Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**HIPAA Privacy and Security Policy and Procedures**
Regulation and Procedure Number:	**URP: 01.270**
Policy Owner:	**Finance and Administration, Office of General Counsel, and Student Life**

POLICY STATEMENT

These University Regulation and Procedures ("***URP***") are designed to specify Texas Woman's University's ("***TWU***" or the "***University***") compliance with the Health Insurance Portability and Accountability Act of 1996 ("***HIPAA***") and as amended under the American Recovery and Reinvestment Act of 2009 and by Section 181.001(b) of the Texas Health and Safety Code. These URP provide for the protection and security of a person's medical information. The establishment of these URP demonstrates TWU's commitment to ensuring individuals' have access to their medical information and are provided protections regarding its use and disclosure. These URP meet the Department of Health and Human Services requirements that TWU communicate clear and specific compliance standards and procedures to applicable parties.

TWU is a hybrid entity, as its primary function is not health care; however, some components of TWU use, or may use, or disclose protected health information ("***PHI***"). TWU consists of health care service components, other services that support the business operations of the health care components, as well as components that are not related to health care services. Only health care components and those components that provide business support to the health care components must comply with all provisions of the privacy rule (see the list on p. ii). However, all TWU components should strive to protect the confidentiality and privacy of PHI consistent with these policies and procedures.

The release of protected information from the covered service or function of TWU to the non-covered service or function of TWU is considered a disclosure under the HIPAA Privacy Rule (the "***Privacy Rule***") for which an authorization must be obtained. However, if a non-health care TWU component provides business associate-like services to the health care component of TWU, and if it is so designated, an authorization is not needed, but the Privacy Rule applies to that component.

The Texas Medical Privacy Act supplements the federal requirements, and it considers a covered entity to be any entity or person that uses, possesses, or obtains PHI.

HIPAA regulations will be followed in administrative activities undertaken by assigned personnel when they involve PHI in any of the following circumstances: health information

privacy, health information security and health information electronic transmission. TWU employs appropriate and comprehensive security and privacy measures that build and maintain a commitment to achieve security and privacy of protected health information. (45 CFR 164.504)

The HIPAA Compliance Officer of TWU, in consultation with the General Counsel of TWU, shall define the health care components of the University and those entities that provide business associate type support services. The remaining components will be designated as non-covered components. The HIPAA Compliance Officer in consultation with the TWU General Counsel will also review this list annually, and will update it as needed. (45 CFR 164.504)

Health care components at TWU considered Covered Entities where HIPAA applies are:

- Student Health Services

These health care components will each maintain a list of their respective business associates.

These Policies shall apply to all health care components listed above. Additionally, all other components of the University that regularly deal with PHI shall consider the efficacy of these policies and, where applicable, comply with these policies to the extent appropriate. It is the goal of the University that, even where HIPAA is not specifically applicable to a particular University component, that component will strive for HIPAA compliance as if that component were actually a covered entity under HIPAA.

APPLICABILITY

This policy is applicable to TWU Faculty, Staff, Students, and Guests.

Table of Contents

Please refer to Appendix I for the Glossary and list of abbreviations used in this URP.

EXHIBITS (SAMPLE DOCUMENTS)

PROCEDURES

Each health care component of TWU must elaborate on any sections of this URP what its mission and scope requires. Additions made by health care components may be more restrictive than the requirements of this policy, but they cannot be less restrictive.

Each health care component must also create protocols and forms that comply with this URP, federal laws and regulations, and Texas laws and regulations, and that are consistent with its mission and its operations. Each covered health care component must also train its workforce in the use of its procedures and forms.

TWU will consider any breaches in the privacy and confidentiality of handling of PHI to be serious, and corrective action will be taken in accordance with University policies and URPs.

ADMINISTRATIVE REQUIREMENTS

TWU complies with the U.S. Department of Health and Human Services Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164, the Texas Medical Privacy Act, and any other applicable federal or state law or regulation. The following procedures are implemented to ensure the privacy of PHI regarding any individual receiving health care services from a health care component of TWU. (45 CFR 164.530)

Business Associate Contracts and other Arrangements (45 CFR 164.504)

A business associate ("***BA***") is a person or entity, other than a workforce member, that performs a function that involves PHI for a health care component of TWU.

Each health care component must establish a business associate agreement ("***BAA***") with each of their BAs, notwithstanding anything to the contrary, prior to using or disclosing PHI. The BAA must meet the legal standards of TWU and must be approved by the TWU General Counsel before it is executed.

The BAA must establish the permitted and required uses and disclosures of PHI by BAs. This use or disclosure must comply with all the federal and Texas privacy laws and regulations in the same way that the health care component must also comply. The contract must meet the requirements of 45 CFR 164.504 and must be approved by the TWU General Counsel prior to execution of the contract.

At a minimum, the BA must contractually agree:

- Not to use or further disclose PHI other than as permitted or required by the contract or as required by law;
- To use appropriate safeguards to prevent use or disclosure of the information other than as provided by the contract;
- To report to the health care component any use or disclosure of the information not provided for by the contract of which it becomes aware;

- That agents and subcontractors of the BA agree to the same restrictions and conditions that apply to the BA in respect to PHI that the agent or subcontractor receives or creates on behalf of the business associate;
- To make PHI available in accordance with the requirements imposed on the health care component;
- To make PHI available for amendment and incorporate any amendments to PHI in accordance with the same requirements imposed on the health care component;
- To make available the information required to provide an accounting of disclosures in accordance with the same requirements imposed on the health care component; and
- To provide the Secretary of Health and Human Services and the Privacy Officer of the health care component with access to all internal practices and records relating to PHI in order to determine whether the health care component is in compliance

At the termination of the contract, the BA must agree:

- To return or destroy all PHI;
- Not to retain copies of the information; and
- If the BA cannot return or destroy the PHI, to extend the protections of the contract to the information and to limit further disclosures.

The health care component must determine and document that the BA has provided satisfactory assurances that it is able to meet the requirements of the BAA and to protect the privacy of PHI. The BAA must authorize termination of the contract if the BA violates a material term of the contract.

If the health care component becomes aware of a BA's violation of the terms of the contract or of federal and Texas laws and regulations, it must take reasonable steps to prevent or to mitigate any improper use or disclosure of PHI. If reasonable steps to correct a BA's contractual violations are not successful in preventing or mitigating improper use or disclosure of PHI, the health care component must:

- Terminate the BAA, if feasible, or
- If termination of the BAA is not feasible, report the problem to the Secretary of Health and Human Services, and
- If appropriate, seek a protective order by referring the matter to the TWU General Counsel

The BA standard does not apply to disclosures made to another health care provider concerning the treatment of an individual patient, and it also does not apply to disclosures to health plans for payment purposes.

Personnel Designations

HIPAA Compliance Officer (45 CFR 164.530)

The TWU HIPAA Compliance Officer (the "***HCO***") is responsible for the development, implementation, revision of TWU Regulations and Procedures related to HIPAA

compliance. (45 CFR 164.530) The HCO shall be contacted if there is a complaint regarding HIPAA procedures and practices at TWU. (45 CFR 164.520) Questions regarding HIPAA provisions should be addressed to the HCO.

Changing Policies and Procedures

The TWU HCO is responsible for maintaining HIPAA compliance at TWU. If changes in federal or Texas laws or regulations require changes in these procedures, the TWU HCO will consult with necessary parties both within and outside the University to develop the required changes.

Changes in these procedures may also be requested by University management or by the management or Privacy Officer of any health care component within the University. Proposed changes will be submitted to the TWU HCO for consideration and development. Changes in these procedures must be approved by the Chancellor and President of TWU. The changes take effect on approval of the Chancellor.

Health care components within TWU must also develop a procedure for changing their HIPAA-related protocols and for updating forms, records, and agreements.

If changes in URPs materially affect the way in which workforce members carry out their duties, then the affected workforce members will be retrained to be in compliance with the changed URP(s). (45 CFR 164.530)

Documentation of Policies and Procedures

The TWU HCO must retain documentation of URP change(s) for a period of seven (7) years from the time the documentation was created, unless a longer period is prescribed by federal or Texas regulations.

TWU and its health care components must maintain the regulations and procedures required by the HIPAA Privacy regulations in written or electronic form. Whenever a communication is required to be in writing, TWU or its health care components, as appropriate, shall maintain a record of this communication, or an electronic copy, as documentation. Whenever an action, activity, or designation is required to be documented, TWU or its health care components, as appropriate, shall maintain a written or electronic record of such action, activity, or designation. (45 CFR 164.530)

Privacy Officer and Contact Person (45 CFR 164.530)

Each health care component of TWU shall designate a Privacy Officer, who will maintain accountability for privacy within the department or clinic. This individual may share this role with other duties, as long as a conflict of interest is not created by his or her multiple duties. In cases where a conflict of interest might arise, the Privacy Officer shall consult with the health care component's manager and with the TWU HCO so that an alternate person may be designated to assume those duties that create the conflict of interest.

Each health care component of TWU shall also designate a Contact Person, who may be the same individual as the Privacy Officer. The role of the Contact Person is to accept complaints.

The Privacy Officer will oversee the health care component's Privacy Program, including:

- Developing and implementing privacy policies and procedures, in accordance with federal and Texas privacy requirements;
- Receiving and processing consents;
- Receiving and processing restrictions on consents;
- Receiving and processing revocations of authorizations;
- Training of all members of the component's workforce who come into contact with PHI;
- Approving all disclosures that do not require a consent, authorization, or opportunity for the patient to agree or object;
- Providing information related to the Notice of Privacy Practices;
- Mitigating the effects of all disclosures that are not compliant with federal or Texas law or with the policies or procedures of the department or clinic;
- Conducting, at least annually, a review of the implementation of the "minimum necessary" requirements;
- Conducting, at least annually, a review of the component's access procedures and relevant records;
- Guiding and assisting in the identification, implementation, and maintenance of privacy policies and procedures in conjunction with the component's management, the TWU General Counsel, and the TWU HIPAA Compliance Officer;
- Reviewing all patient information security plans to align security and privacy practices;
- Performing initial and periodic risk assessments or "privacy audits" and conducting ongoing compliance monitoring activities;
- Overseeing that the component maintains appropriate consent and authorization forms, information notices, and materials that reflect current organization and legal practices and requirements; and
- Overseeing compliance with privacy practices and application of sanctions for failure to comply with privacy practices.

This list provides an overview of the duties of the Privacy Officer and is not comprehensive.

Security Officer and TWU Information Security Officer

A health care component may elect to have the Privacy Officer also serve as the component's Security Officer. The TWU Information Security Officer shall serve as the overall Security Officer for the University for HIPAA purposes and for any health care component that does not select its own Security Officer.

The Privacy Officer for the covered entity is responsible for developing and implementing HIPAA privacy regulations approved by the HIPAA Committee, initial and ongoing HIPAA

privacy training, monitoring the use and disclosure of PHI and investigating HIPAA privacy concerns and complaints.

The Security Officer for the covered entity is responsible for developing and implementing HIPAA security regulations, providing initial and on-going HIPAA security training, monitoring security of TWUs electronic PHI and investigating HIPAA security breaches, concerns, and complaints.

The TWU Information Security Officer is responsible for protecting the confidentiality, integrity, and availability of TWU information systems and electronic PHI ("***EPHI***"), as well as promoting TWU information systems compliance with applicable federal and state laws and regulations.

The TWU Information Security Officer is responsible for:

- Conducting evaluations to avoid a TWU information system from compromising the confidentiality, integrity, or availability of any other TWU information systems;
- Developing, documenting, and disseminating security policies, procedures, and standards for authorized users of TWU information systems and the data contained therein (in conjunction with information system owners);
- Coordinating the selection, implementation, and administration of TWU security controls;
- Organizing regular TWU security awareness and training; and
- Coordinating with TWU's HCO and the HIPAA Committee to support compliance with security policies, procedures, and controls found in the HIPAA Privacy Rule.

The TWU Information Security Officer, with input from the HCO, is responsible for:

- Reviewing the TWU HIPAA Security Policy Manual on an annual basis and, in accordance with Institutional policies and regulations, updating the Manual as necessary. The TWU Information Security Officer shall also make these policies and procedures readily available for all workforce members, including BAs and any third party individuals;
- Developing and implementing regulations and procedures necessary to appropriately protect the confidentiality, integrity, or availability of any other TWU information systems; and
- Overseeing that adequate physical security controls exist to protect TWU's EPHI by implementing a risk management process and conducting periodic risk analysis.

HIPAA Privacy and Security Committee

TWU has created and will maintain a HIPAA Committee, which is responsible for HIPAA Privacy and Security Policies and oversight and is chaired by the HCO.

The HIPAA Committee, in conjunction with the Information Security Officer and the HCO, will develop and maintain a Breach Notification Process to be used in the event of an unauthorized disclosure of EPHI.

Documented Privacy Training (45 CFR 164.530)

The Privacy Officer of each TWU health care component covered by HIPAA is responsible for ensuring that members of the component's workforce are properly trained in the requirements of federal and Texas law. The Privacy Officer will document each training session and the names of the workforce members who completed training. All members of the workforce who come into contact with PHI in performing their job functions shall be trained on the privacy laws and the procedures regarding PHI. Training documentation will be maintained within the health care component's privacy records for at least seven (7) years from the date of training. The Privacy Office will provide a summary annual report of the component's training activities to the TWU HIPAA Compliance Officer.

The term "***workforce***" includes, employees, students, volunteers, and any other individual performing work for the health care component, who is under direct control of the component's management, regardless of whether or not they are paid. (45 CFR 160.103)

Training shall meet the following requirements:

- All current members of the workforce shall complete training no later than the compliance date for the covered entity and will undergo training at least once every two (2) years;
- All newly hired employees must complete HIPAA training prior to performing any duties involving PHI;
- The supervisor of the workforce member is responsible for initiating training;
- Workforce members whose duties are affected by a material change in the privacy laws or policies shall be retrained within two (2) months after the change becomes effective;
- Workforce members who have violated privacy laws, policies, or procedures shall be retrained and (a) the individual will have no access to PHI once a violation has occurred until such individual is retrained and (b) such individual must be retrained within thirty (30) days;
- Training methods may include, but are not limited to, recording sessions, face-to-face training, online sessions, and communications via email, newsletters, or other documents;
- All trainings and participants in trainings will be tracked. The Privacy Office for each health care component is responsible for notifying the unit's supervisor if privacy training is not completed or renewed by members of the workforce under their supervision; and
- Supervisors/Directors of each health care component are responsible for ensuring each member of the workforce under their supervision completes or renews their privacy training in a timely manner.

Privacy Training includes:

- Orientation: Orientation for all new employees with HPI duties includes HIPAA Privacy and Security training, and each new member of the workforce will sign the

Confidentiality Agreement. Training should be completed (a) prior to handling PHI and (b) within thirty (30) days of hire;

- Research: All clinical researchers, co-investigators and research staff must complete the HIPAA Privacy module contained within the Collaborative IRB Training Initiative ("***CITI***").
- Renewal Training: TWU workforce members are required to take refresher training at least once every two years.
- Additional Training: Additional training will be scheduled as needed to address non-compliance issues, to review any changes to federal or state statutes, and/or to minimize the risk of future non-compliance.

Failure to Comply with Training and/or timelines for training may result in in one or more of the following actions until the required training is completed:

- A workforce member may be reported to her or his supervisor for corrective action;
- Suspension of a provider's billing privileges;
- The HIPAA Compliance Committee and /or HIPAA Compliance Officer may be notified; and
- The individual will not be permitted to handle PHI.

TWU health care components must:

- Ban the disclosure of PHI for remuneration, except that covered entities may disclose PHI to other covered entities for treatment, payment, health care operations, insurance or HMO functions, or as authorized or required by federal or state law;
- Provide notice to individuals that their PHI is subject to electronic disclosure and obtain authorization for any electronic disclosure of PHI (apart from disclosures of PHI to other covered entities for treatment, payment, health care operations, insurance or HMO functions, or as authorized or required by federal or state law); and
- Health care providers provide individuals with access to their PHI within fifteen (15) business days of their request.

Documentation of Signed Employee Confidentiality Statement

All workforce members who come into contact with PHI in performing their job function, and who have completed required training in confidentiality procedures, shall acknowledge in writing that they have completed their training, that they have received a copy of the health care component's confidentiality and security agreement, that they understand its contents, and that they will comply with its provisions and with the provisions of federal and Texas law, University policy, and the health care component's policies and procedures.

The component shall provide a form for this purpose and shall keep it on file for a period of seven (7) years from the date when it was signed.

Notice of Privacy Practice

Patient Notice of Privacy Practices

An individual has a right to adequate notice of the uses and disclosures of PHI that may be made by health care components of TWU, and of the individual's rights and TWU's responsibilities with respect to PHI. TWU health care components are required to provide a Notice of Privacy Practices ("***NPP***") to all individuals, as well as to other individuals requesting a copy. Persons who register patients or clients will be responsible for distributing a copy of the NPP to all individuals.

The HCO will develop a standard form of NPP for the University, a copy of which shall be attached as Exhibit 3 to these policies. Each health care component can adopt its own NPP or revise the existing general form, with the consent of the HCO, as follows.

General Requirements

TWU health care components must:

Develop the required NPP, forms, procedures, and workforce training related to this section;

- Provide the notice no later than the date of the first service delivery, including service delivered electronically to an individual and, if possible, determine if a language barrier exists;
- Make a good faith effort to obtain an initial written acknowledgement of the receipt of NPP from the individual and document the receipt of the NPP, using an appropriate acknowledgement form and filing system;
- Have the NPP available at the service delivery site for individuals to take with them;
- Post the NPP in a clear and prominent location in each health care provider's location where it is reasonable to expect individuals seeking service from the TWU health care component to be able to read the NPP (Electronic NPPs must be printed and displayed for individuals to read);
- Whenever the NPP is revised, provide the new NPP to all patients or clients on their next visit on or after the effective date of the revision; and
- Post the NPP on the TWU website.

If an individual is treated on an emergency basis, the TWU health care component may delay providing the NPP and receiving an acknowledgement until a practical time.

Electronic Notice

- If electronic mail is used to send a copy of the NPP to an individual, the electronic mail communication must comply with Uses and Disclosures Section of this URP. If the TWU health care component becomes aware that the email transmission was not successful, it must provide a paper copy of the NPP to the individual.

- Electronic notice by the TWU health care component satisfies the notice requirement if receipt of the NPP is documented and retained by the health care component.
- The individual who is the recipient of an electronic notice retains the right to obtain a paper copy of the NPP from the TWU health care component on request.

Notice of Privacy Practices (NPP) Requirements

The NPP must be written in plain language and must contain the following elements:

- Header. "THIS NOTICE OF PRIVACY PRACTICE (NPP) DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY." This header must be at the top of the notice, in capital letters, or otherwise in a prominent location on the notice.
- Consent. Texas law requires that individuals provide their consent to receive treatment from a health care organization. The NPP provides the individual the opportunity to acknowledge their consent in writing.
- Uses and disclosures. The NPP will contain:
    - A description of the types of uses and disclosures that the TWU health care component is permitted to make, including at least one example for each of the following purposes: Treatment, Payment, and health care Operations ("***TPO***");
    - A description of each of the purposes for which the TWU is permitted or required to use or disclose PHI without the individual's written authorization;
    - A statement that other uses and disclosures will be made only with the individual's written authorization, and that the individual may revoke such authorization, using the appropriate forms;
    - A statement that the TWU component may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual; and
    - A statement that the individual's PHI is subject to electronic disclosure.

- Individual rights. The NPP must contain a statement of the individual's rights with respect to PHI and a brief description of the procedures that the individual would use to exercise these rights:
    - The right to request restrictions on certain uses and disclosures of PHI;
    - The right to receive confidential communications of PHI;
    - The right of the individual to inspect and obtain a copy of the individual's own PHI;
    - The right to request an amendment to PHI;
    - The right to receive an accounting of disclosures of PHI; and
    - The right of an individual, including an individual who has agreed to receive the NPP electronically, to obtain a paper copy of the NPP on request.

- Health care component's duties. The NPP must contain a statement that the TWU health care component:
    - Is required by law to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy practices with respect to PHI and to notify affected individuals following a breach of unsecured PHI;
    - Is required to abide by the terms of the NPP currently in effect;
    - Reserves the right to change the terms of its NPP and to make the new provisions effective for all PHI that it maintains;
    - Will provide individuals with a revised NPP and how it will do so; and
    - May correct health information about an individual upon such individual's request based on such individual's belief that the health information is incorrect; *provided*, that TWU may decline such request within sixty (60) days.

- Complaints. The NPP must contain a statement that individuals may complain to the TWU health care component, and to the Department of Health and Human Services, if they believe that their privacy rights have been violated, a brief description of how the individual may file a complaint with the TWU health care component or the TWU Office of Compliance, and a statement that the individual will not be retaliated against for filing a complaint.

- Contact. The NPP must contain the name, or title, and telephone number of a person or office to contact for further information.

- Effective date. The NPP must contain the date on which the NPP is first in effect, which may not be earlier than the date on which the NPP is printed or otherwise published.

Receive Treatment without Signing Consent

A patient may receive treatment from a TWU health care component without signing a consent for use or disclosure form if the health care component has attempted to obtain the consent form but has been unable to obtain such consent due to emergency situations, or substantial barriers to communicating with the patient and in the exercise of professional judgment that the consent is clearly inferred from the circumstances.

Documentation of Notice

The TWU health care component must document compliance with the notice requirements by retaining copies of the NPP's they have issued. Those persons who register patients or clients shall be responsible for distributing the NPP to all patients or clients, documenting receipt of the acknowledgment form in an appropriate filing system, and retaining the original signed form in the patient's or client's file or record. If the individual refused to sign the acknowledgement form or if it was otherwise impossible to receive an acknowledgement from the individual, the health care component must document on the acknowledgement form the reason why written acknowledgement could not be received.

Revision of Notice

The TWU health care component must promptly revise and make available its NPP whenever there is a material change to its uses or disclosures, an individual's rights, TWU's legal duties, or other privacy practices that are stated in the NPP. Except when required by law, a material change to a term of the NPP may not be implemented prior to the effective date of the NPP in which such material change is reflected.

Consent for the Use and Disclosure of PHI

TWU health care components will obtain written consent prior to using and/or disclosing a student's PHI for health care TPO purposes.

Consents for the use and disclosure of PHI for TPO must have the following elements for the consent to be effective:

- Inform the patient or patient's personal representative that PHI may be used and disclosed to carry out TPO;
- Specify the type of records that will be used or disclosed (e.g., medical records);
- Identify the class of parties to whom disclosure may be made;
- Refer the patient or personal representative to the NPP for a more complete description of such uses and disclosures;
- State the patient or personal representative may request a restriction be placed on the consent (see section regarding Patient Right to Request Restriction of Uses and Disclosures); and
- The consent must be signed and dated by the patient or personal representative.

Specially Protected Medical Records

Substance Abuse Treatment Records Confidentiality

The HIPAA Privacy Regulations consider Substance Abuse Treatment Records to be a unique subset of PHI, which must be treated differently from other types of PHI. A Substance Abuse Treatment Record shall be confidential and be disclosed only for the purposes expressly authorized by the individual who is the subject of the Substance Abuse Treatment Record.

The content of any Substance Abuse Treatment Record may be used and disclosed in accordance with the prior written consent of the individual for TPO. For any other use or disclosure of a Substance Abuse Treatment Record, the TWU health care component or the record custodian must have an authorization from the individual granting the health care component permission to disclose the information prior to the release of any portion of the Substance Abuse Treatment Record.

TWU may, however, disclose the Substance Abuse Treatment Record without the individual's authorization if:

- Medical personnel are required to treat the individual in an emergency situation and require the information for such individual's treatment;
- Qualified personnel are conducting management audits, financial audits, or program evaluation, but such personnel may not identify, directly or indirectly, any individual receiving treatment in any report of such research, audit, or evaluation, or otherwise disclose individual identities in any manner;
- A person is authorized by an appropriate order of a court of competent jurisdiction to receive the information in the Substance Abuse Treatment Record; or
- TWU must report the information in the Substance Abuse Treatment Record by law.

Other Specially Protected Medical Records

The following medical records are subject to special confidentiality protection and shall not be disclosed except as permitted by law:

- Psychotherapy notes;
- Mental health records; and
- HIV/AIDS records.

TWU health care components should contact the TWU Office of General Counsel with questions regarding using or disclosing these records.

De-Identification of PHI (45 CFR 164.502, 164.514)

PHI is rendered anonymous whenever its identifying characteristics are completely removed. PHI must be de-identified prior to disclosure to non-authorized users. De-identified PHI should be used for any permitted purpose whenever this is possible and feasible.

All personnel must strictly observe the following standards for de-identification of PHI. To de-identify PHI, the following identifiers of the patient must be removed:

- Name
- Street address, city, county, and zip code. Exceptions are:
    - States
    - City and/or county, if they include multiple zip codes and more than 20,000 people live in an area in which combined zip codes have the same first three digits
- Names of relatives and employers
- All elements of dates, except the year
- Telephone number
- Fax number
- Email address
- Social security number
- TWU identification number or medical record number
- Health beneficiary plan number

- Account numbers
- Certificate or license number
- Vehicle identifiers, including license plate numbers
- Device ID and serial number
- Universal Resource Locators (URLs)
- Identifier Protocol (IP) addresses
- Biometric identifiers
- Full face photographic images and other comparable images
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and equivalent geocodes
- Any other unique identifying number, characteristic, or code

Whenever possible, de-identified PHI should be used for routine reporting and for quality assurance monitoring or audits.

An authorized user who wishes to encrypt PHI to de-identify it must ensure that the encryption code is not based on information about the individual whose information is being de-identified, and that the code cannot be translated so as to identify the individual.

Re-identification of Protected Health Information (45 CFR 164.502(c))

A health care component may assign a code or other means of record identification to allow information de-identified to be re-identified by the covered entity, provided that the code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and the health care component does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

Texas Health and Safety Code, Chapter 181, requires the individual's consent to apply a re-identification code to the individual's de-identified PHI.

Authorization Requirements for Use and Disclosure (45 CFR 164.508)

The HCO shall develop a standard form of patient authorization, a copy of which shall be attached as Exhibit 2. Each TWU health care component may, with the consent of the HCO, develop the necessary procedures, forms, and training of their workforce members to implement the requirements for processing authorizations and using them for the disclosure of PHI, as discussed in the following sections.

General Requirements

An authorization shall be required for release of PHI to all health care providers, but it is not required for information to be accessed by an attending physician who makes a referral. The referring physician shall always have access to a patient's or client's PHI that is created by a specialist or consulting physician. If the specialist or consulting physician, however, is not on the workforce at TWU, that physician may require the

individual to sign an authorization to release PHI to a referring physician at a TWU health care component.

A patient or client must always sign an authorization to release PHI for reasons that are not related to TPO.

An individual requesting the release of the individual's own PHI must complete and sign the authorization form developed by the health care component. TWU's release of PHI must comply with the directives stated in the authorization. The TWU health care component must save all signed authorizations in the individual's record.

PHI may be disclosed without an authorization or without consent if the law requires such disclosure. All the cases in which this is required and permitted are stated elsewhere in this policy. The TWU health care component from which PHI is released by the health care component or by TWU must document the disclosure in its database used for this purpose.

Verification Requirements (45 CFR 164.514)

With the exception of PHI used for notification of an individual's family, a health care component that is releasing PHI must verify the identity of the party requesting it before the PHI is disclosed, and it must verify the authority of the individual to request the PHI. If a person requests PHI, and if this policy permits the release, the health care component must also require that the requesting party produce any documents or other representations that are required by the law or this policy. If the documents are in good form, and are properly signed and contain the correct content, the health care component can rely on their validity.

The health care component may rely on the identity of a government or public health official who presents proper identification, and may rely on the validity of a written request that is properly submitted on the letterhead of a government agency or public health authority.

The health care component may rely on the authority of a government or public health official or agency to request PHI, provided that the person or agency produces a statement identifying their legal authority. This might take the form of a warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, all of which may be assumed to represent proper legal authority.

The health care component must also exercise sound professional judgment in making disclosures to family of an individual, and it must make a good faith effort to verify the identity and authority of all other parties or agencies requesting PHI.

Requirements for Valid Authorization (45 CFR 164.508)

All authorizations must contain the required core elements. If the use or disclosure of an individual's PHI is for reasons other than TPO, it may also need to include the elements needed:

- For TWU's own uses and disclosures;
- By TWU for another entity's uses and disclosures; or
- For research that includes treatment.

Core Elements (45 CFR 164.508)

A valid authorization must contain at least the following elements and must be written in plain language:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful way. Requests for substance abuse records, including Employee Assistance Program records, require an explanation of the purpose for the request;
- The name or other specific identification of the person or the class of persons who are authorized to make the requested use or disclosure;
- The name or other specific identification of the person or the class of persons to whom a health care component of TWU may make the requested use or disclosure;
- An expiration date for the request. Unless it is revoked sooner, the authorization is valid for one (1) year after the date it is signed;
- A statement of the individual's right to revoke the authorization in writing, any exceptions to the right to revoke, and a description of the process that the individual would use to revoke the authorization;
- A statement that the information used or disclosed pursuant to the terms of the authorization may potentially be re-disclosed by the recipient and no longer protected by the HIPAA privacy regulations;
- Signature of the individual and the date; and
- If a personal representative signs for the individual, a description of the representative's authority to act for the individual.

Elements of Authorization Needed for TWU's Use and Disclosure (45 CFR 164.508)

If an authorization is requested by TWU or by one of its health care components for its own use or disclosure of PHI that it maintains, TWU must include the following requirements in the authorization in addition to the core elements:

- A statement that TWU or the health care component will not condition treatment, payment, or eligibility for benefits on the individual providing the authorization, unless one of these exceptions exist:
    - TWU may condition the provision of research-related treatment on provision of an authorization, or
    - TWU may condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of the PHI to such third party.
- A description of each purpose of the requested use or disclosure.
- A statement that the individual may:
    - Inspect or receive a copy of the PHI to be used or disclosed, and

    - Refuse to sign the authorization.
- If use or disclosure of the requested information will result in direct or indirect remuneration to TWU from a third party, a statement of such remuneration must be included

Elements of Authorization Requested by TWU for Disclosures by Other Entities (45 CFR 164.508)

If a TWU health care component requests an authorization be signed to obtain records from another covered entity for the health care component to carry out TPO, the health care component must include the following requirements in addition to the core elements:

- A description of each purpose of the requested use or disclosure;
- A statement that TWU or the health care component will not condition treatment, payment, or eligibility for benefits on the individual providing the authorization, except for an authorization on which payment may be conditioned; and
- A statement that the individual may refuse to sign the authorization

A copy of the authorization shall be provided to the individual for signature.

Defective Authorizations (45 CFR 164.508)

An authorization is considered defective and invalid if any material information in the authorization is known by TWU or any member of its workforce to be false, or if any of the following defects exist:

- The expiration date has passed or the expiration event is known by the TWU health care component to have occurred;
- The authorization has not been filled out completely or signed;
- The authorization is known by the TWU health care component to have been revoked;
- The authorization lacks any of the core elements; or
- The authorization violates the exception allowing compound authorizations for research purposes.

Compound Authorizations

An authorization for use and disclosure of PHI may not be combined with any other document to create a compound authorization, except for the following:

- An authorization for the use or disclosure of PHI created for research that include the treatment of the individual may be combined;
- An authorization for the use and disclosure of psychotherapy notes may only be combined with another authorization for use and disclosure of psychotherapy notes; or
- An authorization, other than that for a use and disclosure of psychotherapy notes, may be combined with any other such authorization.

Uses and Disclosures to Carry Out Treatment, Payment, or Health Operations (TPO)

HIPAA does not require an authorization for uses or disclosures of PHI for carrying out the following TPOs:

- Use or disclosure for the purpose of TWU's own TPOs;
- Disclosure for treatment activities of another health care provider;
- Disclosure to another covered entity or a health care provider for the payment activities of the entity receiving the information; or
- Disclosure to another covered entity for the health care operations of the entity receiving the information, as long as TWU and the covered entity has or had a relationship with the individual who is the subject of the PHI requested, the PHI pertains to that relationship and the disclosure is for either the first or second bullet points in the definition of "health care operations" or is for health care fraud and abuse detection or compliance.

However, some records maintained by TWU health care components are covered by the Family Educational Rights and Privacy Act ("***FERPA***") and not HIPAA. To cover all records maintained by TWU health care components, TWU requires that TWU workforce members obtain from each patient a signed Consent for the Use and Disclosure of PHI form prior to any use or disclosure of PHI to carry out TPO. Each TWU health care component shall develop the necessary Consent form and ensure that individuals receive it when they receive the NPP. See section regarding Consent for the Use and Disclosure of PHI for additional information.

Authorization Required Prior to Disclosure of Psychotherapy Notes

The TWU health care component may not use or disclose psychotherapy notes for purposes other than TPO without obtaining the patient's or client's signed authorization. The health care component also cannot disclose the psychotherapy notes to the patient or client without his or her signed authorization, as well as a written explanation of the risks or concerns of releasing such records to a non-trained individual.

Psychotherapy notes shall be maintained separately from other parts of the patient's medical record and will only be used and/or disclosed as allowed by law.

An authorization for use or disclosure of psychotherapy notes for TPO is not required under the following situations:

- The notes originated in the same TWU health care component that is carrying out treatment;
- The health care component is disclosing de-identified information from the notes for training programs in which students, trainees, or practitioners in mental health learn how to improve their skills. Only de-identified information may be used for such a purpose;

- The information will be used or disclosed to defend TWU in a legal action, or in any other proceeding in which TWU is a party;
- When the health care component must use or disclose the information as required by the Secretary of Health and Human Services to investigate, audit, or determine compliance with privacy regulations in the TWU health care component. However, psychotherapy notes relating to a student may not be released to the Department of Health and Human Services, as these are either medical records exempt from FERPA or they may be student records, both of which are not covered by HIPAA;
- The use or disclosure is required by law and is limited to relevant requirements of the law;
- The health care component makes the disclosure to a health oversight agency that is carrying out its responsibilities to oversee the treatment and operations of the originator of the psychotherapy notes. The health care component may be required to enter into BAAs with certain health oversight agencies;
- The health care component discloses information to coroners or medical examiners for the purpose of identifying a deceased individual determining a cause of death, or other duties authorized by law; or
- Specific requirements for disclosures that do not require an authorization from an individual are covered elsewhere in this policy.

Texas law protects communications between an individual and a professional providing treatment, and also protects records of the identity, diagnosis, evaluation, or treatment of an individual that is created or maintained by the professional. Texas law does not specifically address psychotherapy notes. Consequently, either HIPAA or FERPA regulations, whichever applies, will be followed by TWU health care components.

Authorization Required: Marketing

TWU and its health care components must obtain an authorization for any use or disclosure of PHI for marketing, except if the communication is in the form of:

- Providing information on health-related products and services in a face-to-face encounter with a patient or client;
- Providing a patient or client with refill reminders or other information on a drug or biologic that is currently being prescribed for the individual, as long as any financial remuneration received by TWU in exchange for making the communication is reasonably related to the cost of making the communication;
- Providing treatment of an individual by a health care provider, except where TWU receives financial remuneration in exchange for making the communication; or
- Providing promotional gifts of nominal value (pens, calendars, etc.).

If the marketing involves financial remuneration to TWU from a third party, the authorization must state that such remuneration is involved.

If TWU or a TWU health care component sends a written marketing communication through the mail, the communication must be sent in an envelope showing only the names and addresses of the sender and recipient and must (1) state the name and toll-free

number of the entity sending the marketing communication; and (2) explain the recipient's right to have the recipient's name removed from the sender's mailing list. The name shall be removed not later than the 5th day after the date TWU receives the request.

No written marketing communication may be sent to an individual without an authorization from the individual.

Authorization Required: Sale of PHI (45 CFR 164.508)

TWU and its health care components must obtain an authorization from an individual for any disclosure of such individual's PHI which constitutes a sale of such individual's PHI. Sale of PHI does not include a disclosure of PHI (1) for public health purposes, (2) for research purposes where the only remuneration received is a cost based fee to cover the cost to prepare and transmit the PHI, (3) for treatment and payment purposes, (4) for the sale, transfer, merger or consolidation of all or part of the covered entity, (5) providing access or accounting to an individual, and (6) as otherwise required by law. Such authorization must state that the disclosure will result in remuneration to TWU.

For example, if a pharmaceutical company offers to pay TWU for a list of patients who suffer from a particular affliction to be used to send discount coupons for a new medication directly to the patients, the arrangement between TWU and the pharmaceutical company would constitute a sale of PHI, and TWU would need to obtain specific patient authorization prior to providing the patient list. Alternatively, if TWU receives grant funding to conduct a program and, in return, must supply PHI to the funder, the provision of PHI is a byproduct of the arrangement and not a sale of PHI.

Uses and Disclosures of PHI

TWU workforce members may use and disclose PHI for health care TPOs only if the patient has signed and executed a Consent for Treatment, which includes a Use and Disclosure of PHI form that grants TWU or the TWU health care component and its workforce members the right to use and disclose PHI to carry out TPO. However, this consent only allows TWU or the health care component to use and disclose the "Minimum Necessary" amount of information required to complete the desired task. In compliance with Texas Health and Safety Code, Chapter 181, each TWU health care component shall develop the necessary Consent for Treatment form and ensure that individuals receive it when they receive the NPP.

Minimum Necessary Use and Disclosure (45 CFR 164.502, 164.514)

For purposes other than those listed below, the use and disclosure of PHI must be limited to the "Minimum Necessary" to satisfy the request or to complete the task. However, if the use or disclosure is for treatment purposes, no limitation to the use and disclosure shall apply. Each TWU health care component shall develop the necessary procedures and training to implement the requirements of this section.

The "Minimum Necessary" provisions SHALL NOT APPLY to the use and disclosure of PHI:

- For treatment purposes;
- For information requested by the individual to whom it belongs;
- For information requested pursuant to a valid authorization by the individual;
- For compliance with standardized HIPAA transactions;
- For required disclosures to the Department of Health and Human Services for enforcement purposes; or
- For instances required by law.

Minimum Necessary Use and Disclosure for Student Workers, Trainees, and Volunteers

Students, trainees, and volunteers are to adhere to the "Minimum Necessary" standard. They shall have access to records only to the degree that their duties require this access, and their supervisor shall train them in the privacy regulations of the TWU health care component in which they provide services. Individual health care components may implement a more restrictive policy with respect to student access to records.

Minimum Necessary Use and Disclosure for Educational Purposes

Faculty, staff, students, and trainees are to use de-identified information when in a classroom setting. A patient's identifying information is not needed for educational purposes.

Limitations of Use and Disclosure

All persons who handle PHI in any manner are expected to know and to abide by the following:

- Determining workforce access to PHI. Access to PHI shall be granted to persons based on their role, as determined by their supervisor, manager, and department head. The TWU health care component shall identify:
    - Those persons or classes of persons in the TWU workforce, including students, trainees, and volunteers, who need access to PHI to carry out their duties, and
    - For each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.
- Requests for Use or Disclosure of PHI. Except in emergency situations, any person requesting PHI from the medical record custodian must include the requestor's name, unique identifier, and the amount of information requested.
- Audits. The TWU health care component Privacy Officer shall be responsible for facilitating random checks to ensure that the minimum necessary standard is being applied when using and disclosing PHI.
- Requests for use and disclosure of entire medical records. Medical record custodians must not release the entire medical record to other TWU departments or BAs unless necessary.
- Good faith judgment. The medical record custodian may rely on the belief that the PHI requested is the minimum amount necessary to accomplish the purpose of the request when:

- The information is requested by a person previously approved for access;
- The information is requested by a professional providing professional services either as an employee or as a BA (such as the General Counsel);
- Making disclosure to entities or agencies associated with health related purposes that do not require consent, authorization, or opportunity to agree or object and also that the requesting official states that the information is the minimum necessary or is required by law;
- IRB or privacy board documentation represents that proposed research meets the minimum necessary standard;
- A requester asserts that the information is necessary to prepare a research protocol; or
- A requester asserts the information is for research on decedents.

Disclosures for Payment

Only the minimum necessary PHI shall be disclosed for payment functions, as provided by contractual agreements. Persons handling PHI for payment shall not discuss or disclose information about an individual's diagnosis or treatment. This policy shall apply to checks collected, credit card paper receipts, envelopes and invoices sent to patients or clients.

Uses and Disclosures Required by Law (45 CFR 164.512)

Members of the workforce at TWU may use or disclose PHI if this use or disclosure is required by law. The information used or disclosed must be limited in scope to comply with and to meet only the requirements of the law.

For PHI about a victim of crime or abuse, TWU may only release the minimum necessary amount of information to law enforcement officials, unless the law requires certain other information to be released, in which case TWU must comply with relevant statutes, laws, regulations, and subpoenas.

TWU workforce members must meet disclosure requirements related to victims of abuse, neglect, or domestic violence; judicial and administrative purposes; and law enforcement purposes.

In response to an order of a court or an administrative tribunal, TWU must release all information, but only that information, required by the order. The minimum necessary standard does not apply.

Uses and Disclosures for Public Health Activities (45 CFR 164.512)

TWU may use or disclose PHI for the public health activities outlined in HIPAA, including reporting disease to a public health authority.

In cases where information is not required by law, a TWU health care component may elect to release PHI without an individual's authorization to public health authorities who

are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability.

A public health authority is an agency of the United States government (e. g., the Food and Drug Administration or Centers for Disease Control), a State (e. g.., the Texas Department of Health), a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or a contract with, a public health agency. Under the direction of a public health authority, a TWU health care component may also release PHI to a foreign government agency that is acting in collaboration with the public health authority.

Examples of information that may be released under this section include, but are not limited to:

- Reporting a disease or injury;
- Reporting vital events, such as births or deaths;
- Conducting public health surveillance, investigations, or interventions;
- Notifying individuals at risk of contracting or spreading a disease, provided that other law authorizes such notification as necessary to carry out public health interventions or investigations;
- Tracking FDA-regulated products;
- Collecting or reporting adverse events from medications, foods, or supplements; product defects or problems; or biological product deviations;
- Enabling product recalls, repairs, or replacements by locating and notifying the individuals who received them; and
- Disclosing PHI at the request of the individual's employer for the limited purpose of workforce medical surveillance or the evaluation of work-related illness and injuries only to the extent that the employer is required to comply with federal and state law. Information disclosed under this provision must be limited to the provider's findings relating to medical surveillance or work-related illness or injury. The individual must receive written notice that the information will be disclosed to the employer.

In all cases, the disclosure must be limited to the minimum necessary, or to the information specifically required by law. The TWU General Counsel shall make the final determination which information may be disclosed under this section.

*Disclosures about Victims of Abuse, Neglect, or Domestic Violence (*45 CFR 164.512)

Members of the TWU workforce may disclose to a government agency PHI about an individual who they have reasonably determined to be a victim of abuse, neglect, or domestic violence, if this disclosure is authorized or required by law and subject to the following conditions:

- The disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of the law;

- If the individual agrees to the disclosure; or
- If the disclosure is expressly authorized by statute or regulation and:
    - A determination is made that the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
    - If the individual is unable to agree because of incapacity, a law enforcement or other public official may authorize to receive the report if:
        - The PHI sought is not intended to be used against the individual; and
        - An immediate enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

The Privacy Officer of the TWU health care entity must promptly inform the individual that such a report has been or will be made, unless:

- There has been a determination that informing the individual would place the individual at risk of serious harm; or
- A surrogate decision maker would be the legally appropriate party to inform, and there has been a determination that this surrogate decision maker is responsible for the abuse, neglect, or other injury, and that informing this person would not be in the best interests of the individual under medical care.

Uses and Disclosures for Health Oversight Activities (45 CFR 164.512)

Members of the TWU workforce may disclose PHI without an authorization to a health oversight agency for oversight activities authorized by law. These activities include:

- Audits;
- Civil, administrative, or criminal investigations, proceedings, or actions;
- Inspections;
- Licensure or disciplinary actions;
- Other activities necessary for appropriate oversight of:
    - The health care system;
    - Government benefit programs for which health information is relevant for beneficiary eligibility;
    - Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
    - Entities subject to civil rights laws for which health information is necessary for determining compliance.

Disclosure is not permitted if the individual is the subject of an investigation or activity and the investigation or activity is not directly related to:

- The individual's receipt of health care;
- A claim for public benefits related to health, for example, food stamps; or
- The individual's qualification for or receipt of public benefits or services when the individual's health is integral to the claim for public benefits or services.

If a health oversight activity or investigation is related to a claim for public benefits that are not related to health, the joint activity or investigation shall be considered a health oversight activity.

The TWU General Counsel will have the final authority to determine the propriety of a disclosure in cases that do not clearly meet the above criteria.

Disclosures by Whistleblowers and Workforce Victims of Crime (45 CFR 164.530)

All TWU workforce members are required to report any suspected violation of federal or Texas laws or regulations, or provisions of this URP. These reports should be made to their supervisor, the Privacy Officer of their health care component, or the TWU HIPAA Compliance Officer.

A member of the TWU workforce or a BA may also disclose PHI without violating this URP if the following conditions are met:

- The workforce member or BA believes in good faith that TWU or one of its health care components has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by TWU or its health care components potentially endangers one or more patients, workers, or the public; and
- The disclosure is to:
    - A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of TWU;
    - An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct at TWU; or
    - An attorney retained by or on behalf of the workforce member or BA for the purpose of determining the legal options of the workforce member or BA with regard to conduct believed to be unlawful or in violation of professional or clinical standards.

A member of the TWU workforce may also disclose PHI without violating this URP if:

- The workforce member is a victim of a criminal act; and
- The disclosure is to a law enforcement official, provided that:
    - The PHI disclosed is about the suspected perpetrator of the criminal act; and
    - The PHI disclosed is limited to the suspected perpetrator's:
        - Name and address;
        - Date and place of birth;
        - Social security number;
        - ABO blood type and Rh factor;
        - Type of injury;
        - Date and time of treatment;

- Date and time of death, if applicable; and
- Description of the individual's distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars or tattoos.

All TWU workforce members shall be allowed to freely discuss and raise questions to managers or to appropriate personnel about situations that they feel are in violation of federal or Texas law or this URP.

No member of the TWU workforce shall intimidate, threaten, coerce, discriminate against, or retaliate against any patient, legally authorized representative, workforce member, association, organization or group that in good faith:

- Discloses or expresses the intention to disclose suspected violations of federal or Texas laws or regulations, or of this URP;
- Provides information to or testifies against the alleged offender or TWU;
- Objects to or refuses to participate in activities that they believe might violate federal or Texas laws or regulations, or this URP;
- Participates in a compliance review, audit, or peer review of health care services; or
- Files a legitimate report, complaint, or incident report.

Workforce members who are alleged and found to have filed a malicious complaint may be subject to disciplinary action.

The TWU HCO will review any allegation of retaliation and will ensure that a proper investigation is conducted.

Disclosures for Judicial and Administrative Proceedings (45 CFR 164.512)

TWU may use or disclose PHI in the course of any judicial or administrative proceeding if one of the following conditions is met:

- The disclosure is in response to an order of a court or administrative agency, but only the PHI expressly authorized by the order may be disclosed;
- The disclosure is in response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or an administrative agency (such as a subpoena from a government agency), provided that:
    - TWU receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to ensure that the subject of the requested PHI has been given notice of the request, as evidenced by an affidavit from the requesting party; or
    - TWU receives satisfactory assurance from the party seeking the information that this party has made reasonable efforts to secure a qualified protective order. A qualified protective order is an order of a court or an administrative tribunal or a stipulation by the parties to a litigation or administrative proceeding that:

        - Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and
        - Requires returning PHI to TWU or requires destroying the PHI and all copies made at the end of the litigation or proceeding.
- TWU receives satisfactory assurances from a party seeking PHI along with a written statement and accompanying documentation that:
    - The party requesting such information has made a good faith attempt to provide written notice to the individual (or to mail a notice to the individual's last known address);
    - The notice included sufficient information about the litigation or proceeding in which the PHI is requested that would enable the individual to raise an objection to the court or administrative tribunal; and
    - The time for the individual to raise objections to the court or administrative tribunal has elapsed and:
        - No objections were filed; or
        - All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.
- TWU receives satisfactory assurances from a party seeking PHI including a written statement and accompanying documentation demonstrating that:
    - The parties to the dispute that gave rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or
    - The party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.

If none of the above conditions are met, TWU has the option to disclose PHI in response to lawful process without receiving full satisfactory assurances, provided that TWU has made its own reasonable efforts:

- To provide notice to the individual sufficient to meet the requirements of this section; or
- To seek a qualified protective order.

Information for Law Enforcement Purposes (45 CFR 164.512)

This section deals with PHI that may be disclosed for law enforcement purposes in which de-identified information is not sufficient for law enforcement's needs.

- For the purpose of complying with laws that require reporting certain kinds of wounds or other physical injuries, TWU may disclose PHI to appropriate law enforcement officials or agencies.
- For the purpose of complying with a court order, warrant, subpoena, summons, grand jury subpoena, administrative request or subpoena, a civil or authorized investigative demand, or similar process authorized by law, TWU may disclose PHI to authorized officials, provided that:

    - The information requested is relevant and material to a legitimate law enforcement inquiry;
    - The request is specific and limited in scope to the purpose for which the information is sought; and
    - De-identified information cannot reasonably be used.
- For the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, TWU may release PHI in response to a request by a law enforcement official, provided that the information is limited to the following:
    - Name and address
    - Date and place of birth
    - Social security number
    - ABO blood type and Rh factor
    - Type of injury
    - Date and time of treatment
    - Date and time of death, if applicable; and
    - A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos.

PHI related to an individual's DNA or DNA analysis, dental records, or typing, sample, or analysis of bodily fluids or tissues may NOT be disclosed in response to such a request for PHI by law enforcement official.

To provide information about an individual who is or is suspected to be a victim of a crime, TWU may release PHI in response to a request by a law enforcement official, provided:

- The individual agrees to the disclosure; or
- TWU is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:
    - The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and that such information is not intended to be used against the victim;
    - The law enforcement official represents that immediate law enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
    - The disclosure is in the best interests of the individual as determined by the TWU health care component and TWU, in the exercise of their professional judgment.

For the purpose of alerting law enforcement of the death of the individual, TWU may disclose PHI about a deceased individual to law enforcement officials, if TWU has a suspicion that such death may have resulted from criminal conduct.

For the purpose of providing evidence of criminal conduct that occurred on TWU premises, TWU may disclose PHI that it believes in good faith constitutes evidence to law enforcement officials.

For the purpose of altering law enforcement of the commission of a crime, TWU may disclose PHI to law enforcement officials if such disclosure is deemed necessary to identify:

- The nature of a crime;
- The location of a crime or of the victim(s) of a crime; and
- The identity, description, and location of the perpetrator of a crime.

Uses and Disclosures about Decedents (45 CFR 164.512)

TWU may disclose PHI about a deceased individual for the following purposes:

- To coroners and medical examiners for the purposes of identifying a deceased person, determining a cause of death, or other duties as authorized by law;
- To funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the deceased. If necessary for the funeral directors to carry out their duties, TWU may disclose PHI prior to and in reasonable anticipation of the individual's death; or
- To organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaver organs, eyes, or tissues for the purpose of facilitating organ, eye, or tissue donation and transplantation.

TWU will not disclose or release PHI about a deceased individual without proper documentation including, but not limited to, court order or Consent for Release of Confidential Information signed by personal representative of the patient if the patient is deceased. (Texas Occupation Code Sec. 159.005)

Uses and Disclosures of PHI by and for Personal Representatives, Minors, and Deceased Individuals (45 CFR 164.502)

A personal representative is any adult who has the capacity to make decisions and who is willing to act on behalf of a patient or client. A personal representative would include an individual who has authority, by law or by agreement from the individual receiving treatment, to act in place of the individual. This includes parents, legal guardians, or properly appointed agents (those with Durable Power of Attorney for health care), or individuals designated by state law.

A minor is an individual under the age of eighteen (18) who has not been legally emancipated by a court, and who also is:

- Not married or previously married;
- Not serving in the armed forces;
- Not an offender in a correctional facility; and
- Not at least sixteen (16) years of age and also who is living away from home and providing his or her own financial support.

As a general rule, minors, incapacitated, and deceased individuals must have a personal representative in order to provide consent or authorization to use and disclose the individual's PHI. TWU must recognize a personal representative who is properly designated as the individual responsible for providing consents and authorizations for any other use or disclosure of PHI.

Exceptions for Minors:

- Once a minor is married or emancipated by court order, then TWU will only use or disclose PHI with written authorization by the emancipated or married minor or a personal representative authorized by the court or the emancipated/married minor.
- An unmarried minor custodial parent who is not emancipated and who consents to treatment for her or his child has authority, as the parent of the child, to authorize use and/or disclosure of the child's PHI.
- If a parent or personal representative of a minor has agreed in writing to confidentiality between TWU and the minor, then the minor will only have the authority to sign a HIPAA Authorization for use and disclosure of PHI subject to that agreement of confidentiality.

Uses and Disclosures Regarding Abuse, Neglect, and Endangerment

Unless a state law requires otherwise, TWU need not recognize a person as the personal representative of an individual if TWU reasonably determines that it is not in the best interest of the individual to do so, and also if it reasonably determines or believes that one of the following conditions exist:

- The individual has been or may be subjected to domestic violence, abuse, or neglect by a parent, guardian, or personal representative; or
- Treating the person as a personal representative could endanger the individual.

Uses and Disclosures Regarding Adults and Emancipated Minors

If a person has authority by law to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to the use and disclosure of PHI, TWU will treat this person as a personal representative of the individual. Once a minor is emancipated, a parent or guardian may no longer be recognized as a personal representative.

Un-emancipated Minors

TWU must recognize as a personal representative a parent, guardian, or other person who has authority by law to act on behalf of an individual who is an un-emancipated minor in making decisions related to use and disclosure of PHI.

If a minor does not require the consent of an adult and may consent to treatment, TWU will treat the minor as an individual who may provide consent or authorization for the release of PHI.

A minor, with authority by law, can act as an individual in cases that include, but are not limited to, the following:

- Diagnosis and treatment of any infectious, contagious or communicable diseases reportable to the Texas Department State Health Services;
- A minor who is unmarried and pregnant can consent to treatment of pregnancy other than abortion;
- A minor can consent to examination and treatment for addiction, dependency or any other treatment directly related to drug or chemical abuse; or
- Counseling for:
    - Suicide prevention;
    - Chemical addiction or dependency; or
    - Sexual, physical, or emotional abuse.

Minors can consent or authorize the release of PHI without requiring parental/guardian involvement (and parents are not notified unless the minor gives their consent).

Deceased Individuals

PHI continues to be protected under HIPAA until fifty (50) years after the death of the individual. TWU and its workforce members cannot release PHI regarding a deceased individual unless a valid personal representative has been established and the personal representative has requested the PHI through the proper authorization process.

If an executor, administrator, or other person has authority under applicable law to act on behalf of a deceased individual or the individual's estate, then TWU must recognize this person as a personal representative. If an executor, administrator, or other court-appointed representative for the deceased individual's estate does not exist, then TWU will recognize the below-listed individuals as authorized to request the release of PHI. The TWU General Counsel shall determine the appropriate person that TWU may recognize as personal representative in doubtful cases.

In the case of a deceased, married individual survived by a spouse with or without descendants:

- Spouse
- Adult children
- Adult grandchildren
- Parents
- Adult descendants of parents (brother and sisters)
- Brothers' and sisters' adult children
- Brothers' and sisters' adult grandchildren
- Grandparents
- Adult descendants of grandparents (uncles and aunts)

In the case of a deceased individual with no spouse (i.e., never married, widowed, or divorced and not remarried), with or without descendants:

- Adult children
- Adult grandchildren
- Parents
- Adult descendants of parents (brothers and sisters)
- Brothers' and sisters' adult children
- Brothers' and sisters' adult grandchildren
- Grandparents
- Adult descendants of grandparents (uncles and aunts)

Research Use of Health Information (45 CFR 164.512)

The use and disclosure of PHI in research must have appropriate authorizations and safeguards in place. The TWU Institutional Review Board ("***IRB***") review process is responsible for determining which federal and Texas standards apply to the use and disclosure of PHI for research. The IRB is expected to comply with the Federal Policy for the Protection of Human Subjects (the "Common Rule"); in instances where the IRB determines not to follow the Common Rule, these HIPAA policies and procedures shall apply, unless another equivalent federal or Texas standard is specifically adopted by the IRB. All researchers and their staff must rigorously comply with the procedures of the IRB and of the Office of Research Services in the use of PHI.

Faculty, staff, and students of TWU may not initiate research involving human subjects without approval of the IRB before the research starts.

Whenever possible, de-identified PHI should be used for research. When de-identified PHI is to be used for research, including public health research, the standards listed below must be followed. In addition:

- PHI used for research should be de-identified at the point of data collection for research protocols approved by the IRB, unless the participant voluntarily and expressly consents to the use of his or her personally identifiable information or the researcher(s) obtain an IRB waiver of authorization; and
- If PHI is de-identified by means of "hashing," "salting," or any other method of replacing or changing existing data to mask identities (for example, shifting all dates forward 21 days, replacing street names with randomly assigned other street names, etc., where a key remains to return the data to its original values), anyone involved in the research project must not disclose the key and must not disclose the mechanism used to re-identify the information.

Uses and Disclosures to Avert Serious Threat to Health and Safety (45 CFR 164.512)

Consistent with applicable law and standards of ethical conduct, TWU may disclose PHI, provided that either TWU, in good faith, believes that the use or disclosure:

- Is necessary to prevent or lessen a serious or imminent threat to the health or safety of a person or the public.
- In the course of treatment that is designed to alter or change the desire to commit the criminal conduct that would be the basis for making a disclosure, or
- When an individual initiates or is referred to a health care component of TWU for treatment, counseling, or therapy.
- Is to a person or persons reasonably able to prevent or lessen the threat.

Or, the disclosure is necessary for law enforcement authorities to identify or apprehend an individual:

- Because of a statement by an individual admitting participation in a violent crime that TWU reasonable believes may have caused serious physical harm to the victim; or
- Where it appears from all the circumstances that the individual has escaped from lawful custody.

Information Required by Specialized Government Functions (45 CFR 164.512)

TWU may disclose PHI for specialized government functions, provided that the TWU Department of Public Safety ("***DPS***") verifies the identity of the individuals representing the specialized government function; and TWU authorizes the release

The specialized government functions to which PHI may be disclosed if necessary and legally appropriate include:

- Armed forces personnel, the Red Cross, or other authorized agents of the Armed Forces, if deemed necessary by appropriate military command authorities to assure the proper execution of a military mission. The appropriate military authority must have published a notice in the Federal Register specifying the appropriate military command authorities and the purposes for which the requested PHI may be used or disclosed;
- Authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities;
- Authorized federal officials for the provision of protecting the President or foreign heads of state;
- The Department of State, for the purpose of making medical suitability determinations;
- A correctional institution, if information about an individual is needed for the treatment of that individual, or for the health and safety of other inmates and of employees of a correctional institution, including those responsible for transporting the individual; and
- Government programs providing public health benefits and government agencies administering such benefits.

Disclosures for Workers' Compensation (45 CFR 164.512)

PHI may be disclosed to comply with Worker's Compensation laws and regulations without the consent, authorization, or opportunity to object by an individual. Such disclosure will be only the minimum necessary information. The records' custodian must carefully review and approve requests for entire records.

Pursuant to Texas Labor Code §402.084 (codified from the Texas Workers' Compensation Act) and the rules of the State Office of Risk Management, the individual is required to sign an authorization to release medical information relating to a workers' compensation claim to the State Office of Risk Management. This information may be released to that agency, as well as to the individual, the individual's representative, and the employer at the time of the individual's injury. Consequently, authorized personnel of TWU may access medical information related to a workers' compensation claim once the individual has signed this authorization.

However, an individual's consent or authorization is not required by the HIPAA Privacy Rules for TWU to respond as an employer to legally valid requests for an individual's PHI that is directly related to a Workers' Compensation claim. However, only the minimum necessary information will be released in response to the request, unless the requestor can give good cause to TWU that additional information must be released.

Use and Disclosure to Family and Friends—Individual Care and Notification (45 CFR 164.510)

TWU health care components may disclose certain PHI to an individual's family member, other relative, a close personal friend of the individual, or any other person identified by the individual with consent, provided that PHI is directly relevant to that person's involvement with the individual's care or payment related to the individual's treatment and health care. TWU health care components may use or disclose PHI to notify or assist in the notification of a family member, a personal representative of the individual, or another person responsible for the care of the individual when this information is related to the individual's location, general condition, or death. TWU may also use and disclose PHI for the purpose of identifying or locating family, close personal friends, or personal representatives.

If the individual is present or otherwise available and if the individual has the capacity to make health care decisions, the TWU health care component may use or disclose the PHI if it:

- Obtains the individual's verbal or written agreement to do s; and
- Provides the individual with the opportunity to object to the disclosure, and the individual does not object or reasonably infers from the circumstance, based on the exercise of professional judgment that the individual does not object to the disclosure.

The workforce member attending the individual shall note in the individual's chart or record, whether or not the individual was able to consent, whether or not consent was given, and what, if any, limitations on disclosure the individual requested.

If the individual is not present or if, because of the individual's incapacity or because of emergency circumstances, the individual does not have the capacity or opportunity to agree or to object, the TWU health care component may, in its exercise of professional judgment, determine whether the disclosure is in the best interest of the individual. If so, it shall disclose only the PHI that is directly relevant to the person's involvement with the individual's health care. TWU health care components may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X rays and other diagnostic media, and similar forms of PHI.

Use and Disclosure for Marketing (45 CFR 164.514)

TWU workforce members may not use, disclose, sell, or coerce an individual to consent to the disclosure, use, or sale of PHI for marketing purposes. The individual, however, may freely consent or authorize such disclosure, using the appropriate forms and procedures.

The following scenarios are not a violation of this URP. A workforce member may:

- Provide information on health-related products and services in a face-to-face encounter with a patient or client.
- Provide a patient or client with common health care communications, such as appointment reminders, prescription refill reminders, and information on disease management and wellness programs.
- Provide the patient or client with information on participating providers or plans in a network or with alternative treatment options.
- Provide the patient or client with sample products.
- Provide promotional gifts that include marketing communications, provided these are of nominal value (pens, calendars, etc.).

No written marketing communication may be sent to an individual without an authorization from the individual. The Texas Medical Privacy Act does not allow a patient's health information to be marketed, or to be used in marketing, without that patient's consent or authorization.

Use and Disclosure for Fundraising (45 CFR 164.514)

TWU or a TWU health care component may use or disclose to a BA or to an institutionally related foundation the following PHI without an authorization for the purpose of raising funds for TWU's benefit:

- Demographic information relating to an individual, including- name, address, other contact information, age, gender, and date of birth;
- Dates of health care provided to an individual;
- Department of service information;
- Treating physician;

- Outcome information; and
- Health insurance status.

With each fundraising communication made to an individual under this section, TWU must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost. If an individual chooses to opt-out of receiving fundraising communications, TWU must ensure that the individual is not sent such communications.

Each TWU health care component that wishes to use or disclose PHI for fundraising in accordance with this section must include the fundraising statement to this effect in the Privacy Notice.

Disclosure for Underwriting (45 CFR 164.514)

A TWU health care component may disclose PHI to a health plan for the purpose of underwriting, premium rating, or other activities related to the creation, renewal, or replacement of a contract for health insurance or other health benefits. However, if the health plan is not awarded a contract for health insurance or other health benefits, the health plan may not use or disclose this protected health information for any other purpose, except as required by law.

PATIENT RIGHTS

Access and Denial of Patient Request for PHI (45 CFR 164.524)

The Privacy Officer of the health care component that retains the individual's records shall be responsible for processing or denying requests by an individual to that individual's own PHI.

Individuals have a right to inspect and receive a copy, at their own expense, of the PHI that is in their designated record, except for the following:

- Full copies of psychotherapy notes, as individuals are only entitled to request and receive a summary of psychotherapy notes;
- Information compiled in anticipation of use in a civil, criminal, or administrative action or proceeding;
- PHI subject to the Clinical Laboratory Improvements Amendments of 1988 ("***CLIA***");
    - PHI exempt from CLIA (42 CFR 493.3) is PHI generated by:
        - Facilities or facility components that perform forensic testing;
        - Research laboratories that test human specimens but that do not report patient-specific results for diagnosis, prevention, treatment, or assessment of the health of patients; and

- Laboratories certified by the National Institutes on Drug Abuse ("***NIDA***") in which drug testing is performed that meets NIDA guidelines and regulations. However, other testing conducted by a NIDA-certified laboratory is not exempt.

Employees should not access PHI of their family or themselves, nor should they request other workforce members to access PHI on their behalf. Employees must follow the same procedures as other patients or authorized individuals to access PHI.

Each TWU health care component shall develop the procedures, forms and workforce training to enable individuals to request access to and copies of their own PHI. The procedures developed must comply with the following:

- Individuals have the right to request access to their own PHI as long as the PHI is maintained in the records of the health care component;
- If TWU or one of its health care components does not maintain the requested PHI but knows where the requested information is maintained, then it must inform the individual where to direct the request for access;
- The individual must make the request in writing, using the appropriate form;
- Upon request for PHI, the workforce members will:
    - Request a picture ID to confirm the identity of the individual requesting the PHI;
    - Provide the PHI requested; or
    - Deny access in writing for one or more of the reasons outlined above.
- Based on Texas law, TWU or the health care component must act on the individual's request no later than the 15th business day after receipt of the request and payment of any necessary fee. If TWU is officially closed during the entire fifteen (15) day period, the request must be acted on in a reasonable time following the reopening of the University (Texas health and Safety Code 181.102). TWU or the health care component shall:
    - Make the information available, in full or in part, for examination; or
    - Inform the authorized requestor if the information does not exist, cannot be found, or is not yet complete. Upon the completion or location of the information, TWU or the health care component shall notify the individual. If the information does not exist or cannot be found, the health care component will make an official notation for file at the TWU facility.

If access is granted, in whole or in part, TWU or the health care component must comply with the following requirements:

- TWU or the health care component must provide the individual access to his or her PHI in the designated record set, including inspection or receiving a copy, or both. If the same PHI that is the subject of a request for access is maintained in more than one designated record set or at more than one location, TWU or the health care component need only produce the PHI once in response to a request for access;

- TWU or the health care component must provide the individual with access to the PHI in the form or format requested by the individual, if it is readily reproducible in such a form or format, or, if not, in a readable hard copy or other form or format that is agreed upon by both parties. However, if the PHI that is the subject of the request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, TWU or the health care component must provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format, or if not, in a readable electronic form and format as agreed to by TWU and the individual;
- TWU or the health care component may provide the individual with a summary of the PHI requested, in lieu of providing access to the PHI, or may provide an explanation of the PHI to which access has been provided, if:
    - The individual agrees in advance to such a summary or explanation; and
    - The individual agrees in advance to the fees imposed, if any, by TWU or the health care component for a summary or explanation.
- Whether summary or explanation, notation will be made by the health care component in the file at the TWU facility.
- TWU or the health care component must provide access as requested by the individual in a timely manner, including arranging with the individual for a convenient time and place to inspect or receive a copy of the PHI, or by mailing the copy of the PHI at the individual's request. TWU or the health care component may discuss the format, scope, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access;
- If the individual's request for access directs TWU or the health care component to transmit the copy of PHI directly to another person designated by the individual, TWU or the health care component must provide the copy to the person designated by the individual. The individual's request must be in writing, signed and must clearly identify the designated person and where to send the copy of PHI; and
- If the individual requests a copy of the PHI or agrees to a summary or explanation of its information, TWU or the health care component may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:
    - Copying, including the cost of supplies for and labor of copying the PHI requested. The fee schedule for these services is set by the State of Texas (www.tmb.state.tx.us);
    - Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;
    - Postage, if the patient has requested that the copy, summary, or explanation be mailed; and
    - Preparing an explanation or summary of the PHI, if agreed to by the individual.

Denial of Access to PHI

TWU or the health care component must allow an individual to request access to inspect or receive a copy of PHI maintained in their records. However, TWU or the health care component may deny an individual's request without providing an opportunity for review when:

- An exception to access exists;
- The individual agreed to temporary denial of access when consenting to participate in research that includes treatment, and the research is not yet complete;
- The records are subject to the Privacy Act of 1974, and the denial of access meets the requirements of that law; and
- The PHI was obtained from someone other than TWU under a promise of confidentiality, and access would likely reveal the source of the information.

TWU or the health care component may also deny an individual access for additional reasons, provided that the individual is given the right to have such denials reviewed under the following circumstances:

- A licensed health care professional has determined that the access is likely to endanger the life or physical safety of the individual or of another person;
- The PHI makes reference to another person who is not a health care professional, and a licensed health care professional designated by the HIPAA Compliance Office has determined that the access requested is likely to cause substantial harm to this other person; or
- The request for access is by the individual's surrogate decision-maker, and a licensed health care professional designated by the HIPAA Compliance Office has determined that access is likely to cause substantial harm to the individual or to another person.

If access is denied on the basis of any criterion above, the individual has the right to have the denial reviewed by a licensed health care professional, who is designated by the HCO and who did not participate in the original decision to deny, to act as the reviewing official. The designee must not have participated in the original decision to deny. TWU or the health care component must provide access or deny access in accordance with the determination of the reviewing official;

If TWU or the health care component denies access, in whole in or part, to PHI, TWU or the health care component must comply with the following:

- To the extent possible, give the individual access to any other PHI requested, after excluding the PHI to which access was denied;
- Provide in a timely manner a written denial to the individual, written in plain language, that contains the following information:
    - The reason for the denial;
    - If applicable, a statement of the individual's review rights, including a description of how the patient may exercise such review rights; and

    - A description of how the individual may complain to TWU.
- If the individual has requested a review of a denial, the TWU HCO must designate a licensed TWU health care professional who was not directly involved in the decision to deny access. TWU must promptly refer a request for review to this licensed health care professional. The licensed health care professional must determine, in a reasonable period of time, whether to provide or to deny access to the requested PHI. The TWU HCO must promptly provide written notice to the individual detailing the findings of the reviewing health care professional, and must then direct that appropriate action be taken to provide or deny access, as addressed in this section.

Patient Right to Restrict Access of Uses and Disclosures (45 CFR 164.522)

TWU health care components must permit an individual to request that the health care components restrict:

- Uses and disclosures of PHI about the individual to carry out TPO; and
- Permitted uses and disclosures as outlined elsewhere in this policy.

Each health care component shall develop the necessary forms and procedures to enable individuals to request restrictions and shall provide workforce members with the training necessary to carry out these procedures.

TWU health care components are not required to agree to a restriction, except that they must agree to the request to restrict disclosure of PHI to a health plan if the disclosure is for the purpose of carrying out payment or health care operations and the PHI pertains solely to a health care item or service for which the individual, or a person other than a health plan on behalf of the individual, has paid out of pocket in full.

If a health care component does agree to a restriction, then TWU or the health care component must document the restriction and may not use or disclose PHI in violation of the restriction, except when the individual who requested the restriction needs emergency treatment and the restricted PHI is required to provide emergency treatment. If restricted PHI is disclosed to another health care provider for emergency treatment, TWU or its health care component(s) must request as soon as practicable in writing that the health care provider not further use or disclose the PHI.

TWU or a health care component may itself use the restricted PHI or may disclose the restricted PHI to a health care provider for other required treatment to the individual. A restriction agreed to by a TWU health care provider cannot be used to prevent:

- Uses or disclosures from being made to the individual for inspection and copying the individual's own PHI;
- The individual from obtaining an accounting of disclosures of PHI; or
- For uses and disclosures for which consent, authorization, or an opportunity to agree or object is not required.

Terminating a Restriction

TWU health care component may terminate its agreement to a restriction if:

- The individual agrees to or requests the termination in writing;
- The individual orally agrees to the termination and the oral agreement is documented; or
- The TWU health care component informs the individual that it is terminating the restriction. PHI created or received before the termination will remain restricted. PHI created or received after the termination will no longer be restricted.

Confidential Communications

A request for restricting confidential communications can occur anytime and requires a change in the individual's designated address. TWU health care components must permit individuals to make requests and must accommodate reasonable requests to receive communications of PHI from TWU health care components by alternative locations or address. TWU health care components:

- May require that individuals make a request for confidential communication in writing;
- May condition the provision of a reasonable accommodation on (a) information regarding how any payment will be handled, if appropriate and (b) specification of an alternative address or other method of contact; and
- May not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

It is the individual's responsibility to change an address back to the original designated address.

Patient Right to Amend One's Own Protected Health Information (45 CFR 164.526)

Patients have the right to amend information collected and maintained about them in their records (designated record set).

All workforce members and TWU health care components must strictly observe the following standards:

- An individual has the right to have a TWU health care component amend PHI or a record about the individual in a designated record for as long as the PHI is maintained in the designated record set.
- A TWU health care component may deny an individual's request for amendment if it determines that the PHI or record that is the subject of the request:
    - Was not created by the TWU health care component, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
    - Is not part of the individual's designated record;

    - Would not be available for inspection under the Access and Denial Request for PHI section of this policy; or
    - Is accurate and complete.
- The individual must make the request to amend the PHI in writing to the TWU health care component with a reason to support the requested amendment. The request shall be on the form developed for this purpose by the health care component.
- The TWU health care component must accept all requests to amend PHI in the designated record set. However, the health care component is not required to act on the individual's request if one of the conditions for denying the request is found to exist.
- The health care component must act on the individual's request for an amendment no later than sixty (60) days after the receipt of the request. If the health care component is unable to act on the amendment within the required sixty (60) day time limit, it may extend the time for its action by no more than thirty (30) additional days, provided that:
    - The health care component provides the individual with a written statement of the reasons for the delay and the date by which action on the request will be completed; and
    - The health care component may have only one such extension of time for action on a request for an amendment.
- If the amendment is granted, in whole or in part, the TWU health care component must:
    - Make the appropriate amendment to the PHI or record that is the subject of the request for amendment by at least identifying the records that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.
    - Inform the individual in writing in a timely manner that the amendment is accepted and obtain the individual's identification of an agreement to have the health care component notify the relevant persons with which the amendment needs to be shared.
    - Make reasonable efforts to inform and provide the amendment within a reasonable time to:
        - Persons identified by the individual as having received PHI about the individual and needing the amendment, and
        - Persons, including BAs, that the health care component knows have the PHI that is the subject of the amendment and that may have relied, or might reasonably rely, on this information to the detriment of the individual.
- If the requested amendment is denied, in whole or in part, the health care component must provide the individual with a timely, written denial. The denial must use plain language and contain:
    - The basis for the denial, in accordance with the procedures specified in this section;
    - Notice that the individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

- A statement that, if the individual does not submit a statement of disagreement, the individual may request that the health care component provide the individual's request for amendment and the denial of the amendment whenever it makes future disclosures of the individual's PHI; and
- A description of how the individual may file a complaint with TWU with respect to student medical records, or to the Secretary of the Department of Health and Human Services with respect to records protected by the HIPAA Privacy regulations.

- Additionally, for denials:
  - The health care component must permit the individual to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such a disagreement. The health care component may reasonably restrict the length of any statement of disagreement;
  - The health care component may prepare a written rebuttal to the individual's statement of disagreement. Whenever a rebuttal is prepared, a copy of the rebuttal must be provided to the individual who submitted the statement of disagreement;
  - The health care component must identify, as appropriate, the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the denial of the request, the individual's statement of disagreement, if any, and the rebuttal, if any, to the designated record set;
  - In its future disclosures:
    - If a statement of disagreement has been submitted by the individual, the health care component must include the individual's request for an amendment, the denial of the request, the individual's statement of disagreement and the rebuttal, if any, or an accurate statement of any such information, with any subsequent disclosures of the PHI to which the disagreement relates;
    - If the individual has not submitted a written statement of disagreement, the health care component must include the individual's request for amendment and its denial, or an accurate summary of this information, with any subsequent disclosures of the PHI only if the individual has requested such action; or
    - When a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included with the disclosure, the health care component may transmit the material required under separate cover to the recipient of the standard transaction.
  - If the health care component is informed by another provider or payer that an amendment has been made to the individual's PHI within the outside entity's records, the TWU health care component must amend the PHI in the designated records that have been received from that outside entity. However, the TWU health care component is not required to amend the PHI

in its own records based on the determination of the outside entity, unless the health care component regards the findings of the outside entity reliable. Questions concerning reliability should be discussed with the TWU General Counsel.
    - Each TWU health care component shall develop the procedures, forms, and training for its workforce members that are necessary to carry out the requirements of this section.

Accounting for Disclosures and Patient Access to Disclosure Logs (45 CFR 164.528, 164.530)

Individuals shall have the right to receive an accounting of PHI disclosures made by TWU health care components in the six (6) years prior to the request (or a shorter time period if requested). Disclosures include those to and by BAs. However, TWU health care components are not required to account for disclosures that occurred prior to the compliance date of April 14, 2003.

TWU health care components must account for disclosures of PHI except for the following disclosures, if applicable:

- To carry out TPO;
- To individuals requesting their own PHI;
- To person's involved in the individual's care or for other notification purposes;
- For national security or intelligence purposes;
- To law enforcement officials;
- That occurred prior to the compliance date of April 14, 2003;
- Which were incidental to a permissible use or disclosure;
- Which were for the purposes of a limited data set;
- Which were for a facility directory or to persons involved in the individual's care, as such disclosures require an opportunity for the individual to agree or object;
- Which were made as a result of an authorization signed by the individual;
- PHI that is (a) subject to CLIA (pursuant to CFR 42 USC 263a), to the extent the provision of access to the individual would be prohibited by law; or (b) exempt from CLIA (pursuant to CFR 42 CFR 493.3).

Right to Accounting of Disclosure of PHI

TWU health care components must provide the individual with a written accounting that meets the following requirements:

- The accounting for each disclosure must include:
    - The date of the disclosure;
    - The name of the entity or person who received the PHI and, if known, the address of this entity or person;
    - A brief description of the PHI disclosed; and
    - A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or in lieu of such a statement:

        - A copy of the individual's written authorization, or
        - A copy of a written request for a disclosure, if any.
- If a TWU health care component has made multiple disclosures of the PHI to the same person or entity for a single purpose, or resulting from a single authorization, the accounting may provide, for these multiple disclosures:
    - The information required above;
    - The frequency, periodicity, or number of the disclosures made during the accounting period; and
    - The date of the last such disclosure during the accounting period.
- The health care component must act on the individual's request for an accounting no later than sixty (60) days after receipt of the request, as follows:
    - Provide the individual with the accounting requested; or
    - If unable to provide the accounting within the time required, it may extend the time to provide the accounting by no more than thirty (30) days, provided that:
        - The health care component, within the sixty (60) day time limit, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and
        - The health care component may have only one such extension of time for action on a request for an accounting.
- The health care component must provide the first accounting to an individual in any twelve (12) month period without charge. The health care component may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual with the same twelve (12) month period, provided that the health care component informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or to modify the request for a subsequent accounting in order to avoid or to reduce the fee. The fee schedule for these services is set by the State of Texas.

Exceptions to the Right of Accounting of Disclosures

In accounting for disclosures of PHI:

- The TWU health care component must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official if this agency or official provide the health care component with a written statement that such an accounting to the individual would reasonably be likely to impede the agency's activities. The written statement must specify the time for which such a suspension is required.
- If the agency or official suspends an individual's right to receive an accounting of disclosures and the statement is made orally, the TWU health care component must:
    - Document the statement, including the identity of the agency or official making the statement;
    - Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

- Limit the temporary suspension to no longer than thirty (30) days from the date of the oral statement, unless a written statement from the suspending agency or official is submitted during this thirty (30) day time period.

Documentation for Accounting of Disclosures

The workforce members of the TWU health care component are required to account for disclosures of PHI by documenting any such disclosure. Each health care component shall develop the necessary procedures, training of workforce members, and database or filing system that will contain the accounting of disclosures and that will comply with this section.

Mitigation of Harmful Effects from Unauthorized Use (45 CFR 164.530)

To the extent practicable, TWU will mitigate any harmful effect that becomes known to TWU as a consequence of the use or disclosure of PHI that violates federal or Texas laws, or the policies or procedures of TWU or of its health care components.

Mitigation may include, but is not limited to the following:

- Taking corrective measures within thirty (30) days to remedy the effect of the violation.
- Retraining workforce members responsible for the violation.
- Disciplining workforce members responsible for the violation, following the procedures specified in this policy and in the appropriate sections of the TWU Policy Manual.
- Revising TWU policies or procedure to prevent a recurrence of the violation.
- Addressing problems with BAs, once TWU has been made aware of the problems.

Reporting Violations of HIPAA (45 CFR 164.530)

Any individual who believes TWU or any of its health care components has violated or is not complying with HIPAA or any other state or federal laws dealing with privacy and confidentiality may file a complaint regarding the alleged violation. Individuals should file their complaint with the Secretary of the Department of Health and Human Services, with the Privacy Officer of the health care component, or with the TWU HIPAA Compliance Officer. Individuals who are students may file a complaint with the Privacy Officer of the health care component.

Each health care component shall develop and implement a set of protocols that enable individuals to file a complaint. These protocols shall specify to whom a complaint shall be delivered and how it will be investigated. If the complainant wishes to make an anonymous complaint, and if the health care component has no provision to accept such a complaint, the complaint can be filed through the TWU Ethics and Compliance Hotline. Each health care component must document all complaints received, and their disposition, if any.

In situations involving workforce members who are students, the Office of Student Life Department shall be notified of the investigation. Members of the workforce who are

found, after an investigation, to have violated this policy or any federal or Texas law or regulation shall be subject to appropriate and applicable disciplinary action, following the procedures in TWU discipline policies.

Individuals may not be asked or expected to waive their right to file a complaint as a condition of receiving treatment by the health care component.

Complaints Related to Privacy and/or Security of PHI

- TWU will provide a process for individuals to file complaints regarding TWU's policies and procedures about the use of disclosure of PHI, or TWU's compliance with its policies and procedures.
- The TWU HIPAA Compliance Officer should be contacted in order to file complaints regarding TWU's policies and procedures that are required by the HIPAA Privacy Rule, or TWU's compliance with its policies and procedures.
- Individuals are not expected nor are they required to waive their rights to file a complaint with TWU or the Department of Health and Human Services as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility of benefits.
- The TWU Ethics and Compliance Hotline may also be used to report HIPAA Privacy-related issues and/or complaints. The caller may remain anonymous.

HIPAA BREACH NOTIFICATION

The American Recovery and Reinvestment Act (the "***ARRA***") created new provisions for the protection of patient privacy in 2009. The new rule requires "notification" after breach of unsecured PHI is discovered by a covered entity, mandates civil monetary penalties for certain violations, and creates a federal civil action for individuals to recover damages (but only allows action to be filed by the State Attorney General).

Notification General Rule: HITECH Section 13402

A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHI (as defined in subsection (h)(1)) shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.

Unsecured PHI Guidance

PHI is "unsecured" if it is not encrypted or destroyed. If PHI is not encrypted or destroyed, then it is susceptible to notification requirements if breach occurs.

The term "unsecured" under the Health Information Technology for Economic and Clinical Health Act ("***HITECH***") is different from the term used in the context of the HIPAA Security Rule. "Unsecured" PHI does not necessarily mean the organization is not in compliance with the HIPAA Security Rule.

Breach

- The term ‘breach’ means the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security, privacy or integrity of PHI maintained by or on behalf of a person.
- Such term does not include any unintentional acquisition, access or use of such information by an employee or agent of the covered entity or BA involved if such acquisition, access, or use, respectively, was made in good faith and within the course and scope of the employment or other contractual relationship of such employee or agent, respectively, with the covered entity or BA and if such information is not further acquired, accessed, used, or disclosed by such employee or agent.

Types of Breaches (resulting from inappropriate acts)

- Acquisition: Breach if intentional acquisition
- Access: Breach if intentional access
- Use: Breach if intentional use
- Disclosure: Breach if intentional or unintentional disclosure

Breaches by Business Associate (BA)

A BA of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHI shall, following the discovery of a breach of such information, notify the covered entity of such breach. Such notice shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such breach.

- HITECH puts the BA in the same position as the covered entity for penalties and following HIPAA,
- If a BA has a breach of unsecured PHI, then that breach also falls under the notification rules.
- However, HITECH requires the BA to notify the covered entity of the breach, and then the covered entity follows through on notifying the individual or authorities.

Discovery of a Breach

A breach shall be treated as discovered by a covered entity or by a BA as of the ***first day on which such breach is known*** to such entity or BA, respectively, (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of such entity or associate, respectively) or should reasonably have been known to such entity or associate (or person) to have occurred.

The date a breach is discovered needs to be:

- Identified; and

- Documented with respect to:
    - Date of discovery if the date the breach was known to have occurred by anyone other than the person who committed the breach; and
    - If breach occurs by BA, then facility must try to get BA to identify date of discovery.

Notification Rules

Covered entity self-disclosure:

- To individual
- To individual's next of kin if individual is deceased
- To media
- To Department of Health and Human Services Timeliness: Reporting time after a breach is no less than sixty (60) calendar days after the discovery of a breach by the covered entity or business associate (45 CFR 164.406).

The burden of demonstrating that notifications were made is on covered entity, including demonstrating the necessity of any delay.

Methods of Notification

To individual:

- Last known address: written notification by first-class mail to the last known address.
- E-mail is allowed if specified as preference by individual.
- In the event of insufficient, or out-of-date contact information, a substitute form of notice is permitted.
- If ten (10) or more individuals have insufficient contact information, then notice may be provided by:
    - A conspicuous posting for a period determined by Health and Human Services on the covered entity's home page;
    - A notice in major print or broadcast media; or
    - A notice to include a toll-free phone number where an individual can learn whether or not the individual's unsecured PHI is possibly included in the breach.
- In the event that possible misuse is imminent and might be prevented or mitigated by immediate notice, notice by telephone or other means, as appropriate, along with notice by mail.

*To Media***:**

- When more than 500 people involved in breach.
- Notice shall be provided to prominent media outlets serving a State or jurisdiction, following the discovery of a breach, if the unsecured PHI of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.

To Department of Health and Human Services:

- When 500 or more individuals are involved in a breach, notice to the Department of Health and Human Services must be given immediately.
- When less than 500 individuals are involved in the breach, the covered entity must maintain a log of the breaches and annually submit the log to the Department of Health and Human Services.
- Public Availability: The Department of Health and Human Services will post names of covered entities with breaches of 500 or more individuals.

Content of Notification (to the Individual)

"***Notice of a Breach***" must include:

- Brief description of what happened;
- Date of the breach;
- Date of the discovery of the breach;
- Types of unsecured PHI that were involved in the breach;
- Steps individuals should take to protect themselves from potential harm;
- What the covered entity involved is doing to investigate the breach, mitigate losses, and to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information (toll-free number, e-mail address, Web site or postal address)

Sanctions for Breaches (45 CFR 164.530)

Each health care component of TWU must develop and implement a policy for disciplinary action in the event that a member of the workforce uses or disclosures PHI in a manner that violates federal or Texas law or regulations, or TWU policies.

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 for termination), the workforce member shall be required to repeat confidentiality training.

Health care components should provide examples of violations that will result in disciplinary action. Examples of violations of privacy laws and policies include but are not limited to:

- Discussing patient information in a public area.
- Leaving a medical record in a public area.
- Leaving a computer that contains PHI unsecured.

- Looking up a patient's PHI for personal rather than for business and claims purposes.
- Accessing patient records out of concern or curiosity.
- Compiling a mailing list with the intent to sell or use for personal purposes or for profit.
- Using or disclosing PHI to personally advance a cause of action.

Penalties

Federal penalties that might be assessed for illegal use or disclosure of PHI include:

- The Department of Health and Human Services reserves the right to investigate complaints and conduct compliance reviews. The Secretary of Health and Human Services has delegated enforcement responsibilities to the Department's Office of Civil Rights (OCR).
- Civil and criminal penalties may be imposed on a covered entity.
- Civil penalties consist of a fine of $100 for each violation up to $25,000 within one (1) year. The health care component can claim an affirmative defense if it had no knowledge of the violation, had exercised due diligence in preventing violations, and would not have known despite its due diligence. The OCR may waive penalties if disclosures are made due to reasonable cause and not willful neglect.
- Criminal penalties may consist of up to $50,000 and one (1) year in jail. If the disclosure was made under false pretenses, the violator may face a fine of $100,000 and five (5) years in jail. An individual improperly disclosing PHI with the intent to sell, transfer, or use health information for commercial advantage, personal gain, or malicious harm may face a $250,000 fine and ten (10) years in jail.

Penalties for violations of the Texas Medical Privacy Act may include:

- The Attorney General may institute an action for injunctive relief and/or civil penalties, not to exceed $3,000 per violation.
- If a court finds that violations constitute a pattern or practice, it can assess additional penalties, which should not exceed $250,000, suspend or revoke applicable licenses, or excluded the covered entity from state funded health care programs.

Prohibition of Retaliation (45 CFR 164.530)

TWU shall not intimidate, threaten, coerce, discriminate against, or retaliate against any patient, legally authorized representative, workforce member, association, organization, or group that in good faith:

- Discloses or expresses the intention to disclose suspected violations of federal or Texas laws or regulations, or of this URP;
- Provides information to or testifies against the alleged offender or TWU;

- Objects to or refuses to participate in activities that they believe might violate federal or Texas laws or regulations, or this URP;
- Participates in a compliance review, audit, or peer review of health services; or
- Files a legitimate report, complaint, or incident report.

Workforce members who are alleged and found to have filed a malicious complaint may be subjected to disciplinary actions.

The TWU HIPAA Compliance Officer will review any allegation of retaliation and will ensure that a proper investigation is conducted.

SECURITY

General Standards (45 CFR 164.306(a), 306(b)(2), 316(a))

The HIPAA Security Standards state that covered entities and BAs must:

1. Ensure the confidentiality, integrity, and availability of all EPHI the covered entity or business associate creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Standards.
4. Ensure compliance with the HIPAA Security Standards by its workforce.
5. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications or other requirements of the HIPAA Security Standards. (pursuant to 45 CFR 164.306(a) and 164.316(a)).

TWU will reasonably and appropriately implement the HIPAA Security Standards and implementation specifications, taking into account the following factors:

1. The size, complexity, and capabilities of the University.
2. The University's technical infrastructure, hardware, and software security capabilities.
3. The costs of security measures.
4. The probability and criticality of potential risks to EPHI.

In accordance with 45 CFR 164.306(d) of HIPAA, TWU must implement **required** implementation specifications under the HIPAA Security Standards. When a standard includes **addressable** implementation specifications, TWU must:

1. Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting EPHI; and
2. Implement the implementation specification if reasonable and appropriate; or
3. If implementing the implementation specification is not reasonable and appropriate:

a. Document why it would not be reasonable and appropriate to implement the implementation specification; and

b. Implement an equivalent alternative measure if reasonable and appropriate.

45 CFR 164.306(e) of HIPAA provides that a covered entity must review and modify the security measures implemented under the HIPAA Security Standards as needed to continue provision of reasonable and appropriate protection of EPHI, and update documentation of such security measures in accordance with 45 CFR 164.316(b)(2)(iii) of HIPAA, which provides that documentation must be reviewed periodically and updated as needed in response to environmental or operational changes affecting the security of the EPHI.

NOTE: HIPAA regulations provide that covered entities are required to document, implement and maintain policies and procedures with respect to PHI that are designed to comply with the standards, implementation specifications, or other requirements of subparts C and D of 45 C.F.R. Part 164. HIPAA requires that the policies and procedures be reasonably designed, taking into account the size and type of activities that relate to protected health information undertaken by a covered entity, to ensure such compliance.

Accordingly, TWU and each health care component may use these *HIPAA Security Policies and Procedures* as a guide for developing and adopting policies and procedures that are designed to comply with HIPAA, taking into account various factors that are specifically applicable to the entity.

Additional safeguards, policies, and procedures may need to be added and modification and customization of the policies and procedures may be necessary. Accordingly, TWU and each health care component should consult with internal and outside advisors to customize, modify and supplement these policies and procedures as necessary.

Designation of a Security Officer (45 CFR 164.308(a)(2))

One or more persons will be appointed to fulfill the role of "Security Officer" as required by HIPAA, in accordance with 45 CFR 164.308(a)(2). The duties and responsibilities of such person(s) include, but are not limited to:

1. With the Privacy Officer, maintaining the formal and written *HIPAA Policies and Procedures*, updating those policies as appropriate, and performing a comprehensive annual review of the policies to ensure the provisions are HIPAA compliant;
2. Creating compliance reports and maintaining such records relating to HIPAA compliance in such time and manner and containing such information as the Secretary of Health and Human Services may deem necessary to determine the status of compliance;
3. Developing, coordinating, and participating in training of all workforce members of HIPAA compliant policies and procedures;
4. Managing and supervising the use of security measures to protect data;

5. Managing and supervising the conduct of workforce members in relation to the protection of data;
6. Performing periodic audits to identify areas that represent significant risk of compliance violations and recommending and/or taking corrective action;
7. Creating and maintaining a reporting system that encourages workforce members and others to submit compliance concerns;
8. Addressing reports of compliance violations and maintaining a log of all security incident reports; and
9. Ensuring that all security incidents of potential HIPAA compliance violations related to the HIPAA Security Standards are investigated, results of the investigation are documented, and action is taken to correct any compliance violation.

Workforce Training (45 CFR 164.308(a)(5))

45 C.F.R. 164.308(a)(5) of HIPAA provides that a covered entity must "implement a security awareness and training program for all members of its workforce (including management)."

To comply with HIPAA's training requirements, each TWU component that is subject to HIPAA shall determine the appropriate members of the component's workforce to receive comprehensive HIPAA training. The HIPAA Compliance Officer will work with each component's Privacy Officer to providing training and training materials; however, each component's Privacy Officer will determine the specific training appropriate for that component's personnel, as well as the specific personnel who will receive training. The training will cover:

1. The HIPAA Privacy Standards;
2. The HIPAA Security Standards;
3. Practical procedures for protecting EPHI;
4. Workforce participation in the enforcement of information access control, information security, and computer system access issues; and
5. Procedures for reporting compliance violations.

Subsequent training will occur as needed to review existing policies and procedures and to introduce any changes to the current *HIPAA Policies and Procedures*, or as otherwise required by law. The security awareness and training program may include any or all of the following:

1. Periodic security updates;
2. Procedures for guarding against, detecting, and reporting malicious software;
3. Procedure for monitoring log-in attempts and reporting discrepancies; and
4. Procedures for creating, changing, and safeguarding passwords pursuant to 45 CFR 164.308(a)(5).

Each TWU component will maintain documentation of training provided to all workforce members.

NOTE: The training requirements set forth in these HIPAA Policies and Procedures may be in addition to the workforce role-based training requirements contained in Section 181 of the Texas Health and Safety Code.

Documentation (45 CFR 164.316(b)(i)-(iii); 22 Tex. Admin. Code §165.1)

TWU will maintain and implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications or other requirements of the HIPAA Security Standards. One of the major components of HIPAA compliance is adequate documentation of all communications, actions, activities, assessments or designations as required to be documented under HIPAA. TWU will pay specific attention to documentation of the following:

1. In the event any addressable HIPAA implementation specifications are determined to be unreasonable and inappropriate, the reason why such implementation specification is not reasonable and appropriate;
2. Modifications of a user's right of access to systems storing EPHI;
3. The Contingency Plans (as discussed below);
4. If applicable, repairs and modifications to physical components of the facility related to security (e.g., hardware, walls, doors, locks); and
5. If applicable, movements of hardware and electronic media; and any person responsible for such movement.

TWU will also create and retain documentation of:

1. All training provided to members of TWU's workforce;
2. Any workforce member sanctions as a result of a HIPAA compliance violation; and
3. All complaints of compliance violations, and the results of any investigation.

Documentation that is required to be maintained under HIPAA is to be retained for a period of six (6) years from the date of its creation or the date when it was last in effect, whichever is later. Documentation shall be made available to those persons responsible for implementing the procedures to which the documentation pertains so that compliance with procedures may be monitored. Certain documentation may also be periodically reviewed and updated as needed in response to environmental or operational changes affecting the security of EPHI in accordance with 45 CFR 164.316(b)(i)-(iii).

NOTE: Documentation that is required to be maintained under HIPAA may be required to be maintained for longer or shorter periods of time under other laws, state or federal health care program (e.g., Medicare, Medicaid) regulations, and/or by private contract (e.g., by private contract with an insurer). For example, Texas law requires physician medical records to be maintained for a minimum of seven (7) years from the date of the patient's last treatment or, if the patient was younger than eighteen (18) years of age when last treated by TWU, until the patient reaches age twenty-one (21) or seven (7) years from the last date of treatment, whichever is

longer.[1] Additionally, Texas Medical Board rules specify that the physician may destroy medical records that relate to any civil, criminal, or administrative proceedings only if the physician knows the proceeding has been finally resolved.[2] TWU shall retain documents containing PHI for the longest length of time required by state and federal law, regulation, or contract as applicable to the document. Please note that these Documentation policies and procedures are in addition to the record retention requirements contained in all other applicable laws, regulations, and/or contracts.

Mitigation (45 CFR 164.308(a)(6)(i)-(ii))

TWU shall mitigate, to the extent practicable, any harmful effect that is known to it relating to a use or disclosure of PHI in violation of these *HIPAA Policies and Procedures* or the requirements of HIPAA by TWU or any of its BAs. Each violation of these *HIPAA Policies and Procedures* or the HIPAA regulations shall be disclosed to the Security Officer, who shall evaluate the course of action to mitigate damage caused by such violation on a case-by-case basis, in accordance with 45 CFR 164.308(a)(6)(i)-(ii).

Security Management Process (45 CFR 164.308(a)(1)(i))

TWU will establish and implement a formal security management process to address the prevention, detection, containment and correction of potential security incidents pursuant to 45 CFR 164.308(a)(1)(i). This process shall include, but may not be limited to the following:

1. Risk Analysis. TWU will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of EPHI in TWU's possession. TWU will regularly re-conduct the risk analysis as necessary.

2. Risk Management. TWU will implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in order to comply with 45 CFR 164.306(a) of the HIPAA Security Standards.

3. Sanction Policy. TWU will apply appropriate sanctions in accordance with these *HIPAA Policies and Procedures* against those workforce members that fail to comply with these *HIPAA Policies and Procedures*.

4. Information System Activity Review. TWU will regularly review records of information activity to monitor the security of the system. This review may include review of audit logs, access reports, security incident tracking reports, or any other documentation generated to assist TWU with its efforts to monitor the performance of the system's security measures.

---

[1] *See* 22 TEX. ADMIN. CODE § 165.1.
[2] *See Id*.

Security Management Process: Risk Analysis (45 CFR 164.308(a)(1)(ii)(A))

TWU will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI in the TWU's.[3] Risk analysis may include the following steps:

☐ Characterize system and scope of analysis.

- Identify all electronic media containing EPHI.
- Identify potential risks and vulnerabilities to the confidentiality, availability and integrity of the EPHI that TWU creates, stores, receives or transmits.

☐ Gather information.

- Identify and document where all EPHI is stored, received, maintained or transmitted.
- Collect information regarding physical, environmental and operational security systems.

☐ Identify threats.[4]

- Natural threats (e.g., natural disasters, floods, earthquakes, tornadoes).
- Human threats (e.g., malicious software, unauthorized access to confidential information, unintended deletion or alteration of EPHI, hackers).
- Environmental threats (e.g., power failure, temperature, pollution or chemicals).

☐ Identify vulnerabilities.[5]

- Identify system flaws or weaknesses that could be exploited.
- Technical weaknesses.
- Non-technical weaknesses.

---

[3] 45 CFR 164.308(a)(1)(ii)(A). See U.S. Department of Commerce, National Institute of Standards and Technology, *Guide for Conducting Risk Assessments (NIST Special Publication 800-30 Revision 1)* (Sept. 2012), http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf (last visited September 5, 2013) ("NIST SP 800-30").

[4] NIST SP 800-30 defines a "threat" as "any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, [or] other organizations . . . through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service."

[5] NIST SP 800-30 defines a "vulnerability" as "a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source." NIST SP 800-30 defines "threat source" as "the intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability."

☐ Assess TWU's current security measures.

- Technical measures (e.g., software and hardware, authentication processes, access control).
- Non-technical measures (e.g., policies and procedures, guidelines, physical and environmental security measures).

☐ Determine likelihood of security breach (in consideration of all threat and vulnerability combinations).

- High likelihood.
- Medium likelihood.
- Low likelihood.

☐ Analyze impact of security breach (including relevant losses if no security measures were in place).

- High impact.
- Medium impact.
- Low impact.

☐ Determine level of risk.

- Analyze the likelihood of an identified threat exploiting an identified weakness and the potential resulting impact.
- Consider all threat and vulnerability combinations and the potential resulting impact of each combination.
- Consider ability of current security measures to reduce or eliminate risk.

☐ Identify and document potential solutions to reduce and manage risk.

☐ Document actions taken to assess potential risks and vulnerabilities.

☐ Review and document risk analysis process and results.

☐ Periodically review and update the risk analysis assessment.

NOTE: The risk analysis documentation will be used in the risk management process described below. HIPAA does not require a specific format for documenting the risk analysis process and results.

Security Management Process: Risk Management (45 CFR 164.308(a)(1)(ii)(B))

TWU will implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in order to comply with 45 CFR 164.306(a) of the HIPAA Security Standards, in accordance with 45 CFR 164.308(a)(1)(ii)(B). 45 CFR 164.306(a) of the HIPAA Security Standards requires that TWU: (1) ensure the confidentiality,

integrity, and availability of all EPHI TWU creates, receives, maintains, or transmits; (2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Standards; and (4) ensure compliance with the HIPAA Security Standards by its workforce. This process shall include, but may not be limited to the following:

1. Develop a written risk management plan (evaluate and prioritize risk- reducing security measures identified in the risk analysis process);
2. Implement the risk management plan (e.g., timelines, budget and personnel assignments for implementing risk-reducing security measures);
3. Evaluate and monitor implementation of security measures; and
4. Periodically review and update risk management plan.

Security Management Process: Sanction Policy (45 CFR 164.308(a)(1)(ii)(C))

HIPAA compliance violations are serious matters and TWU will respond in a manner consistent with the severity of the violations, the degree of intent or carelessness of responsible workforce members, and the probability that future violations will occur, in accordance with 45 CFR 164.308(a)(1)(ii)(C). Disciplinary actions will be decided upon after the Security Officer has investigated the Incident Report, interviewed responsible workforce members and any other person with knowledge of the violation, determined damage caused by the violation, and consulted with the responsible workforce member's supervisor. Disciplinary actions may take the following forms:

1. Workforce Training. The workforce member may receive additional training for minor infractions, with documentation of such training added to the workforce member's personnel file.

2. Oral Reprimand. The workforce member may receive an oral reprimand concerning the violation. Documentation of such reprimand will be added to the workforce member's personnel file.

3. Written Reprimand. The workforce member may receive a memorandum documenting the nature of the written admonishment, with a copy of such memorandum to the workforce member's personnel file. The memorandum should include the time, date, and nature of the compliance violation, directions for correcting behavior causing the compliance violation, and future consequences if the behavior is not corrected.

4. Suspension. The workforce member may be suspended for an appropriate period of time without pay. Documentation of such suspension will be added to the workforce member's personnel file.

5. Termination. Employment may be terminated for HIPAA compliance violations. The workforce member will be notified in writing of the reason for termination, and copies of such writing will be added to the workforce member's personnel file.

Security Management Process: Information System Activity Review (45 CFR 164.308(a)(1)(ii)(D))

TWU will periodically review records of information system activity to monitor performance of security measures and activity of its systems pursuant to 45 CFR 164.308(a)(1)(ii)(D). Documentation generated and reviewed may include:

1. Audit logs;
2. Access reports;
3. Security incident tracking reports; or
4. Any other documentation generated to assist us with our efforts to monitor the performance of the system's security measures.

To ensure that system activity is appropriately monitored and reviewed, the following intervals have been established commensurate with the level of risk associated with each system as determined through the risk analysis:

1. High risk systems will be reviewed at least every 30 days;
2. Moderate risk systems will be reviewed at least every 180 days; and
3. Low risk systems will be reviewed at least every 365 days.

Workforce Security (45 CFR 164.308(a)(3)(i))

The HIPAA Security Standards under 45 CFR 164.308(a)(3)(i) require TWU to implement procedures to ensure that all members of its workforce using EPHI to perform the functions of their job have appropriate access to such EPHI, while restricting access to EPHI for those workforce members with jobs that do not require such access.

To limit workforce member access to EPHI, TWU shall:

1. Identify the persons or groups of persons who need access to EPHI to carry out their job function;
2. Identify the type of EPHI to which each person or group needs access and the conditions under which access is needed; and
3. Make reasonable efforts to limit the access of staff to only the information appropriate to accomplish the duties of job requirements.

Only workforce members with jobs requiring access to EPHI will receive such access. No supervisor will authorize any member of our workforce to access, receive, or review such information unless a workforce member has a need to access, receive or review such information in connection with the workforce member's job description. Any workforce member receiving EPHI shall not use the information other than as required for the performance of the workforce member's job duties, and shall not disclose such information to any other person except where such other person is also authorized to access such information. Workforce members are directed not to disclose user identification numbers or passwords with any other workforce member.

Workforce Security: Authorization and/or Supervision Policy (45 CFR 308(a)(3)(ii)(A))

The HIPAA Security Standards under 45 CFR 164.308(a)(3)(ii)(A) require TWU to address whether it is reasonable and appropriate to implement a policy addressing authorization and/or supervision of workforce members with access to EPHI in light of the likely contribution such a policy would have on its efforts to protect EPHI in its possession.

After analyzing whether it would be reasonable and appropriate to implement an authorization and/or supervision policy, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because _____ _____ ___.**

The following alternative policy has been implemented:

_____

_____

_____

_____

_____

_____

Workforce members needing access to EPHI to perform the duties of their respective job functions will be granted an authorization to access EPHI by the Security Officer or his/her designee. The authorization shall describe the scope and means of access granted to each workforce member. Workforce members will be assigned unique profiles and passwords that will limit access to programs and databases. Workforce members may only access EPHI to the extent authorized to do so.

From time to time, workforce members that do not regularly access EPHI as part of their job function may need to access EPHI due to the temporary delegation of a particular function or as directed by his/her supervisor. In such circumstances, workforce members needing access to EPHI must immediately contact the Security Officer to obtain temporary authorization to access. In lieu of issuing temporary authorization, the Security Officer may determine to allow supervised access to EPHI. Workforce members may not

access EPHI through the use of any other person's access identification number or password.

Occasionally, individuals that are not workforce members may need to access EPHI or locations where EPHI resides. For example, it may be necessary for operations or maintenance personnel to access TWU's servers, other hardware or software to perform system upgrades or to fix components of our system. In such circumstances, workforce members will:

1. Sign in each person needing access to systems containing EPHI by obtaining:

   ☐ Full name;

   ☐ Employer name and number;

   ☐ Copy of work order, if any; and

   ☐ Reason for needing access.

2. Confirm that a BAA exists between TWU and the person or company for which the person works, and notify the Security Officer if no such agreement exists.

3. Notify the Security Officer or his/her designee of arrival and prohibit access to TWU's systems until receipt of further instructions by the Security Officer or his/her designee.

Workforce Security: Workforce Clearance Procedure (45 CFR 308(a)(3)(ii)(B))

The HIPAA Security Standards under 45 CFR 164.308(a)(3)(ii)(B) require TWU to address whether it is reasonable and appropriate to implement a policy addressing workforce clearance procedures in light of the likely contribution such a policy would have on TWU's efforts to protect EPHI in its possession.

After analyzing whether it would be reasonable and appropriate to implement a workforce clearance procedures policy, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because _____ _____ ___.**

The following alternative policy has been implemented:

_____

_____

_____

_____

_____

_____

To determine that the access of a workforce member to EPHI is appropriate, TWU shall implement a screening process of each workforce member based upon the scope and necessity of access to EPHI in order to perform one's job function. This screening process may include any or all of the following:

1. Reference checks;
2. Background checks;
3. Verification of licensure;
4. Inquiry with licensing board; or
5. Any other screening procedure identified during the risk analysis deemed feasible and necessary to ensure that access to each workforce member is appropriate.

Any clearance procedure implemented will be for the purpose of determining the appropriate level of access to EPHI given to individual workforce members. Access to EPHI shall be granted in a manner consistent with the "minimum necessary" requirements of the HIPAA Privacy Standards.

Workforce Security: Termination Procedures (45 CFR 164.308(a)(3)(ii)(C))

The HIPAA Security Standards under 45 CFR 164.308(a)(3)(ii)(C) require TWU to address whether it is reasonable and appropriate to implement a policy addressing procedures for terminating a workforce member's access to EPHI in light of the likely contribution such a policy would have on TWU's efforts to protect EPHI in its possession.

After analyzing whether it would be reasonable and appropriate to implement a termination procedures policy, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because _____**

_____

___.

The following alternative policy has been implemented:

_____

_____

_____

_____

_____

_____

Workforce members with access to EPHI may need to have that access terminated at some point due to a change in a workforce member's job function or separation of service. When either circumstance occurs, TWU will:

1. Terminate passwords issued to any such workforce members allowing access EPHI. Workforce members that have experienced a change of job function but continue to perform work for TWU will continue to have access to the hardware and software necessary to perform the workforce member's new job function;
2. Retrieve keys and access cards issued to workforce member, if any, that are no longer needed by the workforce member for purposes of the work performed by the workforce member;
3. Retrieve any and all EPHI in control of the workforce member, if any, that is no longer needed by the workforce member for purposes of the work performed by the workforce member;
4. Disable access to software and email programs; and
5. Escort the workforce member out of the building if employment or other arrangement with TWU is terminated.

Information Access Management (45 CFR 164.308(a)(4)(i))

TWU will implement measures to restrict access to EPHI to those persons with a need for access to perform the functions of their jobs pursuant to 45 CFR 164.308(a)(4)(i). Limiting access to EPHI is intended to reduce the risk of inappropriate disclosure, alteration or destruction of such information. The information access management process may include any or all of the following:

1. Procedures for granting access to EPHI through individual workstations, transactions, programs, processes, or other mechanisms. This is likely to include categorization of access by job function; specified user names and passwords for workstations, programs and processes based upon a particular user's need to access such workstations, programs or processes;
2. Procedures establishing, documenting, reviewing and modifying a user's right of access to a workstation, transaction, program or process; and

3. Any other procedure deemed reasonable and necessary to further the purpose of protection of the integrity, confidentiality, and availability of EPHI.

Access to EPHI shall be granted in a manner consistent with the "minimum necessary" requirements of the HIPAA Privacy Standards.

Information Access Management: Access Authorization (45 CFR 164.308(a)(4)(ii)(B))

The HIPAA Security Standards under 45 CFR 164.308(a)(4)(ii)(B) require TWU to address whether it is reasonable and appropriate to implement a policy addressing access authorization in light of the likely contribution such a policy would have on TWU's efforts to protect EPHI in its possession.

After analyzing whether it would be reasonable and appropriate to implement an access authorization procedures policy, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because _____ _____ ___.**

The following alternative policy has been implemented:

_____

_____

_____

_____

_____

_____

In order to protect the integrity, confidentiality, and availability of EPHI, TWU will limit workforce member access to EPHI so as to authorize workforce members to access only those workstations, programs, processes, or other mechanisms necessary to perform their individual job functions. The Security Officer or the Security Officer's designee shall determine for each workforce member the level of access such workforce member must be granted in order to properly and efficiently perform the duties of his/her job description. The Security Officer or the Security Officer's designee shall approve and maintain documentation of the systems each workforce member is authorized to access.

Workforce members must not access EPHI through workstations, programs, processes, or other mechanisms for which they have not received authorization. If temporary access is needed, workforce members must contact the Security Officer and request such access. Any workforce member that becomes aware of unauthorized access to EPHI must immediately notify the Security Officer.

Information Access Management: Access Establishment and Modification (45 CFR 164.308(a)(4)(ii)(C))

The HIPAA Security Standards under 45 CFR 164.308(a)(ii)(C) require TWU to address whether it is reasonable and appropriate to implement a policy addressing access establishment and modification procedures in light of the likely contribution such a policy would have on TWU's efforts to protect EPHI in its possession.

After analyzing whether it would be reasonable and appropriate to implement an access establishment and modification policy, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because _____ _____ ___.**

The following alternative policy has been implemented:

_____

_____

_____

_____

_____

_____

The following procedures shall be followed to establish, review, modify, and document access to EPHI:

1. Establishing Access. When a workforce member is hired or experiences a change in job description that prompts a need for access to EPHI, the hiring person will contact the Security Officer and assist the Security Officer in the identification of workstations, programs, processes, or other mechanisms that the workforce member will need to access for purposes of employment or other arrangement with TWU. The Security Officer

shall review and approve the request for access as appropriate and undertake the necessary procedures (creating usernames and passwords, etc.) to initialize access to the appropriate systems. Once the request for access has been processed, the Security Officer shall notify the workforce member and any other authorized persons of the workforce member's login credentials. The Security Officer shall log access authorizations for each workforce member.

2. Reviewing and Modifying Access. As workforce members experience changes of job functions or separate from service, access to EPHI must be reviewed and modified. To ensure that workforce members maintain appropriate access to EPHI, the following procedures will be followed:

A. *Periodic Review*. The Security Officer or the Security Officer's designee will periodically review access authorizations of workforce members. The Security Officer may request assistance of supervisors to determine whether current access authorizations are appropriate given the job descriptions of workforce members. In the event it is determined that access to a particular system is no longer appropriate, the Security Officer will initiate the proper steps to rectify the access issue and notify the workforce member and his/her supervisor once the change in access authorization is effective.

B *Notification of Changes in Access Requirements*. The roles, responsibilities, or employment status of a workforce member is likely to change during the course of employment or other arrangement with TWU. When such a change results in a change in the workforce member's need to access EPHI, the workforce member's supervisor shall promptly notify the Security Officer of the need to change the workforce member's access privileges.

C. *Modification of Access Privileges*. Upon receiving results of a periodic review or a notification of a change in access requirements, the Security Officer or the Security Officer's designee shall initiate the modification of the appropriate workforce member's access privileges. Once the modification is complete, the Security Officer or the Security Officer's designee shall notify the workforce member and/or the workforce member's supervisor of the modification and maintain documentation of such modification in the access authorization log.

Security Awareness and Training (45 CFR 164.308(a)(5)(i))

TWU will implement a security awareness and training program for all members of its workforce (including management) in accordance with 45 CFR 164.308(a)(5)(i). The security awareness and training program may include any or all of the following:

1. Security reminders for periodic security updates;
2. Procedures for guarding against and reporting malicious software;
3. Procedures for monitoring log-in attempts and reporting discrepancies;
4. Procedures for creating, changing, and safeguarding passwords; and

5. Any other procedure deemed reasonable and necessary to further the purpose of security awareness and training.

Training will occur as needed to review existing policies and procedures, and to introduce any changes to the current *HIPAA Policies and Procedures*, changes related to new or updated equipment or technology or as otherwise required by law.

Security Awareness and Training: Security Reminders (45 CFR 164.308(a)(5)(ii)(A))

The HIPAA Security Standards under 45 CFR 164.308(a)(5)(ii)(A) require TWU to address whether it is reasonable and appropriate to implement a policy addressing security reminders in light of the likely contribution such a policy would have on its efforts to protect EPHI in its possession.

After analyzing whether it would be reasonable and appropriate to implement a policy concerning security reminders, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because _____ _____ ___.**

The following alternative policy has been implemented:

_____

_____

_____

_____

_____

The _____ [Note: TWU to name appropriate person] of TWU's IT Department will develop a system of on-line, email-based, or log-in screen based reminders designed to inform workforce members of their privacy and security obligations. TWU shall document implementation of all security reminders (type, date, message, etc.).

Security Awareness: Protection from Malicious Software (45 CFR 164.308(a)(5)(ii)(B))

The HIPAA Security Standards under 45 CFR 164.308(a)(5)(ii)(B) require TWU to address whether it is reasonable and appropriate to implement a policy addressing protection from malicious software in light of the likely contribution such a policy would have on its efforts to protect EPHI in its possession.

After analyzing whether it would be reasonable and appropriate to implement a policy concerning protection from malicious software, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because _____ _____ ___.**

The following alternative policy has been implemented:

_____

_____

_____

_____

_____

_____

In order to protect TWU's systems from attacks from malicious software, TWU implements the following:

1. Virus Protection Software. Through risk analysis, TWU has determined that it is appropriate to use anti-virus software on its computers. TWU will monitor the effectiveness of the anti-virus software and update it as necessary.

2. Email Usage. Electronic mail should be used for business purposes. EPHI shall not be transmitted by email for any reason except as necessary for a workforce member to perform job functions. Users of email shall avoid distasteful, inflammatory, harassing, or otherwise unacceptable comments or attachments. In the event the email system is deemed to be a moderate or high risk system during the risk analysis, additional limitations on email usage may be communicated to workforce members to help protect the confidentiality, integrity, and availability of EPHI.

3. Internet Usage. The Internet is to be used for business purposes only. Downloading files from the Internet is one way malicious software can attack computer systems. If reasonable and appropriate, TWU may restrict access rights to the Internet to ensure protection of its systems.

4. Third Party Software. No third party software may be installed on computers or workstations without the express consent of the Security Officer.

Security Awareness: Log-in Monitoring (45 CFR 164.308(a)(5)(ii)(C))

The HIPAA Security Standards under 45 CFR 164.308(a)(5)(ii)(C) require TWU to address whether it is reasonable and appropriate to implement a policy addressing log-in monitoring in light of the likely contribution such a policy would have on its efforts to protect EPHI in its possession.

After analyzing whether it would be reasonable and appropriate to implement a log-in monitoring policy, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because _____ _____ ___.**

The following alternative policy has been implemented:

_____

_____

_____

_____

_____

_____

TWU intends to protect the confidentiality, integrity, and availability of EPHI created, received, stored, transmitted, and retained on or through its systems. As workforce members access systems and EPHI, it is prudent to monitor system activity by each workforce member. To accomplish this, TWU may establish a log-in monitoring system that allows it to monitor log-in attempts and other system activity. The Security Officer or the Security Officer's designee will generate and review log-in activity.

Security Awareness: Password Management (45 CFR 164.308(a)(5)(ii)(D))

The HIPAA Security Standards under 45 CFR 164.308(a)(5)(ii)(D) require TWU to address whether it is reasonable and appropriate to implement a policy addressing password management in light of the likely contribution such a policy would have on its efforts to protect EPHI in its possession.

After analyzing whether it would be reasonable and appropriate to implement a password management policy, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because _____ _____ ___.**

The following alternative policy has been implemented:

_____

_____

_____

_____

_____

_____

Hackers often target passwords as means to unauthorized access to computer systems. As TWU's systems contain EPHI, it is important to create a system to manage and protect passwords to mitigate the risk of unauthorized access to these systems. The following general guidelines apply to the creation modification and safeguarding of passwords:

1. Password Creation. Passwords should be at least eight (8) characters in length and should not be related to a person's identity, history or environment. Each workforce member should have an individual password that is not shared by any other person.

2. Password Modification. Passwords should be changed reasonably often, but no less than once every quarter. If it is determined that a password has been compromised, the password will be replaced as quickly as possible. If a password is forgotten, it is to be replaced, not reissued. Passwords will be deleted when a workforce member no longer needs access to a particular system or separates from employment or other arrangement with TWU.

3. Password Protection. Workforce members shall not disclose or share their passwords with any person other than those persons specifically designated by the Security Officer. Workforce members shall be responsible for protecting passwords in their possession, and shall not post them on monitors or any other location in plain view.

Security Incident Procedures (45 CFR 164.308(a)(6)(i)-(ii))

A "security incident" is the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system. A security incident may include attempts to gain unauthorized access to EPHI, unwanted disruption or denial of service of systems processing or providing access to EPHI, unauthorized use of a system for the processing or storage of EPHI, or impermissible changes to systems that provide access to EPHI.

As a covered entity, it is TWU's responsibility to have procedures to identify occurrences of security incidents, respond to and mitigate harmful effects of security incidents and document the outcomes of all responses in accordance with 45 CFR 164.308(a)(6)(i).

1. Identifying and reporting security incidents. System vulnerabilities have been identified through the risk analysis process, and the Security Officer may implement procedures to monitor known system vulnerabilities. Any person that suspects or becomes aware of a security incident is required to immediately notify the Security Officer or the Security Officer's designee. The Security Officer or the Security Officer's designee will make note of the reported security incident and commence an investigation.

2. Investigation, response and mitigation. Once the security incident has been reported, the Security Officer or the Security Officer's designee will initiate an investigation into the causes and effects of the security incident. The results of the investigation will be documented. The Security Officer shall ensure that reasonable efforts are made to mitigate harmful effects of the security incident and shall decide upon a course of action to reduce the risk of future security incidents.

3. Documentation of outcomes. The Security Officer or the Security Officer's designee shall monitor for effectiveness and document the outcomes of the action taken in response to the security incident. If the response is ineffective the Security Officer shall work towards implementation of a reasonable and appropriate action plan to reduce the risk of future security incidents pursuant to 45 CFR 164.308(a)(6)(ii).

See the Sample HIPAA Security Incident Log Form, below.

Sample HIPAA Security Incident Log Form – Documents to be Reviewed and Customized Prior to Use

[TWU/NAME OF COMPONENT]'S

HIPAA SECURITY INCIDENT LOG FORM

GENERAL INFORMATION:
Name and Title of Individual Reporting Incident: _____
Date and Time Incident Reported: _____
Name and Title of Individual Who Received

Incident Report: _____

INFORMATION REGARDING INCIDENT:
Date and Time of Incident: _____
Place of Incident: _____
Date and Time of Incident Discovery: _____
Description of Investigation Completed (*Describe persons interviewed, records reviewed, etc.*):

_____
_____
_____
_____
_____
_____
_____

Description of Findings Regarding Incident (*Describe cause of incident, protected health information involved, etc.):*

_____
_____
_____
_____
_____
_____
_____

Description of TWU's Response (*Describe steps taken to mitigate harm, notification given, agencies (e.g., police, FBI, HHS) contacted, action taken to prevent future security incidents, etc.*):

_____
_____
_____
_____
_____
_____
_____

Signature of Security Officer: _____ Date: _____

Contingency Plan (45 CFR 164.308(a)(7)(i), 45 CFR 164.308(a)(7)(ii)(D)-(E))

Over the course of time, TWU may experience unexpected loss of operations of one or more of its systems. In the event of such a system emergency, the Security Officer must be contacted immediately. The Security Officer or the Security Officer's designee may activate one or more of TWU's contingency plans in response to such system emergencies. The following contingency plans have been developed:

1. Data-back up plan;
2. Disaster recovery plan; and
3. Emergency mode operation plan (pursuant to 45 CFR 164.308(a)(7)(i)-(ii)).

Additionally, TWU may develop the following procedures with respect to its contingency plans:

1. Testing and revision procedures; and
2. Applications and data criticality analysis (pursuant to 45 CFR 164.308(a)(7)(ii)(D)-(E)).

In the event of a system emergency, supervisors should contact the Security Officer for contingency plan implementation instructions and follow those instructions accordingly.

The purpose of contingency planning is to establish strategies for recovering access to EPHI in the event of a system compromise or other emergency situation.

Contingency Plan: Data Backup Plan (45 CFR 164.308(a)(7)(ii)(A))

When developing a data backup plan, TWU will consider incorporating the following components:

1. Regular backup of critical information;
2. Offsite storage of critical backup media (tapes, etc.) and hard copy documentation;
3. Methods for authorized individuals to access backed up data, including offsite back-ups;
4. Documented instructions for activating backed up data;
5. Testing of the data backup plan to ensure the system can be restored in the event of a system emergency; and
6. Periodic review and revision of backup procedures.

The purpose of the data backup plan is to ensure that critical data is maintained and safely stored offsite in a format that is retrievable and useable in the event of a system compromise or other emergency situation pursuant to 164.308(a)(7)(ii)(A).

Contingency Plan: Disaster Recovery Plan (45 CFR 164.308(a)(7)(ii)(B))

When developing a disaster recovery plan, TWU shall consider incorporating the following components:

1. Guidelines for the Security Officer to follow when determining whether to activate the disaster recovery plan;
2. Specific tasks and responsibilities of disaster recovery team members;
3. Procedure for assessing damage;
4. Procedures for restoring critical functions or accessing alternate equipment, space, etc.;
5. Alternate processing methods for lost systems (paper methods instead of computerized methods, etc.);
6. Complete workforce member information, vendor contacts, and vital records maintained offsite;
7. Testing of disaster recovery plan; and
8. Periodic review and revision of disaster recovery plan procedures.

The purpose of the disaster recovery plan is to establish procedures to restore any loss of data in the event of a system compromise or other emergency situation pursuant to 45 CFR 164.308(a)(7)(ii)(B).

Contingency Plan: Emergency Mode Operation Plan (45 CFR 164.308(a)(7)(ii)(C))

When developing an emergency mode operation plan, TWU will consider incorporating the following components:

1. Identify crisis management team members, roles and functions;
2. Identify a center of command through which team members and workforce members may communicate information;
3. Procedures for continued access and use of EPHI;
4. Testing of the emergency mode operation plan; and
5. Periodic review and revision of the emergency mode operation plan procedures.

The purpose of the emergency mode operation plan is to enable continuation of critical processes for protection and security of EPHI in the event of a technical failure, power outage or other emergency situation pursuant to 45 CFR 164.308(a)(7)(ii)(C).

Contingency Plan: Testing and Revision Procedures (45 CFR 164.308(a)(7)(ii)(D))

The HIPAA Security Standards under 45 CFR 164.308(a)(7)(ii)(D) require TWU to address whether it is reasonable and appropriate to implement a policy addressing the testing and revision of contingency plans in light of the likely contribution such a policy would have on TWU's efforts to protect EPHI in its possession.

After analyzing whether it would be reasonable and appropriate to implement a testing and revision procedures policy, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because** _____
_____
___.

The following alternative policy has been implemented:

_____

_____

_____

_____

_____

TWU will ensure that adequate procedures are in place to periodically test the Contingency Plans (i.e., data backup, disaster recovery, and emergency mode operation plans). Any errors or malfunctions identified during this review will be evaluated and corrected, if possible.

Contingency Plan: Applications and Data Criticality Analysis (45 CFR 164.308(a)(7)(ii)(E))

The HIPAA Security Standards under 45 CFR 164.308(a)(7)(ii)(E) require TWU to determine whether it is reasonable and appropriate to assess relative criticality of specific applications and data in support of other contingency plan components.

After analyzing whether it would be reasonable and appropriate to assess relative criticality of specific applications and data, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because** _____
_____
___.

The following alternative policy has been implemented:

_____

_____

_____

_____

_____

_____

TWU will identify its software applications (data applications that store, maintain or transmit EPHI) and determine how important each is to patient care or business needs, in order to prioritize for data backup, disaster recovery and/or emergency mode operation plans. A prioritized list of specific applications and data will help determine which applications or information systems get restored first and/or which must be available at all times.

Evaluation (45 CFR 164.308(a)(8))

TWU shall periodically perform technical and nontechnical evaluations, based upon the HIPAA standards and environmental or operational changes affecting the security of EPHI, that establish the extent to which TWU's security policies and procedures meet the requirements of HIPAA under 45 CFR 164.308(a)(8). In the event that TWU concludes after an evaluation that its security policies and procedures no longer meet the requirements of HIPAA, TWU shall revise such policies and procedures accordingly. On-going evaluations of the technical and nontechnical aspects of TWU's security measures shall be performed on a scheduled basis (such as annually or every two (2) years) as well as in response to changes in TWU's operations or environment. The Security Officer shall document all evaluations and resulting changes, if any.

Business Associate Contracts (45 CFR 164.308(b)(1)-(3))

TWU may permit a BA to create, receive, maintain, or transmit EPHI on its behalf only if TWU obtains satisfactory assurances, in accordance with HIPAA, that the BA will appropriately safeguard the information; provided, however, that TWU is not required to obtain such satisfactory assurances from a BA that is a subcontractor of TWU's direct BA (however, BAs should have a contractual relationship with the subcontractor providing for similar assurances). TWU shall document the required satisfactory assurances through a written contract or other arrangement with the BA that meets the applicable requirements of HIPAA under 45 CFR 164.308(b)(1)-(3).

A BAA must establish the permitted and required uses and disclosures of PHI by the BA. The contract may not authorize the BA to use or disclose PHI in a manner that would violate the requirements of HIPAA, if done by TWU. A BAA must provide that the BA will:

- ☐ Not use or further disclose the information other than as permitted or required by the contract or as required by law;

- ☐ Use appropriate safeguards and comply, where applicable, with the HIPAA Security Standards with respect to EPHI, to prevent use or disclosure of the information other than as provided for by the contract;

- ☐ Report to TWU any use or disclosure of the information not provided for by the contract of which it becomes aware;

- ☐ Ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the BA agree to the same restrictions and conditions that apply to the BA with respect to such information;

- ☐ Make available PHI in accordance with 45 C.F.R. § 164.524 of the HIPAA Privacy Standards;

- ☐ Make available PHI for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. § 164.526 of the HIPAA Privacy Standards;

- ☐ Make available the information required to provide an accounting of disclosures in accordance with 45 C.F.R. § 164.528 of the HIPAA Privacy Standards;

- ☐ To the extent the BA is to carry out any of TWU's obligations under HIPAA, comply with all requirements that apply to TWU in the performance of such obligation;

- ☐ Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the BA on behalf of, TWU available to the Secretary of Health and Human Services for purposes of determining TWU's compliance with its obligations under HIPAA;

- ☐ At termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the BA on behalf of TWU that the BA still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

- ☐ Authorize termination of the BAA by TWU if TWU determines that the BA has violated a material term of the contract under 45 CFR 164.314(a) and 45 CFR 164.504(e).

NOTE: BAAs are similarly referenced in the Privacy Policies sections above.

NOTE: BAAs must allow TWU to terminate the contract if TWU determines that the BA has violated a material term of the contract.

Facility Access Controls (45 CFR 164.310(a)(1))

TWU will implement measures to restrict access to its electronic information systems and facility(ies) to help protect the EPHI contained within its office(s) in accordance with 45 CFR 164.301(a). Limiting access to the facility(ies) is intended to help protect the confidentiality, integrity and availability of EPHI. Facility access controls may include any or all of the following:

1. Procedures to allow facility access in support of restoration of lost data in the event of an emergency;
2. Procedures to safeguard the facility and the equipment therein;
3. Procedures to control and validate access to the facility(ies) based on the role and function of individuals; and
4. Procedures to document repairs and modification to the physical components of a facility which are related to security.

Physical Safeguards

Facility Access Controls: Contingency Operations (45 CFR 164.310(a)(2)(i))

The HIPAA Security Standards under 45 CFR 164.310(a)(2)(i) require TWU to address whether it is reasonable and appropriate to implement a policy establishing contingency operations in light of the likely contribution such a policy would have on TWU's efforts to protect EPHI in its possession.

After analyzing whether it would be reasonable and appropriate to implement a contingency operations policy, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because _____ _____ ___.**

The following alternative policy has been implemented:

_____

_____

_____

_____

_____

_____

In the event of an emergency, TWU has established systems to maintain physical security while providing access to the facility(ies) to authorized personnel so that those individuals may work to restore lost data on systems containing EPHI. In the event keyless entry systems fails, the Security Officer shall immediately contact individuals with keys to the building to gain access. In addition to this "Contingency Operations" policy, the Security Officer may also implement the appropriate "Contingency Plans" discussed in these *HIPAA Policies and Procedures* to ensure that all workforce members are working toward recovery of system operations and protection of EPHI.

Facility Access Controls: Facility Security Plan (45 CFR 164.310(a)(2)(ii))

The HIPAA Security Standards under 45 CFR 164.310(a)(2)(ii) require the TWU to address whether it is reasonable and appropriate to implement a policy establishing a

facility security plan in light of the likely contribution such a policy would have on TWU's efforts to protect EPHI in its possession.

After analyzing whether it would be reasonable and appropriate to implement a facility security plan, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because** _____ _____ ___.

The following alternative policy has been implemented:

_____

_____

_____

_____

_____

_____

TWU has implemented the following facility protection measures to permit individuals with legitimate business needs to access the facility(ies) while preventing unauthorized access, tampering and/or theft of equipment or EPHI:

1. Keyless entry system with individualized access cards;
2. Locks on doors from the waiting room to the treatment areas;
3. Key locks on exterior doors;
4. Key locks on interior offices and equipment storage areas; and
5. Security system.

Facility Access Controls: Access Control and Validation Procedures (45 CFR 164.310(a)(2)(iii))

The HIPAA Security Standards under 45 CFR 164.310(a)(2)(iii) require TWU to address whether it is reasonable and appropriate to implement a policy establishing access control and validation procedures in light of the likely contribution such a policy would have on TWU's efforts to protect EPHI in its possession.

After analyzing whether it would be reasonable and appropriate to implement a policy addressing access control and validation procedures, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because _____ _____ ___.**

The following alternative policy has been implemented:

_____

_____

_____

_____

_____

_____

TWU has implemented the following measures to control and validate access to its facility(ies) based upon the role and function of the person desiring access:

1. Patients will sign-in using normal TWU sign-in procedures and will be escorted to and from treatment areas.

2. All other visitors, including contract workers, will sign-in at the front desk and provide:

☐ Full name

☐ Employer name and number (if person needs access to facility for work-related reason)

☐ Copy of work order, if any

☐ Reason for needing access

3. Non-patient visitors shall be escorted while in the facility(ies) and shall be monitored if performing contract work. Facility access shall be limited to the minimum amount necessary to perform the functions of the person's job (if a contractor) or to accomplish the purpose of the visit.

4. Any workforce member that observes a patient or other visitor wandering the halls or attempting to gain unauthorized access to any area within TWU's facility(ies) shall immediately contact the Security Officer.

Facility Access Controls: Maintenance Records (45 CFR 164.310(a)(2)(iv))

The HIPAA Security Standards under 45 CFR 164.310(a)(2)(iv) require TWU to address whether it is reasonable and appropriate to implement a policy concerning maintenance records in light of the likely contribution such a policy would have on TWU's efforts to protect EPHI in its possession.

After analyzing whether it would be reasonable and appropriate to implement a maintenance records policy, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because _____ _____ ___.**

The following alternative policy has been implemented:

_____

_____

_____

_____

_____

_____

The Security Officer or the Security Officer's designee shall be responsible for facility and equipment maintenance. A log shall be maintained documenting repairs and modifications to the physical components of the facility that relate to security, including hardware, doors, walls, locks, security system maintenance, etc. Information contained in the log shall include:

1. Description of equipment or facility component repaired or maintained;
2. Description of location of equipment or facility component;
3. Description of actual repair or maintenance; and
4. Date of repair or maintenance.

Workstation Use and Security (45 CFR 164.310(b)-(c))

The HIPAA Security Standards under 45 CFR 164.310(b)-(c) require TWU to implement procedures specifying proper functions to be performed at workstations; the manner in which to perform such functions; and physical attributes and surroundings of a specific workstation or a class of workstations that can access EPHI.

Proper workstation use is critical to TWU's efforts to protect the confidentiality, integrity, and availability of EPHI accessed, created, stored, and maintained by TWU. To best protect EPHI through the use of TWU's workstations, workforce members shall:

1. Access only such hardware or software programs that workforce members need to perform the functions of their job and refrain from accessing any hardware or software program that is not needed to perform a job-related function;

2. Refrain from downloading any unauthorized software;

3. Refrain from transmitting EPHI to any third party unless previously authorized to do so;

4. Refrain from accessing private email accounts and opening any emails or attachments that are not related to workforce member's job or from an unknown sender;

5. Not remove any hardware, software or EPHI from the facility without prior permission from the Security Officer;

6. Not disclose usernames or passwords to any person other than the Security Officer;

7. Not use usernames or passwords of any other workforce member to gain access to any system containing EPHI;

8. Log off workstations or enable a password protected screen saver when leaving a workstation that has access to EPHI;

9. Work with the Security Officer to physically adjust workspaces to keep computer monitors out of view of persons passing by the workstation; and

10. Work with the Security Officer to develop workstation-specific procedures to help physically secure each workstation and protect EPHI from access by unauthorized individuals.

Device and Media Controls (45 CFR 310(d)(1)-(2)(ii))

The HIPAA Security Standards under 45 CFR 164.310(d)(1)-(2)(ii) require TWU to implement procedures to govern the receipt and removal of hardware and electronic

media that contain EPHI, and the movement of such hardware and electronic media into and out of TWU's facility(ies).

To comply with these HIPAA requirements, TWU has implemented the following policies:

A. Disposal

1. No workforce member shall dispose of EPHI, including EPHI contained on electronic media, without first contacting the Security Officer. The Security Officer shall provide instructions for removal or disposition of EPHI and may monitor the process to ensure that EPHI removed may not be reconstructed.

2. TWU will replace hardware from time to time to maintain or improve operational efficiency. No hardware will be removed, transferred or sold before EPHI is removed.

B. Media Re-Use

1. Media used for daily back-up of data do not need to have EPHI removed on a daily basis before being used again.

2. Other media that is not used for purposes of daily back-up of data shall have EPHI removed prior to being used again.

The HIPAA Security Standards under 45 CFR 164.310(d)(2)(iii)-(iv) also require TWU to address whether it is reasonable and appropriate to account for movement of hardware and electronic media in the facility and whether copies of EPHI contained on such hardware or electronic media should be created prior to movement.

After analyzing whether it would be reasonable and appropriate to implement the policies below, TWU has determined that:

_____ **It is reasonable and appropriate to implement procedures to (*please check as appropriate*) ____ account for movement of hardware and electronic media; ____ create a data backup prior to moving hardware and electronic media.**

_____ **It is not reasonable and appropriate to implement procedures to (*please check as appropriate*) ____ account for movement of hardware and electronic media; ____ create a data backup prior to moving hardware and electronic media because _____ _____ _____.**

The following alternative policy has been implemented:

_____

_____

C. Accountability

The Security Officer or his/her designee shall maintain a record of the movements of hardware and electronic media in the facility(ies) or otherwise in TWU's possession, whether for use within or outside TWU's facility(ies). The record shall include the starting location, the final location, the name of the person that moved the hardware or electronic media, and the date of the move. This procedure shall not apply to daily offsite backups.

D. Data Backup and Storage

The Security Officer shall oversee the creation of retrievable, exact copies of EPHI, when needed, before movement of equipment containing EPHI.

Technical Safeguards

Access Control (45 CFR 164.312(a)(1))

In accordance with 45 CFR 164.312(a)(1), TWU will implement measures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights. In addition to the assignment of unique user identifications and establishing and implementing procedures for obtaining necessary EPHI during an emergency, these processes may include any or all of the following:

1. Automatic logoff procedures; and
2. Encrypting and decrypting EPHI.

Access Control: Unique User Identification (45 CFR 164.312(a)(2)(i))

User identification is a way to identify a specific user of an information system, typically by name and/or number. A unique user identifier allows an entity to track specific user activity when that user is logged into an information system. It enables an entity to hold users accountable for functions performed on information systems with EPHI when logged into those systems. TWU shall assign a unique name and/or number for identifying and tracking each user who accesses EPHI pursuant to 45 CFR 164.312(a)(2)(i).

Access Control: Emergency Access Procedure (45 CFR 164.312(a)(2)(ii))

In accordance with 45 CFR 164.312(a)(2)(ii), in the event of an emergency, the Security Officer shall implement the Contingency Plans, as necessary, and shall begin the process of retrieving critical EPHI. The Security Officer may consult with the office administrator and the physicians concerning requesting assistance retrieving critical EPHI from vendors, if necessary.

The Security Officer may request certain workforce members to assist with data retrieval, in which case the Security Officer will coordinate assistance from workforce members with the office administrator.

Access Control: Automatic Logoff (45 CFR 164.312(a)(2)(iii))

The HIPAA Security Standards under 45 CFR 164.312(a)(2)(iii) require TWU to address whether it is reasonable and appropriate to implement a policy addressing automatic logoff of workstations in light of the likely contribution such a policy would have on TWU's efforts to protect EPHI in its possession.

After analyzing whether it would be reasonable and appropriate to implement an automatic logoff policy, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because** _____ _____ ___**.**

The following alternative policy has been implemented:

_____

_____

_____

_____

_____

_____

All workstation computers, personal computers with remote access, or any other application that accesses EPHI with log-in capabilities shall be programmed to log out after fifteen (15) minutes of inactivity. Once an application has been logged out, the user will be required to log-in before accessing the application again.

Access Control: Encryption and Decryption (45 CFR 164.312(a)(2)(iv))

The HIPAA Security Standards under 45 CFR 164.312(a)(2)(iv) require TWU to address whether it is reasonable and appropriate to implement a policy addressing encryption and decryption of EPHI in light of the likely contribution such a policy would have on TWU's efforts to protect EPHI in its possession.

After analyzing whether it would be reasonable and appropriate to implement an encryption and decryption policy, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because** _____ _____ ___**.**

The following alternative policy has been implemented:

_____

_____

_____

_____

_____

_____

TWU will install and configure encryption and decryption products and encrypt and decrypt EPHI in its possession as and when deemed appropriate by the Security Officer. TWU will store decryption tools in a separate location from the data.

Audit Controls (45 CFR 164.312(b))

The HIPAA Security Standards under 45 CFR 164.312(b) require TWU to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI. TWU shall implement reasonable and appropriate audit controls (such as periodic review of information system audit reports) based on TWU's risk analysis assessment and security system capabilities.

Integrity (45 CFR 164.312(c)(1))

The HIPAA Security Standards under 45 CFR 164.312(c)(1) require TWU to implement procedures to protect EPHI from improper modification or destruction. These procedures may include mechanisms to authenticate EPHI.

The purpose of this standard is to prevent the unauthorized alteration or destruction of EPHI by both technical (e.g., electronic media errors or failures) and non-technical (e.g., environment, accidents, intentional acts) sources.

Integrity: Mechanism to Authenticate EPHI (45 CFR 164.312(c)(2))

The HIPAA Security Standards under 45 CFR 164.312(c)(2) require TWU to address whether it is reasonable and appropriate to implement a policy addressing mechanisms to authenticate EPHI in light of the likely contribution such a policy would have on TWU's efforts to protect EPHI in its possession.

After analyzing whether it would be reasonable and appropriate to implement a mechanism to authenticate EPHI, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because** _____ _____ ___**.**

The following alternative policy has been implemented:

_____

_____

_____

_____

_____

_____

TWU shall implement one or more mechanisms to authenticate EPHI to ensure that EPHI has not been altered or destroyed in an unauthorized manner. Such mechanisms may include error-correcting memory, magnetic disc storage, digital signatures, check sum technology, or any other mechanism deemed appropriate by TWU.

Person or Entity Authentication (45 CFR 164.312(d))

The HIPAA Security Standards under 45 CFR 164.312(d) require TWU to implement procedures to verify that a person or entity seeking access to EPHI is the one claimed. There are a number of ways TWU may verify the identity of a person or entity, including but not limited to:

1. Implementation of a password system;
2. Assignment of a personal identification number;
3. Telephone callbacks;
4. Implementation of a token system; or
5. Use of digital signatures.

The Security Officer shall designate the method and manner in which workforce members shall verify the identity of a person or entity seeking access to EPHI.

Transmission Security (45 CFR 164.312(e)(1), 164.312(e)(2)(i)-(ii))

The HIPAA Security Standards under 45 CFR 164.312(e)(1) require TWU to implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network. Technical security measures may include any or all of the following:

1. Integrity controls; and
2. Encryption.

The HIPAA Security Standards under 45 CFR 312(e)(2)(i)-(ii) require TWU to address whether it is reasonable and appropriate to implement a policy addressing integrity controls and encryption and decryption of EPHI in light of the likely contribution such a policy would have on TWU's efforts to protect EPHI in its possession.

After analyzing whether it would be reasonable and appropriate to implement an encryption and decryption policy, TWU has determined that:

_____ **It is reasonable and appropriate to implement the policy set forth below.**

_____ **It is not reasonable and appropriate to implement the policy set forth below because** _____ _____ ___.

The following alternative policy has been implemented:

_____

_____

As additional integrity safeguards, TWU shall periodically review the methods used to transmit EPHI over an electronic network and identify available and appropriate measures to protect EPHI as it is transmitted, select appropriate solutions, and document decisions.

As additional encryption safeguards, TWU will install and configure encryption products and encrypt and decrypt EPHI in its possession as and when deemed appropriate by the Security Officer.

SECURITY SAFEGUARDS (45 CFR 164.530)

Each TWU health care component must develop and implement administrative protocols and practices, as well as technical and physical safeguards that reasonably protect health information from intentional and unintentional use and disclosure that violates federal or Texas law and regulations.

TWU Safeguard Requirements for Health Care Components (45 CFR 164.504)

Policies regarding TWU's HIPAA Security Safeguards and Procedures are covered in TWU's HIPAA Security Manual.

Those covered by this policy must develop and implement adequate protection between covered and non-covered functions or components. This protection shall be implemented by means of firewalls, policies, and procedures.

The health care component Privacy Officer must be consulted and must approve the implementation of protection measures that affect the operation of the health care component. Protection measures that are proposed and that are implemented must also be filed with the HIPAA Compliance Officer for review.

Use of Electronic Communication of PHI

Fax Transmittal of PHI

Each TWU health care component must develop protocols and forms that adhere to the following standards relating to facsimile (fax) communications of an individual's medical records, and each workforce member must follow the designated procedures:

- PHI may only be sent by fax when the original record or mail-delivered copies will not meet the needs for TPO.

- Information transmitted must be limited to the minimum necessary to meet the requester's needs.
- Except as authorized by state or federal law, or as authorized by the individual's consent, a properly completed and signed authorization must be obtained before releasing PHI.
- The following types of medical information are protected by federal and/or state statute and may not be faxed or photocopied without specific written patient authorization, unless required by law:
    - Psychotherapy treatment by a psychiatrist or a licensed psychologist;
    - Other professional services of a licensed psychologist;
    - Social work counseling and therapy;
    - Domestic violence victims' counseling;
    - Sexual assault counseling.;
    - HIV test results, and an individual's written authorization is required for each separate release request;
    - Records relating to sexually transmitted disease; and
    - Alcohol and drug abuse records protected by federal confidentiality rules (cf. 42 CFR Part 2).
- A designated fax cover page, marked CONFIDENTIAL, must be used to send faxes containing PHI.
- Workforce members must take reasonable precautions to send the PHI to the correct location, using the correct phone number. If they are uncertain of the fax number, they must first call the location and verify the fax number with a person at the remote location.

Documentation of Successfully Transmitted Faxes

The TWU health care component sending a fax for TPO purposes may wish to maintain a copy of the fax transmittal or fax confirmation sheet in the individual's record, but it is not required to do so.

The health care component sending a fax for non-TPO purposes, based on an authorization of the individual or based on a request that does not require the consent of the individual, must maintain a copy of the fax transmittal sheet or, if available, the fax confirmation sheet in the individual's record. It must also enter the transmission into the health care component's disclosure accounting database.

Misdirected Faxes

If a fax is known to have arrived at an incorrect location, the workforce member must obtain the incorrect number from the fax memory and must attempt to contact a party by phone at the remote location to request that the misdirected fax be destroyed in its entirety. If no one is available by phone at the remote location, a form designated by the health care component must be faxed to the incorrect number with a request that the misdirected fax be destroyed in its entirety. The number to which the misdirected fax was sent must be entered into the disclosure accounting database with a notation that the fax was sent erroneously to that location.

Receipt of Faxes with PHI

Fax machines designated for receiving PHI must not be located in areas accessible to the general public or to workforce members who do not have authorization to access PHI. The director of the health care component, in conjunction with workforce members responsible for security, shall designate a secure location for fax machines.

Incoming fax documents are confidential PHI and must be handled in compliance with this policy and with the health care components procedures and practices.

If a fax is received in error, the receiving department shall immediately notify the sending party, and then shall either destroy it in its entirety or shall follow the directions of the sending party.

Email Transmission of PHI

Electronic mail that is sent, received, or stored on computers that are owned, leased, administered, or otherwise under the custody and control of TWU is the property of TWU and subject to this URP.

- Email transmission of PHI shall only be permitted after encryption has been implemented in the TWU email system.
- Email containing PHI must be treated with the same degree of privacy and confidentiality as the patient's medical record.
- TWU health care components shall make all email messages sent or received that concern the treatment of an individual part of the individual's record.
- Emailing PHI with the TWU email system is permitted for TPO.
- TWU workforce members may not send or forward any PHI outside the TWU email network unless specifically authorized by the individual.
- When using email TWU workforce members must limit the information transmitted to the minimum necessary to meet the requestor's needs and must use de-identified PHI whenever possible.
- All external disclosures of PHI through email must comply with policy and procedures that deal with authorizations and accounting of disclosures.

Email Correspondence Between TWU Workforce Members and Patients or Clients

Prior to using email to correspond with patients or clients, the individual must consent to the use of the email for transmitting confidential PHI and must indicate this in writing on their patient consent form and sign the form.

- TWU workforce members must make sure that the individual has given written consent to correspond through email before doing so.
- Email clients must permit encryption of the PHI transmitted.
- Email should not be used to replace a clinical visit. A health care provider must use due care in determining if email is appropriate for the individual's treatment, based on the individual's case history.

- At the conclusion of a dialogue with an individual, all emails regarding health care must be forwarded to the medical records custodian to become part of the individual's medical record.

Medical Records Including Email Correspondence Between Physicians

Physicians may email other TWU physicians within the TWU internal email system regarding patient matters.

If email contains PHI for treatment, the email must be printed and forwarded to the medical records custodian to become part of the individual's medical record.

Accounting for Email Disclosures

When email is used for disclosing PHI, the release must be documented in compliance with this URP.

Maintenance and Storage of PHI

TWU health care components have a duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. All TWU workforce members must strictly observe the following standards for storing PHI:

- Before regular working hours have ended, workforce members must clean desks and working areas so that PHI is properly secured, unless the immediate area can be secured from unauthorized access.
- When not in use, PHI must always be protected from unauthorized access. When left in an unattended room, such information must be appropriately secured.
- If PHI is stored on the hard disk drive or other internal components of a computer workstation, personal computer, or personal digital assistant ("***PDA***"), it must be protected by either a password or encryption. Unless encrypted when not in use, computers and their storage units must be secured from unauthorized access.
- If PHI is stored on diskettes, CD-ROMs, ZIP disks, or any other type of removable data storage media, it cannot be commingled with other electronic information.
- If backup copies of PHI are moved to a location away from campus to ensure redundancy and integrity of data, the remote location must be secure and the person transporting the copies must have security clearance and documented training in the requirement of the Privacy Act.
- When PHI is being released through teleconference or video feed, TWU workforce members must treat the protection of the PHI in the same manner as PHI recorded on paper, thereby securing access to the teleconference or video to authorized personnel only. Support staff for the teleconference or video feed must have documented training regarding HIPAA compliance procedures if they will have contact with PHI during the teleconference or video feed.
- PHI stored in medical equipment (EKG, etc.) must be kept secure and disposed of in compliance with this policy.

Each TWU health care component shall develop the procedures and workforce training necessary to ensure the integrity and confidentiality of stored PHI.

Printing and Copying of PHI

All TWU workforce members must strictly observe the following standards relating to the printing and copying of PHI:

- PHI in hardcopy format must be disposed of in accordance with this policy and with records retention schedules;
- Printed versions of PHI should not be copied indiscriminately or left unattended and open to compromise;
- Printers and copiers used for printing and copying PHI should be in a secure, non-public location. If the equipment is in a public location, the information being printed or copied is required to be strictly monitored;
- PHI must not be downloaded to personally owned mobile devices, including mobile storage devices (e.g., Cell phone, CD, DVD, flash drive, or external drive);
- PHI should never be stored on social networking websites or transmitted through peer-to-peer applications;
- Defective copies or printouts of PHI must be secured and immediately disposed of, in compliance with this policy;
- Access controls must be enforced to ensure that workforce members who transport and dispose of PHI have appropriate security clearance and training; and
- PHI printed to a shared printer shall be promptly removed from the printer and secured.

Disposal of PHI

All TWU workforce members must strictly observe the following standards for disposal or hardcopy and electronic copies of PHI:

- PHI must not be discarded in trash bins, recycle bins (including those with locks), or other locations accessible to the public;
- PHI must be personally shredded or disposed of in any reasonable way that renders documents unreadable;
- Printed material and electronic data containing PHI shall be disposed of in a manner that ensures confidentiality; and
- Each individual handling PHI is responsible for ensuring that documents containing PHI are either secured or destroyed. Supervisors are likewise responsible for ensuring that their employees and volunteers adhere to this policy.

Destruction of Convenience Copies

TWU health care component officers and directors shall provide workforce members in their health care component with access to shredders for proper disposal of confidential printouts containing PHI.

Electronic Copies

Secure methods shall be used to dispose of electronic data and output. Acceptable methods are determined by the University Computing Center to be compliant with Texas law and Department of Information Resources and General Services Commission Regulations.

Destruction of Originals

Original documents shall be retained in accordance with records retention schedules, and then shall be destroyed in compliance with this URP. PHI printed material shall be shredded by a workforce member authorized to handle and personally shred the PHI. Microfilm or microfiche must be cut into pieces or chemically destroyed. If hardcopy PHI cannot be shredded, it must be incinerated, using a BA that specializes in the disposal of confidential records.

Documentation of Destruction

To ensure that PHI is in fact destroyed and disposed of properly, TWU workforce members or a bonded BA specializing in this service must carry out the destruction of PHI.

If TWU workforce members destroy the records, the TWU workforce member must use the records destruction form provided by their health care component or department to record the date and method of destruction, and a description of the records being destroyed.

If a bonded BA destroys the PHI, such bonded BA must provide the TWU health care component Privacy Officer with a document of destruction that contains the following information:

- Date of destruction;
- Method of destruction;
- Description of the disposed records;
- Inclusive dates covered;
- A statement that the records have been destroyed in the normal course of doing business; and
- The signatures of the individuals supervising and witnessing the destruction.

The TWU health care component shall retain destruction documents permanently.

APPENDIX I

ACRONYMS

BA Business Associate

DPS Department of Public Safety

DRS Designated Record Set

EPHI Electronic Protected Health Information

HCC Health Care Components

HCO HIPAA Compliance Officer

HCP Health Care Provider

HOC Health Care Operations

ITR Indirect Treatment Relationship

LDS Limited Data Set

NPP Notice of Privacy Practice(s)

PHI Protected Health Information

TPO Treatment, Payment, and health care Options

TWU Texas Woman's University

GLOSSARY

Administrative Safeguards (45 CFR 164.304): administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

Authentication (45 CFR 164.304): the corroboration that a person is the one claimed.

Availability (45 CFR 164.304): the property that data or information is accessible and usable upon demand by an authorized person.

Breach (45 CFR 164.402):

(1) Includes the acquisition, access, information in a manner which compromises the security or privacy of the protected health information. An acquisition, access, use, or

disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;

(iii) Whether the protected health information was actually acquired or viewed; and

(iv) The extent to which the risk to the protected health information has been mitigated.

(2) Excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted;

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed; and

(iii) A disclosure of protected health information where a covered entity or business associate 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.

Business Associate (BA) (45 CFR 160.103)**:**

(1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in 45 CFR §164.501), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves

the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) Business associate includes:

(i) A health information organization, electronic-prescribing gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) Business associate does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of §164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

(5) A covered entity may use a business associate, including a health care clearinghouse, to conduct a transaction covered by this part. If a covered entity chooses to use a business associate to conduct all or part of a transaction on behalf of the covered entity, the covered entity must require the business associate to do the following (45 CFR 162.920):

(i) Comply with all applicable requirements of this part.

(ii) Require any agent or subcontractor to comply with all applicable requirements of this part.

Common Control (45 CFR 164.103): exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

Common Ownership (45 CFR 164.103): exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Confidentiality (45 CFR 164.304): the property that data or information is not made available or disclosed to unauthorized persons or processes.

Consents: Unless there is an emergency, TWU health care components should not treat a patient if an individual has not signed and executed the proper HIPAA consent form. TWU workforce members may use and disclose PHI for Treatment, Payment, and health care Options (TPO) without obtaining the consent of the individual only in the following instances:

- When an indirect treatment relationship exists;
- When an emergency situation exists;
- When treatment is required by law; or
- When substantial barriers in communication exist and the patient's consent is clearly inferred from the circumstances.

If failure to obtain consent occurs, the reasons for the failure to obtain consent must be documented on the consent form.

It should be clearly understood the consent for the use and disclosure of PHI does not allow TWU or its workforce members to use or disclose PHI for any reasons other than for TPO. For TWU to use and disclose PHI for purposes other than for TPO, the individual must sign an authorization.

Psychotherapy notes are not to be included as PHI that may be disclosed, unless consent is sought for each such use or disclosure.

Consents to use and disclose PHI for TPO must have the following elements for the consent to be effective:

- Inform the patient or surrogate decision maker that PHI may be used and disclosed to carry out TPO;

- Refer the patient or surrogate decision maker to the NPP for a more complete description of such uses and disclosures and state that the patient or surrogate decision maker has the right to review the NPP prior to signing the consent;

- State the patient or surrogate decision maker may request a restriction be placed on the consent (see Section 10.7.5.4.1); and

- The consent must be signed by the patient or surrogate decision maker and dated. TWU health care components reserve the right to change their privacy practices described in their NPP. If a TWU health care component changes the terms of its NPP, it will describe how the patient or surrogate decision maker may obtain a revised NPP.

Covered Entity (45 CFR 160.103) means:

(1) A health plan;

(2) A health care clearinghouse; or
(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Under Texas Health and Safety Code 181.001, Covered Entity also means any individual who:

> (A) For commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis, engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information. The term includes a business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, health care provider, or person who maintains an Internet site;
>
> (B) Comes into possession of protected health information;
>
> (C) Obtains or stores protected health information under this chapter; or
>
> (D) Is an employee, agent, or contractor of a person described by Paragraph (A), (B), or (C) insofar as the employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits protected health information.

Section 181.001(b), of the Texas Health and Safety Code expands the definition of "covered entity" to include any entity that engages in "assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information," as well as any entity that "comes into possession of" or "obtains or stores" protected health information.

Covered Functions (45 CFR 164.103): those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Defective Consents: Lack an element required in the consent or become defective if the consent has been revoked.

Designated Record Set (DRS) (45 CFR 164.501):

(1) A group of records maintained by or for a covered entity that is:
  (i) The medical records and billing records about individuals maintained by or for a covered health care provider;
  (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
  (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.
(2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

TWU designates the following as components of the Designated Record Set:

- Primary Medical Records including, but not limited to:
    - Reports of relevant physical examinations;
    - Diagnostic and therapeutic orders;
    - Clinical observations;
    - Reports of procedures, tests and results;
    - Summaries and plans at the conclusion of evaluation and treatment;
    - Correspondence to or from health care providers;
    - Prescription information.
- Billing Records are the information maintained by TWU in its electronic billing system used to receive payment for health care services provided by a TWU health care component.

Exclusions from the DRS are secondary records which are not part of the DRS, but may be placed in the medical record for convenience. Secondary Records include, but are not limited to:

- Copies of medical records and/or reports from other health care providers that were sent to TWU for consultation services;
- Letters to and from the individual;
- Requests and correspondence from insurance companies not responsible for the payment of the individual's account;
- Correspondence to and from any attorney or record service;
- Correspondence and/or reports generated by clinic personnel sent out on behalf of and at the request of the individual;
- Audit, survey, or research information;
- All other entries which are not part of the official health record, specifically that do not contain details of direct patient care/treatment made by TWU workforce members in the regular course of business at or near the time treatment was provided.

DRSs will be retained for a period of (7) years from the date of its creation or the date when it last was in effect, whichever is later.

Disclosure (45 CFR 160.103): The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Electronic Media (45 CFR 160.103):

(1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; and
(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of

removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

Electronic Protected Health Information (EPHI) (45 CFR 160.103): Information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information as specified in this section.

Encryption (45 CFR 164.304): 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.

Facility (45 CFR 164.304): the physical premises and the interior and exterior of a building(s).

Health Care (45 CFR 160.103): care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health Care Component (HCC) (45 CFR 164.103): a component or combination of components of a hybrid entity designated by the hybrid entity as 'health care components.'

Health Care Operations (HOC) (45 CFR 164.501/164.506): Any one of the following activities to the extent the activities are related to providing health care:

- Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting patients with information about treatment alternatives, and related functions that do not involve treatment;
- Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
- Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding,

securing or placing a contract for reinsurance of risk relating to claims for health care;
- Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
- Business planning and development, such as conducting cost management and planning related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or covered policies, and;
- Business management and general administrative activities:
    - Management activities related to HIPAA compliance;
    - Customer service;
    - Resolution of internal grievances;
    - Due diligence; and
    - Activities designed to de-identify health information and fundraising activities for the benefit of the institution.

Health Care Provider (HCP) (45 CFR 160.103): A provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x (u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health Information (45 CFR 160.103): any information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

HIPAA Compliance Officer (HCO): The person responsible for the development, implementation, and revision of TWU policies, regulations, and procedures related to HIPAA compliance. (45 CFR 164.530)

Hybrid Entity (45 CFR 164.103): A single legal entity:

(1) That is a covered entity;

(2) Whose business activities include both covered and non-covered functions; and

(3) That designates health care components in accordance with paragraph § 164.105(a)(2)(iii)(C).

Indirect Treatment Relationship (ITR): A relationship between an individual and a health care provider in which:

- The health care provider delivers health care to the individual based on the orders of another health care provider; and
- The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services, products or reports to the individual.

Individual (45 CFR 160.103): The person who is the subject of protected health information.

Individually Identifiable Health Information (45 CFR 160.103): Information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
    (i) That identifies the individual; or
    (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Information System (45 CFR 164.304): an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity (45 CFR 164.304): the property that data or information have not been altered or destroyed in an unauthorized manner.

Limited Data Set (LDS) (45 CFR 164.514): PHI that excludes direct identifiers of the individual or of relatives, employers, or household members of the individual including names, address (other than town/city, state, and zip code), telephone numbers, fax numbers, email addresses, social security numbers, medical records, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers and serial numbers (including license plate numbers, device identifies and serial numbers, URLs, IP addresses, biometric identifiers (including finger and voice prints), and full face photographic images.

Malicious Software (45 CFR 164.304): software, for example, a virus, designed to damage or disrupt a system.

Minimum Necessary: When using or disclosing PHI or when requesting PHI from another health care provider or health organization, TWU must limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. Minimum Necessary does not apply in the following circumstances:

- Disclosures by a health care provider for treatment (students and trainees are included as health care providers for this purpose);
- Uses and disclosures based upon a valid consent to use and disclose PHI for treatment, payment and health care operations or a valid authorization to use and disclose PHI;
- Disclosures made to the Secretary of Health and Human Services;
- Uses and disclosures required by law; and
- Uses and disclosures required by other sections of the HIPAA privacy regulations. For a more detailed explanation of Minimum Necessary, see Section 10.7.4.

Notice of Privacy Practice (NPP) (45 CFR 164.520): Covered Entities are required to provide a notice of privacy practices to patients that include: (1) how the covered entity may use and disclose PHI; (2) the patient's rights as noted by HIPAA; and (3) how PHI will be maintained and protected.

Password (45 CFR 164.304): confidential authentication information composed of a string of characters.

Payment*:* Any activities undertaken either by a health plan or by a health care provider to obtain premiums, determine or fulfill its responsibility for coverage and the provision of benefits or to obtain or provide reimbursement for the provision of health care. These activities include but are not limited to:

- Determining eligibility, and adjudication or subrogation of health benefit claims;
- Risk adjusting amounts due based on enrollee health status and demographic characteristics;
- Billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care processing;
- Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
- Utilization review activities, including pre-certification and preauthorization services, concurrent and retrospective review of services; and
- Disclosure to consumer reporting agencies of certain PHI relating to collection of premiums or reimbursement.

Physical Safeguards (45 CFR 164.304): physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Protected Health Information (PHI) (45 CFR 160.103): individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:
    (i) Transmitted by electronic media;

(ii) Maintained in electronic media; or
(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information:
(i) In Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
(ii) In Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
(iii) In Employment records held by a covered entity in its role as employer.
(iv) Regarding a person who has been deceased for more than 50 years.

Security or Security Measures (45 CFR 164.304): All of the administrative, physical, and technical safeguards in an information system. Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Security Incident (45 CFR 164.304): The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Technical Safeguards (45 CFR 164.304): The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

Transaction (45 CFR 160.103): The transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information.
(2) Health care payment and remittance advice.
(3) Coordination of benefits.
(4) Health care claim status.
(5) Enrollment and disenrollment in a health plan.
(6) Eligibility for a health plan.
(7) Health plan premium payments.
(8) Referral certification and authorization.
(9) First report of injury.
(10) Health claims attachments.
(11) Health care electronic funds transfers (EFT) and remittance advice.
(12) Other transactions that the Secretary may prescribe by regulation.

Treatment: The provision, coordination, or management of health care related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or for the referral of a patient for health care from one health care provider to another.

Treatment, Payment, and health care Options (TPO): Commonly used phrase and abbreviation for treatment, payment, and health care options.

Use (45 CFR 160.103): *With respect to individually identifiable health information*: The sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

User (45 CFR 164.304): A person or entity with authorized access.

Workforce (45 CFR 160.103): employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Workstation (45 CFR 164.304): an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

Unsecured Protected Health Information (45 CFR 164.402): protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5.

SPECIAL NOTES

Each Covered Entity must develop its own Authorization to Disclose and Protected Health Information and Privacy Practice Notice.

Relationship between HIPAA and FERPA

The HIPAA Privacy Regulations safeguards “protected health information,” whereas the Family Educational Rights and Privacy Act (FERPA) deals with the privacy of “education records.” The U.S. Department of Health and Human Services specifically exempted from its definition of “protected health information” FERPA’s education records.

FERPA defines education records as those records that contain information directly related to a student that are maintained by an education agency, institution or a person acting for the agency or institution. FERPA education records do not include records of students who are eighteen (18) years or older, or are attending post-secondary educational institutions, which are:

- Created or maintained by a physician, psychiatrist, psychologist, or recognized professional or paraprofessional acting or assisting in that capacity;
- Created, maintained, or used only in connection with the provision of treatment to the student; and
- Not available to anyone, except a physician or appropriate professional reviewing the record as designated by the student.

Any use or disclosure of the above medical records for other purposes, including providing access to the individual student who is the subject of the information, turns the record into an educational record protected by FERPA.

However, a student may access his or her medical records by making a request under the Texas Public Information Act. To avoid the need to apply two different standards to student records, HIPAA excludes from its definition of "protected health information" the student medical records that an educational institution obtains, whether or not they qualify as education records.

This policy recognizes that both HIPAA and FERPA require authorization from an individual to disclose their protected health information. In some circumstances, FERPA requirements may be more stringent than HIPAA requirements. To facilitate the operation of all TWU health care components, all discussions of consents and authorizations in this policy apply to both HIPAA and FERPA records. The health care component shall develop only one set of forms and procedures to comply with both sets of federal regulations. The health care component Privacy Officer shall be responsible for overseeing the processing of authorizations and requests for PHI, regardless of which set of regulations applies. However, the Privacy Officer will ensure that the permissions needed to approve a HIPAA or FERPA request will be obtained from the proper authority. The TWU Office of General Counsel shall have the authority to approve all FERPA requests, and is designated as the final authority for many types of HIPAA requests.

There will be instances in which student records will be converted from HIPAA records to FERPA records. For example, students with disabilities requesting accommodations are often asked to produce a physician's certification of disability before the institution makes the requested accommodation. The information disclosed by the non-institution-affiliated physician ceases to be protected health information under HIPAA once the information is shared, at the student's request, with the institution. TWU must accept this information and protect it as it would receive and protect any other HIPAA PHI. However, now that the student has made the medical information available to the institution, it falls under the protections of FERPA and may not be further released without the student's permission.

Under no circumstances are students medical or student educational records disclosed to the Department of Health and Human Services as a part of a Department of Health and Human Services audit or investigation of any TWU health care component.

Publication Date: 07/02/2021

Revised: 02/23/2023

Exhibit 1 – Sample Business Associate Agreement

(Attached)

Sample Business Associate Agreement – Documents to be Reviewed and Customized Prior to Use

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the "BA Agreement") is entered into and effective as of the _____ day of _____, 20___ ("Effective Date") by and between ***[insert name of TWU Covered Entity]*** ("Covered Entity"), and ***[insert name of Business Associate]*** ("Business Associate") (collectively, the "Parties").

WITNESSETH

WHEREAS, Covered Entity is a "covered entity" as defined in the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder ("HIPAA"), and as described in the Health Information Technology for Economic and Clinical Health Act ("HITECH") provisions of the American Recovery and Reinvestment Act of 2009 ("ARRA") (and together HIPAA, HITECH and ARRA are the "Regulations"); and

WHEREAS, Business Associate provides ***[specifically describe services]*** services (the "Services") for Covered Entity ***[under the terms of that certain agreement between the Parties executed [date]]*** (the "Services Agreement"), the performance of which involves the creation, receipt, maintenance, or transmission of certain Protected Health Information, as defined in 45 CFR 160.103 and limited to the information created or received by Business Associate from or on behalf of Covered Entity ("PHI"); and

WHEREAS, HIPAA requires that Covered Entity enter into written agreements with its business associates in order to regulate the use and disclosure of certain protected health information of Covered Entity; and

WHEREAS, Covered Entity and Business Associate agree to enter into this BA Agreement under the terms and conditions set forth herein to meet the applicable requirements for such business relationships under HIPAA.

NOW THEREFORE, for and in consideration of these premises, the Parties' other mutual covenants contained herein, and other good and valuable consideration, the receipt and adequacy of which are forever acknowledged and confessed, the Parties hereto acknowledge, covenant, and agree as follows:

1. Obligations of Business Associate

1.1. Permitted Uses and Disclosures of PHI. Business Associate shall use and disclose any PHI it may receive from Covered Entity only to perform the Services under the Service Agreement and carry out the obligations of Business Associate under the BA Agreement, and in accordance with applicable federal and state laws, including but not limited to HIPAA.

Business Associate will only use or disclose the minimum necessary PHI and will abide by Covered Entity's policies and procedures relative to minimum use. Business Associate may not use or disclose PHI in a manner that would violate HIPAA if done by Covered Entity, except as specifically set forth herein. Business Associate may also use or disclose PHI for the proper management and administration of the Business Associate, for data aggregation services related to the health care operations of Covered Entity, or to carry out its legal responsibilities, but only to the extent any such disclosure is required by law or if (i) the Business Associate obtains reasonable assurances from the person or entity to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed, and (ii) the person or entity agrees to notify the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached. To the extent Business Associate is to carry out any obligation of Covered Entity under Subpart E of 45 CFR Part 164, Business Associate shall comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligation. Business Associate shall not use or further disclose PHI other than permitted or required by this BA Agreement or as otherwise required by law.

1.2 Safeguards. Business Associate shall implement and use appropriate administrative, physical and technical safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI and prevent the use or disclosure of PHI other than as set forth in this BA Agreement or as permitted or required by law. Business Associate shall communicate important security changes associated with the Services to Covered Entity in a commercially reasonable timeframe.

1.3 Reporting Disclosures of PHI. In the event Business Associate, its agents, employees or contractors use or disclose PHI in violation of this BA Agreement, Business Associate shall report such use or disclosure to Covered Entity as soon as Business Associate becomes aware of such violation, including the circumstances surrounding the use or disclosure and a description of the PHI inappropriately used or disclosed. In compliance with 45 CFR 164.410, Business Associate shall report to Covered Entity any security incident of which it becomes aware, provided that Business Associate shall only be required to notify Covered Entity of unsuccessful security incidents upon request. Business Associate agrees to notify Covered Entity in the event of any breach of unsecured PHI held by or under the control of Business Associate, including the identity of the affected individual(s) and all other relevant information, within three (3) business days of becoming aware of such breach. Unless the context of the relationship specifically requires otherwise, the parties disclaim any agency relationship between Covered Entity and Business Associate.

1.4 Mitigation of Harmful Effects. Business Associate shall establish procedures for mitigating harmful effects of any improper use or disclosure of PHI that Business Associate reports to Covered Entity.

1.5 Third Party Agreements. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), Business Associate shall require all of its subcontractors and agents that create, receive, maintain, transmit, use or have access to PHI under this BA Agreement to agree in

writing to adhere to the same or substantially similar restrictions, conditions and requirements applicable to the use or disclosure of such PHI as required herein.

1.6 Access to Information. Within ten (10) business days of a request by Covered Entity for access to PHI about an individual contained in a Designated Record Set (as defined in 45 CFR 164.501) in Business Associate's possession, Business Associate shall make available to Covered Entity such PHI for so long as such information is maintained in the Designated Record Set by Business Associate. In the event any individual requests access to his or her own PHI directly from Business Associate, Business Associate shall forward such request to Covered Entity upon receipt of same. Business Associate shall reasonably cooperate with Covered Entity to provide an individual, at Covered Entity's written direction, with access to the individual's PHI in Business Associate's possession within ten (10) business days of Business Associate's receipt of written instructions for same from Covered Entity. Any denials of access to PHI requested shall be the responsibility of Covered Entity.

1.7 Amendment of PHI. Business Associate agrees to make PHI in a Designated Record Set available for amendment and to incorporate any appropriate amendments at the direction of and in the time and manner designated by Covered Entity. Business Associate further agrees to forward to Covered Entity any request for amendment of PHI made directly by an individual to Business Associate upon receipt of such request, and take no action on such request until directed by Covered Entity.

1.8 Accounting of Disclosures. Business Associate agrees to document disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528 and to provide Covered Entity with an accounting of such disclosures in the time and manner designated by Covered Entity. Business Associate further agrees to forward to Covered Entity any request for an accounting of disclosures of PHI made directly by an individual to Business Associate upon receipt of such request. To the extent Business Associate maintains PHI in an electronic health record, Business Associate agrees to account for all disclosures of such PHI upon the request of an individual for a period of at least three (3) years prior to such request (but no earlier than the effective date of this BA Agreement), as required by HITECH; such accounting shall be directly to the individual if requested by Covered Entity.

1.9 Access to Books and Records. Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of the Department of Health and Human Services for purposes of determining compliance with the requirements of HIPAA.

1.10 Additional Security and Data Breach Obligations under the Regulations. Business Associate acknowledges that it is subject to the security and data breach provisions of HIPAA and agrees to abide thereby. Business Associate also agrees to abide by all of the privacy provisions set forth in Title XIII, Subtitle D of ARRA, including without limitation restrictions on marketing and sales of PHI and requirements relating to limited data sets and minimum necessary disclosures. Business Associate shall ensure that any subcontractors and agents engaged to fulfill the Services are bound by terms and conditions substantially similar to those

in this BA Agreement. Additionally, Business Associate shall ensure that such subcontractors and agents comply with the Regulations.

2. Obligations of Covered Entity

2.1 Notice of Privacy Practices. Covered Entity agrees to provide Business Associate with a copy of Covered Entity's "Notice of Privacy Practices," required to be provided to individuals in accordance with 45 CFR 164.520, as well as any subsequent changes to such notice.

2.2 Changes to or Restrictions on Use or Disclosure of PHI. Covered Entity will provide Business Associate with Covered Entity's changes to, or revocation of, permission to use or disclose PHI if such changes affect Business Associate's permitted or required uses or disclosures. Covered Entity will further notify Business Associate of any restriction to the use or disclosure of PHI agreed to by Covered Entity in accordance with the provisions of 45 CFR 164.522, and any restriction requested by an individual which Covered Entity is required to comply with in accordance with the provisions of HITECH.

2.3 Requested Uses or Disclosures of PHI. Covered Entity shall not request Business Associate to use or disclose PHI in any manner inconsistent with state or federal law.

3. Term and Termination

3.1 Term. This BA Agreement shall be deemed effective on the Effective Date and shall continue in effect until all obligations of the Parties have been met, unless otherwise terminated under the terms and conditions set forth herein.

3.2 Termination for Cause. Upon Covered Entity's knowledge of a material breach of this BA Agreement by Business Associate, its agents or subcontractors, this BA Agreement and the Services Agreement may be immediately terminated by Covered Entity, as provided under 45 CFR 164.504(e)(2)(iii). At its option, Covered Entity may choose to (i) provide Business Associate with written notice of the existence of a material breach of this BA Agreement; and (ii) permit Business Associate to cure the material breach within a reasonable timeframe, upon mutually agreeable terms. In the event Business Associate is afforded an opportunity and fails to cure the breach in accordance with such mutually agreeable terms, this BA Agreement and the Services Agreement may be immediately terminated at the option of Covered Entity. In the event Covered Entity violates its obligations under HIPAA in a manner related to this BA Agreement, Business Associate shall provide Covered Entity with notice of such breach; if Covered Entity does not cure such breach within a reasonable period of time, Business Associate may terminate this BA Agreement.

3.3 Effect of Termination and Obligations of Business Associate Upon Termination. Upon termination of this BA Agreement, Business Associate shall return or, if approved by Covered Entity, destroy all PHI created or received by Business Associate, its agents and subcontractors to the extent feasible, without retaining any copies of such PHI. If Business Associate and Covered Entity mutually agree that return or destruction of the PHI is not reasonably feasible, Business Associate agrees to extend the protections of PHI under this BA

Agreement and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible.

The obligations of Business Associate under this paragraph shall survive the termination of this BA Agreement.

4. Miscellaneous Provisions

4.1 Definitions and Interpretation; Indemnification. All words used herein but not defined herein shall have the meanings set out in HIPAA, and this BA Agreement shall be interpreted in such a fashion as to cause the parties to be in compliance with HIPAA. Notwithstanding any other provision of the BA Agreement, to the extent permitted by applicable law, Covered Entity and Business Associate agree to indemnify, defend and hold harmless each other and each other's respective employees, directors, officers, subcontractors, agents or other members of its workforce, each of the foregoing hereinafter referred to as an "Indemnified Party," against all actual and direct losses suffered by the Indemnified Party and all liability to third parties arising from or in connection with any breach of this BA Agreement or of any warranty hereunder or from any negligence or wrongful acts or omissions, including failure to perform its obligations under HIPAA, by the indemnifying party (the "Indemnifying Party") or its employees, directors, officers, subcontractors, agents or other members of its workforce. Accordingly, to the extent permitted by applicable law, the Indemnifying Party shall reimburse any Indemnified Party for any and all actual and direct losses, liabilities, lost profits, fines, penalties, costs or expenses (including reasonable attorneys' fees) which may for any reason be imposed upon any Indemnified Party by reason of any suit, claim, action, proceeding or demand by any third party which results from the Indemnifying Party's breach hereunder. The provisions of this paragraph shall survive the expiration or termination of this BA Agreement for any reason.

4.2 Assignment. Neither party shall have the right to assign its rights or obligations under this BA Agreement without the prior written consent of the other party, and any such attempted assignment shall be void.

4.3 Amendment. This BA Agreement shall not be modified or amended except as specifically described in this section, or by a written document executed by each of the parties to this BA Agreement, and such written modification or amendment shall be attached hereto. The Parties acknowledge and agree that any future amendments to the Regulations affecting Business Associate agreements are hereby incorporated by reference into this BA Agreement as if set forth in this BA Agreement in their entirety, effective on the later of the effective date of this BA Agreement or such subsequent date as may be specified by such Regulations.

4.4 Waiver of Provisions. Any waiver of any terms and conditions of this BA Agreement must be in writing, and signed by both Business Associate and Covered Entity. The waiver of any of the terms and conditions of this BA Agreement shall not be construed as a waiver of any other terms and conditions of the BA Agreement.

4.5 Parties In Interest; No Third-Party Beneficiaries. Except as otherwise provided in this BA Agreement, the terms and conditions of this BA Agreement shall inure to the benefit of and be binding upon the respective heirs, legal representatives, successors and permitted assigns of the parties to this BA Agreement. Neither this BA Agreement nor any other agreement contemplated in this BA Agreement shall be deemed to confer upon any person not a party to this BA Agreement any rights or remedies contained in this BA Agreement.

4.6 Governing Law. This BA Agreement, the rights and obligations of the parties hereto, and the entire relationship between the parties relating hereto shall be governed by and construed and enforced in accordance with the substantive laws of the state of Texas and with HIPAA.

4.7 Notice. Whenever this BA Agreement requires or permits any notice, request, or demand from one party to another, the notice, request, or demand must be in writing to be effective and shall be deemed to be delivered and received (i) if delivered by overnight or courier service, when actually received by the party to whom notice is sent or (ii) if delivered by mail (whether actually received or not), at the close of business on the third business day next following the day when placed in the mail, postage prepaid, certified or registered, addressed to the appropriate party, at the address of such party set forth below (or at such other address as such party may designate by written notice to all other parties in accordance herewith):

If to Covered Entity: ***[insert name of TWU Covered Entity]***

Attn: Privacy Officer

[Address of TWU Covered Entity]

If to Business Associate: _____

_____

_____

_____

4.8 Authorization. The Parties executing this BA Agreement hereby warrant that they have the authority to execute this BA Agreement and that their execution of this BA Agreement does not violate any bylaws, rules, or regulations applicable to them.

4.9 Counterparts. This BA Agreement may be executed in multiple counterparts, each of which shall be deemed an original, and all of which together shall constitute one and the same instrument.

[*Signature page follows*]

IN WITNESS WHEREOF, the Parties hereto have executed this BA Agreement as of the date first written above.

[Insert name of Business Associate]

By: _____
Its: _____
Date: _____

[Insert name of Covered Entity]

By: _____
Its: _____
Date: _____

Exhibit 2 – Sample Authorization Form

(Attached)

Sample Authorization to Use or Disclose Protected Health Information – Documents to be Reviewed and Customized Prior to Use

AUTHORIZATION TO USE OR DISCLOSE PROTECTED HEALTH INFORMATION

This authorization may be used to permit a covered entity (as such term is defined by HIPAA and applicable Texas law) to use or disclose an individual's protected health information. Individuals completing this form should read the form in its entirety before signing and complete all the sections that apply to their decisions relating to the use or disclosure of their protected health information.

Information regarding patient for whom authorization is made:

Full Name: _____

Other Name(s) Used: _____ Date of Birth: _____

Address: _____ City: _____ State: _____ Zip Code: _____

Phone: (____) _____ Email *(Optional)*: _____

Information regarding health care provider or health care entity authorized to disclose this information:

Name: _____

Address: _____ City: _____ State: _____ Zip Code: _____

Phone: (____) _____ Fax: (____) _____

Information regarding person or entity who can receive and use this information:

Name: _____

Address: _____ City: _____ State: ____ Zip Code: ____

Phone: (___) _____ Fax: (___) _____

Specific information to be disclosed

Medical Record from (insert date) _____ to (insert date) _____

Entire Medical Record, including patient histories, office notes (except psychotherapy notes, test results, radiology studies, films, referrals, consults, billing records, insurance records, and records received from other health care providers.

Other:

Include: ***(Indicate by Initialing)***	**Reason for release of information**
	(Choose all that Apply)
_____ Drug, Alcohol or Substance Abuse Records Mental Health Records (Except Psychotherapy Notes)	Treatment/Continuing Medical Care
_____ HIV/AIDS-Related Information (Including HIV/AIDS Test Results)	Personal Use
	Billing or Claims
_____ Genetic Information (Including Genetic Test Results)	Insurance
	Legal Purposes
	Disability Determination
	School
	Employment
	Other *(Specify)*: _____

The individual signing this form agrees and acknowledges as follows:

(i) **Voluntary Authorization**: This authorization is voluntary. Treatment, payment, enrollment or eligibility for benefits (as applicable) will not be conditioned upon my signing of this authorization form.

(ii) **Effective Time Period**: This authorization shall be in effect until the earlier of two (2) years after the death of the patient for whom this authorization is made or the following specified date: Month: _____ Day: _____ Year: _____.

(iii) **Right to Revoke**: I understand that I have the right to revoke this authorization at any time by writing to the health care provider or health care entity listed above. I understand that I may revoke this authorization except to the extent that action has already been taken based on this authorization.

(iv) **Special Information**: This authorization may include disclosure of information relating to **DRUG, ALCOHOL** and **SUBSTANCE ABUSE, MENTAL HEALTH INFORMATION**, except psychotherapy notes, **CONFIDENTIAL HIV/AIDS-RELATED INFORMATION**, and GENETIC INFORMATION only if I place my initials on the appropriate lines above. In the event the health information described above includes any of these types of information, and I initial the corresponding lines in the box above, I specifically authorize release of such information to the person or entity indicated herein.

(v) **Signature Authorization**: I have read this form and agree to the uses and disclosure of the information as described. I understand that refusing to sign this form does not stop disclosure of health information that has occurred prior to revocation or that is otherwise permitted by law without my specific authorization or permission. I understand that information disclosed pursuant to this authorization may be subject to re-disclosure by the recipient and may no longer be protected by federal or state privacy laws.

SIGNATURES:

Patient/Legal Representative:_____Date:_____

If Legal Representative, relationship to Patient: _____

Witness (optional):_____Date_____

A minor individual's signature is required for the release of certain types of information, including for example, the release of information related to certain types of reproductive

care, sexually transmitted diseases, and drug, alcohol or substance abuse, and mental health treatment.

Signature of Minor (if applicable): _____Date: _____

Exhibit 3 – Sample Notice of Privacy

(Attached)

Exhibit 4 – Sample HIPAA Security Incident Log Form

(Attached)

Sample HIPAA Security Incident Log Form – Documents to be Reviewed and Customized Prior to Use

[NAME OF PRACTICE]'S
HIPAA SECURITY INCIDENT LOG FORM

GENERAL INFORMATION:

Name and Title of Individual Reporting Incident: _____

Date and Time Incident Reported: _____

Name and Title of Individual Who Received Incident Report: _____

INFORMATION REGARDING INCIDENT:

Date and Time of Incident: _____

Place of Incident: _____

Date and Time of Incident Discovery: _____

Description of Investigation Completed *(Describe persons interviewed, records reviewed, etc.)*:

_____
_____
_____
_____
_____

Description of Findings Regarding Incident *(Describe cause of incident, protected health information involved, etc.):*

_____
_____
_____
_____
_____

Description of Practice's Response *(Describe steps taken to mitigate harm, notification given, agencies (e.g., police, FBI, HHS) contacted, action taken to prevent future security incidents, etc.):*

_____

_____

_____

_____

_____

Signature of Security Officer:_____ Date: _____

Exhibit 5 – Sample HIPAA Privacy Breach and Notification Assessment

(Attached)

Sample HIPAA Privacy Breach Risk and Notification Assessment – Documents to be Reviewed and Customized Prior to Use

[Name of Practice]

HIPAA PRIVACY BREACH
RISK AND NOTIFICATION ASSESSMENT

Date Reported		**Patient Name / Number**	
Date Occurred		**State**	

This Risk and Notification Assessment is used to evaluate and answer the following questions:

- ☐ Does the breach require notification as it poses more than a low probability that the data has been compromised?
- ☐ Does the breach meet one of the four notification exceptions?
- ☐ Does the breach require notification under state notification requirements?
- ☐ Does the breach require notification to the Secretary of HHS?
- ☐ Does the breach require notification to local media outlets?

LOW PROBABILITY OF COMPROMISE:

Use the following risk assessment factors in determining notification requirements based on the **low probability of compromise standard** to determine whether the breach poses more than "a low probability that the protected health information has been compromised based on a risk assessment" involving the below four factors. Assess each risk factor using a "Low, Medium or High" risk assessment factor and provide supporting facts specific to the incident.

Risk Factor	Risk Assessment	Facts Specific to this Incident
Nature of the Data Element Breached Analyze the nature of the data elements compromised. ☐ Patient names associated with certain financial, demographic or diagnostic information pose a higher probability of compromise than information	[Select Low, Medium or High]	[List specific facts and information]

Risk Factor	Risk Assessment	Facts Specific to this Incident
not associated with a patient name. ☐ The nature of the information disclosed poses a risk of identity theft (e.g. SSN or financial information in combination with patient name).		
Identity of the Person(s) to Whom the Information was Disclosed Analyze the identity of the unauthorized individuals accessing the data. ☐ Was the information disclosed to a physician or other covered entity? ☐ Was the information returned, deleted or destroyed by the recipient? ☐ Was the recipient a party to a lawsuit or someone otherwise likely to retain or use the data?	[Select Low, Medium or High]	[List specific facts and information]
Likelihood the Information was Actually Acquired or Viewed Consider whether the data was on a password-protected device or otherwise unlikely to be acquired or viewed, versus whether the data was acquired by a hacker, for example. ☐ The PHI was returned or the device found prior to it being accessed for an improper purpose. ☐ The unauthorized individual(s) receiving the information certify that they did not view the information.	[Select Low, Medium or High]	[List specific facts and information]

Risk Factor	Risk Assessment	Facts Specific to this Incident
Ability of the Entity to Mitigate the Risk to the Information Consider appropriate breach prevention, monitoring and mitigation measures that can be taken in response to the breach. ☐ Immediate steps were taken to confirm and ensure the recipient of the impermissible disclosure destroyed or returned the information it received.	[Select Low, Medium or High]	[List specific facts and information]

CONCLUSION: Based on this risk assessment, the impermissible use or disclosure of unsecured PHI:

☐ **Does not** pose a more than a low risk of compromise.

☐ **Does** pose more than a low risk of compromise.

NOTIFICATION EXCEPTIONS:

In addition to the low probability of compromise standard, HHS created **four (4) notification exceptions** to the breach notification standards. If any of the following four exceptions are met, notification of the breach is not required. Assess each exception using a "Yes/No" assessment factor and provide supporting facts specific to the incident.

Exception to Notification Requirements	(Yes/No) Meets Exception	Facts Specific to this Incident
Practically De-Identified Information Disclosure of Health Information that does not include the 18 specific identifiers listed in the HIPAA Privacy Standards.[6]		

[6] The list of 18 specific identifiers in Section 164.514 of the HIPAA Privacy Standards includes: names; geographic subdivisions smaller than a state; all elements of dates (except year) for dates directly related to an individual (e.g., date of birth, admission, discharge, death); telephone numbers; fax numbers; email addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers (serial or license plate numbers); device identifiers and serial numbers; web universal resource locators (URLs); internet protocol (IP) address numbers; biometric identifiers (finger and voice prints); full face photographic images and any comparable

Exception to Notification Requirements	(Yes/No) Meets Exception	Facts Specific to this Incident
Certain Unintentional Uses Unintentional use, access or acquisition of PHI by a workforce member or individual acting under the authority of a covered entity or business associate, if made in good faith, within the scope of authority and does not result in further use or disclosure.		
Certain Inadvertent Disclosures Inadvertent disclosure of PHI by a person who is authorized to access PHI at the covered entity or business associate if the recipient is authorized to access PHI at the same covered entity or business associate or organized health care arrangement, and the disclosed PHI is not further used or disclosed.		
Incidents Involving No Ability to Retain PHI Covered entity or business associate has a good faith belief that the recipient was not reasonably able to retain the PHI.		

CONCLUSION: Based on this risk assessment, the impermissible use or disclosure of unsecured PHI:

☐ **Does not** meet at least one of the four (4) notification exceptions.

☐ **Does** meet at least one of the four (4) notification exceptions.

STATE LAW

images; and any other unique identifying number, characteristic, or code, except as permitted by Section 164.514(c).

Texas has enacted security breach notification laws that are more stringent than the federal breach notification rules. Each incident should be investigated to ensure that, although it does not required notification under federal law, notification is not required under Texas law.

General Notification Requirement:

Texas law requires a person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information to disclose any breach of system security, after discovering or receiving notification of the breach, to any individual (who is a resident of Texas or another state that does not require notification of a breach of security system) whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Please see Texas Bus. & Comm. Code § 521.001, *et seq*.

CONCLUSION: Based on review of the applicable Texas security breach notification laws, the impermissible use or disclosure of unsecured PHI:

☐ **Does not** require disclosure under state law.

☐ **Does** require disclosure under state law (complete in the box below the state reporting requirement).

OTHER NOTIFICATION REQUIREMENTS:

In the case of a breach involving any **500 or more individuals**, the covered entity must notify the Secretary of HHS **at the same time** that individuals are notified.

CONCLUSION: Based on the number of patients involved, the impermissible use or disclosure of unsecured PHI:

☐ **Does not** require notification to the Secretary of the HHS.

☐ **Does** require notification to the Secretary of the HHS **simultaneous** with the patient notification.

☐ **Does** require notification to the Secretary of the HHS within 60 days after the end of the calendar year.

In the case of a breach involving any 500 or more residents of any state or jurisdiction, the covered entity must notify prominent media outlets of that state or jurisdiction within 60 days of the date of discovery of the breach. Each incident should be evaluated against this requirement:

☐ **Does not** require notification of prominent media outlets in the state or jurisdiction.

☐ **Does** require notification of prominent media outlets in the state or jurisdiction.

NOTIFICATION SUMMARY

Yes	No	
		Notification required under federal law
		Notification required under state law
		Notification required to Secretary of HHS
		Notification required to prominent media outlets

Chief Privacy Officer _____ Date _____

Exhibit 6 – Sample Notification Letter to Practice Patients

(Attached)

Sample Notification Letter to Practice Patients – Documents to be Reviewed and Customized Prior to Use

[Date]

[Name here]
[Address 1 Here]
[Address 2 Here]
[City, State, Zip Code]

Dear [_____ Patient Name]:

I am writing to you with important information about a recent breach of your personal information from [_____] (the "Practice"). We became aware of this breach on [Insert Date] which occurred on or about [Insert Date]. The breach occurred as follows: [Describe event and include the following information:

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

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

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

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

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

We also advise you to immediately take the following steps:

☐ Call the toll-free numbers of anyone of the three major credit bureaus (below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge.

- **Equifax:** 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241.

- **Experian:** 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013.

- **TransUnion:** 1-800-680-7298; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

☐ Order your credit reports. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.

☐ Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information.

We take very seriously our role of safeguarding your personal information and using it in an appropriate manner. The Practice apologizes for the stress and worry this situation has caused you and is doing everything it can to rectify the situation.

We have established a toll-free number to call us with questions and concerns about the loss of your personal information. You may call [Insert Toll Free number] during normal business hours with any questions you have.

We have also established a section on our Web site with updated information and links to Web sites that offer information on what to do if your personal information has been compromised.

[Insert Closing Paragraph Based on Situation]

Sincerely,
[Insert Applicable Name/Contact Information]

Exhibit 7 – Sample Notification Letter to Secretary of Health & Human Services

(Attached)

Sample Notification Letter to Secretary of Health & Human Services – Documents to be Reviewed and Customized Prior to Use

[Date]

Secretary of Health & Human Services
The U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201
Telephone: 202-619-0257
Toll Free: 1-877-696-6775

Dear Secretary:

In compliance with the American Recovery and Reinvestment Act of 2009 (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH), we are notifying you of a recent breach of unsecured protected health information (PHI). The breach involved [Insert Number] patients of [Practice Name]. We became aware of this breach on [Insert Date] which occurred on or about [Insert Date]. The breach occurred as follows:

Describe event and include the following information as communicated to the victims:

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

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

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

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

E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an email address, Web site, or postal address.

On behalf of [Insert Practice Name] I am communicating this information to you in compliance with ARRA/HITECH.

If you have any questions or require further information, please contact me at [Insert Contact Information].

Sincerely,

[Insert name]

Exhibit 8 – Sample Media Notification Statement/Release

(Attached)

Sample Media Notification Statement/Release – Documents to be Reviewed and Customized Prior to Use

[Date]

Contact: [Insert Contact Information Including Phone Number/E-Mail Address]

IMMEDIATE RELEASE
[_____] NOTIFIES PATIENTS OF BREACH OF UNSECURED PERSONAL INFORMATION

[_____] notified [Insert Number] patients of a breach of unsecured personal patient protected health information after discovering the following event:

Describe event and include the following information as communicated to the victims:

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

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

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

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

E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an email address, Web site, or postal address.

In conjunction with local law enforcement and security experts, [the Practice] is working to notify impacted patients to mitigate the damages of the breach. [The Practice] has in place safeguards to ensure the privacy and security of all patient health information. As a result of this breach, steps are underway to further improve the security of its operations and eliminate future risk.

In a notification to patients, [the Practice] has offered their resources as well as … [Insert as Applicable]. [The Practice] has also encouraged its patients to contact their financial institutions to prevent unauthorized access to personal accounts.

[The Practice] has trained staff available for patients to call with any questions related to the data breach. Patients may call [Insert Phone Number Here] from [Insert Hours] with

any questions. In addition, patients may visit [the Practice] Web site at [www._____] for further information.

> "[The Practice] understands the importance of safeguarding our patients' personal information and takes that responsibility very seriously," said [Insert Name], President and CEO. "We will do all we can to work with our patients whose personal information may have been compromised and help them work through the process. We regret that this incident has occurred, and we are committed to prevent future such occurrences. We appreciate our patients' support during this time.
>
> Please direct all questions to [Enter Contact Information].

Exhibit 9 – Initial Risk Analysis Worksheet

(Attached)

RISK ANALYSIS – OVERVIEW

Covered Entities (such as _____) and their Business Associates (each an "Entity" for purposes of this document) must conduct a Risk Analysis for HIPAA compliance (§ 164.308(a)(1)(ii)(A)). The risk analysis must be an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the electronic Protected Health Information ("EPHI") held by the Entity.

The Risk Analysis shall be conducted by an assessment team assembled by the Privacy Officer and Security Officer (which for smaller Entities, may be the same person), and shall include employees knowledgeable about the systems used by the Entity for storage, viewing, accessing, manipulating, and transmitting EPHI, including hardware, software, and Entity capabilities (both technical and financial).

The assessment team shall use the following to categorize and analyze risks and vulnerabilities of the Entity outlined above relative to each system. The assessment team shall score the risks and vulnerabilities associated with each system component, and shall address those items with the highest risk first.

The assessment team shall meet as often as the Privacy Officer deems necessary to review the Risk Assessment for current applicability, revise as necessary, re-review systems that have been added, identify new risks and vulnerabilities, and take any other action as may be necessary to ensure the confidentiality, integrity and availability of EPHI held by the Entity.

IMPORTANT ELEMENTS TO UNDERSTAND

To better understand risk analysis and risk management processes, Entities should be familiar with several important terms, including "vulnerability," "threat," and "risk". These are not actually defined in the Security Rule itself, but CMS uses these common industry terms in discussing risk analysis and risk management.

VULNERABILITY – Defined in NIST SP 800-30 as "[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy." Vulnerabilities, whether accidentally triggered or intentionally exploited, could potentially result in a security incident, such as inappropriate use or disclosure of EPHI. Vulnerabilities may be grouped as technical and non-technical.

THREAT – An adapted definition, from NIST SP 800-30 is "[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability/" There are several types of threats that may occur within an information system or operating environment. These include: (1) Natural threats – floods, earthquakes, tornadoes; (2) Human threats – enabled or caused by humans and may include intentional (e.g. network

and computer based attacks, malicious software upload, and unauthorized access to EPHI) or unintentional (e.g. inadvertent data entry or deletion) actions.

RISK – this definition is clearer once threat and vulnerability are defined. An adapted definition of risk from NIST SP 800-30, is: "The net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur. ****Remember: a threat must have the capability to trigger or exploit a vulnerability to create risk.***** Risks arise from legal liability or mission loss due to – (a) unauthorized disclosure, modification or destruction of information, (b) unintentional errors and omissions, (c) IT disruptions due to natural and man-made disasters, and (d) failure to exercise due care and diligence in the implementation and operation of the IT system. Risk is a function of (1) the likelihood of a given threat triggering or exploiting a particular vulnerability, and (2) the resulting impact on the organization. This means that risk is not a single factor or event, but rather a combination of factors or events that, if they occur, may have an adverse impact on the Entity.

RISK ANALYSIS AND RISK MANAGEMENT STEPS

Check-The-Box -- Risk Analysis Steps for Entities:

[_____] 1. Assemble the assessment team. The Privacy Officer and Security Officer (which may be the same person) must assemble an assessment team, which team shall include the Privacy Officer, the Security Officer, and other employees knowledgeable about the systems used by the Entity for storage, viewing, accessing, manipulating, and transmitting EPHI, including hardware, software, and Entity capabilities (both technical and financial). The size and makeup of the team will depend on the size and complexity of the Entity. It should include employees engaged in general management, clinical operations, IT, physical operations, human resources, medical records, procurement, and any other activities directly related to or having a direct impact on the confidentiality, integrity, and availability of the EPHI held by the Entity.

[_____] 2. Identify the scope of analysis. The risk analysis scope that the Security Rule requires is the potential risks and vulnerabilities to the confidentiality, availability and integrity of all EPHI that an Entity creates, receives, maintains or transmits. This includes all EPHI in all forms of electronic media. (Examples of such media include hard drives, floppy disks, CDs, DVDs, Smart Cards, PDAs, transmission media, and thumb drives and all other external storage drives.)

[_____] 3. Gather data. (Gather relevant data of EPHI.) An Entity must identify where the EPHI is stored, received, maintained or transmitted. An Entity could gather relevant data by reviewing past and/or existing projects; performing interviews; distributing questionnaires; reviewing documentation; or using other data gathering techniques. The data on EPHI gathered using these methods MUST be documented.

[_____] 4. Identify and document potential threats and vulnerabilities. Entities must identify and document reasonably anticipated threats to EPHI. To start, Entities may compile a categorized list of threats, giving consideration to all potential threats that could cause harm to the system and its processing environment. After the list is compiled, the Entity should reduce the list to only those reasonably anticipated threats. For most entities, human threats will be of the greatest concern, because human threats have the potential to be triggered or exploited more frequently than natural or environmental threats. When identifying potential threats, Entities must also identify and document vulnerabilities, which, if triggered or exploited by a threat, would create a risk to EPHI. The Entity should create a list of vulnerabilities, both technical and non-technical, associated with existing information systems and operations that involve EPHI. Sources of information to identify non-technical vulnerabilities may include previous risk analysis documentation, audit reports, or security review reports. Sources of information to identify technical vulnerabilities may include assessments of information systems, information system security testing, or publicly available vulnerability lists and advisories.

[_____] 5. Assess current security measures. The goal of this step is to analyze current security measures implemented to minimize or eliminate the likelihood that a threat will trigger or exploit a system vulnerability. For example, a vulnerability is not likely to be triggered or exploited by a threat if effective security measures are implemented. Security measures can be both technical and non-technical. Technical measures are part of information systems hardware and software. Examples of technical measures include access controls, identification, authentication, encryption methods, intrusion detection software, automatic logoff and audit controls. Non-technical measures are management and operational controls such as policies, procedures, standards, guidelines, accountability and responsibility, and physical and environmental security measures. Security measures can also be both preventive and detective. Preventive measures inhibit attempts to violate security policy and include such measures as access control enforcement, encryption, and authentication. Detective measures warn of violations or attempted violations of security policy and include such controls as audit trails and intrusion detection methods. The output of this step should be documentation of the security measures an Entity uses to safeguard EPHI. The output should identify whether security measures required by the Security Rule are already in place. The documentation should also identify if current security measures are configured and used properly.

[_____] 6. Determine the likelihood of threat occurrence. Once the first five steps are complete, the Entity has the information needed to determine the likelihood that a threat will trigger or exploit a specific vulnerability and the resulting impact to the Entity. “Likelihood of occurrence” is the probability that a threat will trigger or exploit a specific vulnerability. Entities should consider each potential threat and vulnerability combination and rate them by likelihood (or probability) that the combination would occur. Such ratings such as high, medium and low or numeric representations of probability may be used to represent likelihood of occurrence. The ratings used will depend on the Entity’s approach. For example, an Entity may choose to rate risks as high, moderate and low (as per chart below). The following is instructive:

- High Likelihood – a high probability exists that a threat will trigger or exploit one or more vulnerabilities. This might be due to the existence of multiple organizational deficiencies, such as absence, inadequacy or improper configuration of security controls, or due to geographic location (such as within a flood zone).

- Medium or Moderate Likelihood – a moderate probability exists that at threat will trigger or exploit one or more vulnerabilities due to the existence of a single organizational deficiency, such as the lack of security measures.
- Low Likelihood – a low probability exists that a threat will trigger or exploit a single vulnerability due to the existence of a single organizational deficiency, such as improper configuration of security controls.

The output of this step should be documentation of all threat and vulnerability combinations with associated likelihood ratings that may impact the confidentiality, availability and integrity of EPHI of an Entity.

[_____] 7. Determine the potential impact of threat occurrence. If a threat triggers or exploits a specific vulnerability, there may be potential outcomes. For Entities, the most common outcomes include, but are not limited to:

- Unauthorized access to or disclosure of EPHI
- Permanent loss or corruption of EPHI
- Temporary loss or unavailability of EPHI
- Loss of financial cash flow
- Loss of physical assets.

All of these outcomes have the potential to affect the confidentiality, availability and integrity of EPHI. Measuring the impact of a threat occurring in an Entity can be performed using different methods. The most common methods are qualitative and quantitative. Both of these methods allow an Entity to measure risk. The Qualitative Method rates the magnitude of the potential impact resulting from a threat triggering or exploiting a vulnerability on a scale such a high, medium and low. The Quantitative Method measures the tangible potential impact of a threat triggering or exploiting a specific vulnerability, using a numeric value associated with the resource costs. This might include resource costs, such a repair costs to information systems or the replacement cost for an asset that is lost or stolen. This method provides valuable information for a cost-benefit analysis associated with risks. An entity may use either method or a combination of these two methods to measure impact on the organization. The output of this step should be documentation of all potential impacts and rating associated with the occurrence of threats triggering or exploiting vulnerabilities that affect confidentiality, availability, and integrity of EPHI within an Entity.

[_____] 8. Determine the level of risk. Entities should determine the level of risk to EPHI. The level of risk is determine by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk level determination may be performed by assigning risk level based on the average of the

assigned likelihood and impact levels. A risk level matrix can be used to assist in determining risk levels. A risk level matrix is created using values for likelihood of threat occurrence and resulting impact of threat occurrence. One output of this step should be documented risk levels for all threat and vulnerability combinations identified during risk analysis. Another output should be a list of corrective actions to be performed to mitigate each risk level.

[_____] 9. Identify security measures and finalize documentation. Once risk is identified and assigned a risk level, the Entity should begin to identify the actions required to manage the risk. The purpose of this step is to begin identifying security measures that can be used to reduce risk to a reasonable and appropriate level. Any potential security measures that can be used to reduce risks to EPHI should be included in documentation. The Security Rule requires the risk analysis be documented but does not require a specific format. A risk analysis report could be created to document the risk analysis process, output of each step and initial identification of security measures. The risk analysis documentation is a direct input to the risk management process to be used by management to make decisions on policy and procedural, budgetary, and system operational and management changes.

[_____] 10. Analyze non-electronic PHI for similar risks. Identify areas where non-electronic PHI is stored, used, or transmitted by the Entity. Paper record storage and use, fax transmission, and mailed hard-copy documents are likely areas where the Entity will use, maintain, store or transmit non-electronic PHI. Conduct the same type of analysis as discussed in steps 2-9 above, and add non-electronic PHI risk areas and security measures to the documentation.

[_____] 11. Continue assessing risks; repeat risk assessment. Conduct the same type of analysis as discussed in steps 2-9 above on a formal, regular basis, as well as whenever specific incidents, changes in technology or operations, or changes in personnel occur within the Entity. This means repeating these risk analysis steps as needed to address risks associated with new technologies and/or business operations.

Risk Management Steps for Entities Are:

[_____] 1. Develop and implement a risk management plan -- The first step in the risk management process should be to develop and implement a risk management plan. The purpose of the plan is to provide structure for the Entity's evaluation, prioritization and implementation of risk-reducing security measures. For the plan to be successful, key members of the Entity's workforce, including senior management and other key decision makers, must be involved. The outputs of the risk analysis process will provide these key workforce members with the information needed to make risk prioritization and mitigation decisions. The risk prioritization and mitigation decisions will be determined by answering questions such as:

- Should certain risks be addressed immediately or in the future?
- Which security measures should be implemented.

An important component of the risk management plan is the plan for implementation of the selected security measures. The implementation component of the plan should address:

- Risks (threat and vulnerability combinations) being addressed;
- Security measures selected to reduce the risks;
- Implementation project priorities, such as: required resources; assigned responsibilities; start and completion dates; and maintenance requirements.

The output of this step is a risk management plan that contains prioritized risks to the Entity, options for mitigation of those risks, and a plan for implementation. The plan will guide the Entity's actual implementation of security measures to reduce risks to EPHI to reasonable and appropriate levels.

[_____] 2. Implement security measures. Once the risk management plan is developed, the Entity must begin implementation. This step will focus on the actual implementation of security measures (both technical and non-technical) within the Entity.

[_____] 3. Evaluate and maintain security measures. Risk analysis and risk management are not one-time activities, but they are on-going, dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The final step in the process is to continue evaluating and monitoring the risk mitigation measures implemented. The Security Rule does not specify how frequently to perform risk analysis and risk management. The frequency of performance will vary among Entities.

RISK ANALYSIS

CATEGORY: _____
SYSTEM NAME: _____

IDENTIFIED THREATS	IDENTIFIED VULNERABILITIES	PROBABILITY SCORE[7]	EPHI SCORE[8]	ENTITY SCORE[9]	SUM OF SCORES	POTENTIAL SOLUTIONS	ACTION TAKEN

[7] **Low (1-3)** = EPHI not sensitive, not likely to be targeted, or system is protected by security adequate security measures; **Moderate (4-6)** = EPHI is moderately sensitive, may be targeted, or the system remains vulnerable though some controls are in place; **High (7-9)** = Highly sensitive EPHI, hot target, or limited or ineffective controls in place.

[8] **Low (1-3)** = Breach not likely to have significant impact on confidentiality, integrity or availability of EPHI; **Moderate (4-6)** = Breach may cause moderate impact on confidentiality, integrity or availability of EPHI; **High (7-9)** = Breach likely to significantly impact confidentiality, integrity or availability of EPHI.

[9] **Low (1-3)** = Breach unlikely to cause significant harm to patients or customers, or to operations or reputation of the Entity; **Moderate (4-6)** = Breach may cause moderate harm to patients or customers, or to operations or reputation of Entity; **High (7-9)** = Breach likely to cause significant harm to patients or customers, or to operations or reputation of Entity.