromise the security or privacy of the PHI:
(a) Names;
(b) Postal address information, other than town or city, State;
(c) Telephone numbers;
(d) Fax numbers;
(e) E-mail addresses;
(f) Social security numbers;
(g) Medical record numbers;
(h) Health plan beneficiary numbers;
(i) Account numbers;
(j) Certificate/license plate numbers;
(k) Vehicle identifiers and serial numbers;
(l) Device identifiers and serial numbers;
(m) Web URLs;
(n) Internet Protocol (IP) address numbers;
(o) Biometric identifiers, including finger and voice prints;
(p) Full face photographic images and any comparable images;
(q) Date of birth; or
(r) Zip code.

A. To the extent that the use or disclosure does not involve the use or disclosure of the above identifiers, the Privacy Officer need not continue to Step 4 and notice to the individual is not required. However, the Privacy Officer shall log the improper use or disclosure in the individual's Accounting log. In addition, the Privacy Officer shall document in a Risk Assessment log demonstrating in the Risk Assessment documentation that the use or disclosure of PHI did not include the above identifiers.

B. To the extent, the use or disclosure of PHI includes the above referenced identifiers, the Privacy Officer shall perform the following steps of the risk assessment.

**Step 4:** Determine the Likelihood that the PHI is Accessible and Useable by Unauthorized Persons. PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:

1. Electronic PHI has been encrypted as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

---

5 The following guidance is based on the Guidance and Request for Information set forth in 74 FR 162, August 24, 2009). Please note that the following may need to be updated as the Secretary issues additional guidance.

6 45 C.F.R. 164.304, definition of “encryption.”
(a) Valid encryption processes for data at rest are consistent with NIST Special Publication 800–111, Guide to Storage Encryption Technologies for End User Devices.\(^7\)

(b) Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800–52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800–77, Guide to IPsec VPNs; or 800–113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140–2 validated.\(^8\)

2. The media on which the PHI is stored or recorded has been destroyed in one of the following ways:

(a) Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

(b) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800–88, Guidelines for Media Sanitization,\(^9\) such that the PHI cannot be retrieved.

To the extent PHI is rendered unusable, unreadable, or indecipherable by the above materials, it is not necessary to provide notice.

**Step 5: Harm To Individual.** The Privacy Officer must assess whether the acquisition, use, or disclosure poses a significant risk of financial, reputational, or other harm to the individual. Factors to consider include:

(a) The identity of who impermissibly used or disclosed the PHI or who impermissibly received the PHI. (If, for example, PHI is impermissibly disclosed to another entity governed by HIPAA, there may be less risk of harm to the individual. In contrast, if PHI is impermissibly disclosed to any entity or person that does not have similar obligations to maintain the privacy and security of the PHI, the risk of harm to the individual is much greater);

(b) The likelihood that unauthorized individuals will know the value of the information and use or sell it;

(c) The type of information (i.e., mental health services, substance abuse, or sexually transmitted diseases). However, in performing the risk assessment, the Privacy

\(^7\) Available at [http://www.csrc.nist.gov/](http://www.csrc.nist.gov/).
Officer should keep in mind that many forms of PHI (not just information about sexually transmitted diseases and similarly sensitive PHI) should be considered sensitive for purposes of the risk of reputational harm—especially in light of fears of employment discrimination;

(d) Broad reach of potential harm (blackmail, disclosure of private facts, disclosure of sensitive PHI, mental pain and emotional distress, address information for victims of abuse, humiliation, identity theft);

(e) Likelihood harm will occur (which depends on manner of actual breach and types of data such as SS#, passwords, mother’s maiden name and information useful for identity theft); and

(f) If identity theft or fraud is a risk, review www.whitehouse.gov/obm/memoranda/fy2006/task_force

Step 6: Review the physical, technical, and procedural safeguards employed by TEXAS A&M SCHOOL OF PUBLIC HEALTH or TEXAS A&M SCHOOL OF PUBLIC HEALTH Business Associate (as applicable). The Privacy Officer should review appropriate counter-measures, such as monitoring systems for misuse of the PHI and patterns of suspicious behavior that can be taken by TEXAS A&M SCHOOL OF PUBLIC HEALTH.

Step 7: Mitigate Harm. Upon determining that an impermissible use or disclosure occurred, the Privacy Officer shall take immediate steps to mitigate the impermissible risk or disclosure.

When possible, the Privacy Officer shall obtain the recipient’s written satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed. If such mitigating steps eliminate or reduce the risk of harm to the individual to a less than a “significant risk,” then it is not necessary for the Privacy Officer to provide notice to the individual. In such event, the inappropriate disclosure or use should be noted in the individual’s Accounting Log. In the event the Privacy Officer determines that a “significant risk” still exists, the Privacy Officer shall post notice in the manner set forth below.

When appropriate, the Privacy Officer should consider purchasing theft identity insurance for individuals.

Step 8: Documentation. The Privacy Officer shall document his/her Risk Assessment process and conclusions. To the extent that the Privacy Officer determines that it is not necessary to provide notice, the Privacy Officer’s Risk Assessment must demonstrate the factors considered in determining that breach notification was not required.
FURTHER INFORMATION:

For questions, additional detail, or to request changes to this policy, please contact A&M School of Public Health Office of Research Office or HIPAA Compliance Office

CROSS REFERENCES:

Other Policies in this Manual may have specific application and should be referred to especially;
- Computer and Network Security,
- Health Insurance Portability and Accountability Act (HIPAA)
- Use of Institutional Data
- HIPAA and Research at TEXAS A&M College of Medicine, College of Dentistry, Texas A&M Physicians Practice

First Published for Review: July 15, 2015
Effective Date: January 12, 2016
Date Approved: January 12, 2016
Date Published: January 12, 2016

Revision History (and effective dates):

Preceding HIPAA Manual Published by TAMHSC in Spring 2013
Original SPH HIPAA Compliance Program enacted in July 2013

REFERENCES

https://www.umaryland.edu/media/umb/oaa/hrp/documents/study-tools-docs/hipaaflowchart.pdf