HIPAA AND MEDICAL PRIVACY: Guidelines for Faculty, Staff and Students Relating to Protected Health Information

I. Introduction:

Pursuant to SAM 01.D.05, the duties of the General Counsel include, in part, issuing guidelines with regard to the use of protected health information. This document provides guidelines for the protection of the confidentiality of protected health information as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology Act of 1996 ("HITECH Act"), the Texas Medical Records Privacy Act, and related regulations. As provided by section 2.5 of SAM 01.D.05, it is the responsibility of each component university of the University of Houston System (the "UHS" or "System"), and each member of their workforce, whether paid or unpaid, to adhere to these guidelines.

Each department of the System creating, using, receiving, maintaining, or transmitting protected health information whether for health care or business related services ("Health Care Component") must also create written procedures and forms to comply with these guidelines and to apply to the department's specific mission and operations. Each Applicable Department must also train its workforce, whether paid or unpaid, in the use of departmental procedures and forms.

II. Distinction between HIPAA and the Texas Medical Record Privacy Act

To determine how these guidelines impact you, it is necessary to understand the difference between HIPAA and the Texas Medical Record Privacy Act. HIPAA is a federal law limited to only certain types of entities (health care providers, insurers, healthcare clearinghouses, and their business associates) that transmit Protected Health Information in electronic form for specific types of transactions. The Texas Medical Records Privacy Act (Chapter 181 of the Texas Health and Safety Code) has a broader reach than HIPAA and is in many senses stricter.

Both laws utilize the same definition of **Protected Health Information ("PHI")**. For purposes of these guidelines, **Protected Health Information** is: Any written, verbal or electronic health information, including payment information, that: (1) can possibly identify the particular individual to which the information applies; and (2) is created or received by a health care provider, health plan, employer, or health care clearinghouse. PHI can include demographic information collected from an individual.

The distinction lies in the types of entities covered under each law ("**Covered Entity**").

A. HIPAA Covered Entity: HIPAA only applies to specific entities *that furnish or are paid for healthcare items or services*, particularly those using, receiving or transmitting information in *electronic* form relating to certain transactions relating to health care or payment for health care. The specific entities are:

- Individual or group health plans that provide or pay for cost of medical care (insurers)
- Health care clearinghouses (billing services)
- Health care providers conducting certain transactions in electronic form (practitioners)
- Business associates and their subcontractors (vendors providing a business function for us that involves disclosure of our PHI).

If your department constitutes one of those types of entities and transmits PHI in electronic form to conduct transactions involving those listed below, then your department constitutes a HIPAA Covered Entity. The types of transactions include:

- Claims
- Benefit eligibility
- Referral authorization
- Enrollment
- Claim status
- Healthcare and premium payments
- Coordination of benefits

HIPAA Covered Entities must also comply with the Texas Medical Records Privacy Act.

B. Covered Entity Under Texas Law

A Covered Entity under the Texas Medical Record Privacy Act is any individual or entity who, for business purposes or on a non-profit or pro bono basis, creates, receives, obtains, maintains, uses, stores or transmits Protected Health Information. These include but are not limited to a business associate, health care payor, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, or health care provider, or a person maintaining an Internet site. This definition has a much broader scope than HIPAA.

III. UHS as a HIPAA Hybrid Entity

UHS is a HIPAA covered entity whose business activities include both covered and non-covered functions. Accordingly, UHS has elected to consider itself a hybrid entity for HIPAA purposes and will designate its HIPAA covered health care components. UHS' designated health care components must comply with the HIPAA Privacy Rule and the HIPAA Security Rule, as well as the Texas Medical Records Privacy Act and other specific laws and rules governing their specific practices.

UHS's Privacy Officer and the UHS Office of General Counsel shall define UHS's health care components that constitute both HIPAA covered entities and those which constitute covered entities under Texas law. This list will be reviewed every two years and updated as needed.

IV. Definitions used in these Guidelines

1. Breach means the unauthorized acquisition, access, use, or disclosure of PHI, which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

2. Business Associate is a person or entity, other than a workforce member, that performs a function or service for a HIPAA covered entity involving its patients' or clients' Protected Health Information. A Business Associate may be a department within UHS or an unaffiliated third party.

3. Covered Entity. *See* Sections II(A) and II(B).

4. Health Care Component means a UHS department that is a HIPAA and/or Texas law Covered Entity regardless of whether it constitutes a health care provider or another department handling Protected Health Information.

5. Health care operations means any of the following activities to the extent the activities are related to providing health care:

   a. Conducting quality assessment and improvement activities;
   b. 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;
   c. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, or for reinsurance of risk relating to claims for health care;
   d. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
   e. 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
   f. Business management and general administrative activities:
   g. Management activities related to HIPAA compliance;
   h. Customer Service;
   i. Resolution of internal grievances; and
   j. Due Diligence.

6. HIPAA mean the Health Insurance Portability and Accountability Act of 1996, codified at 42 USC § 1320d and any current and future regulations promulgated under HIPAA, including but not limited to 45 CFR Parts 160 and 164.

7. HIPAA Privacy Rule. The "HIPAA Privacy Rule" establishes national standards to protect individuals' medical records and other protected health information. The HIPAA Privacy Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The HIPAA Privacy Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. The HIPAA Privacy Rule is located at 45 CFR Part 160 and Subparts A and E of Part 164.

8. HIPAA Security Rule. The HIPAA Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic Protected Health Information. The "HIPAA Security Rule" requires risk analysis and practices to secure HIPAA Covered entities' electronic systems, including mobile/portable devices and access and use of remote systems. The HIPAA Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164. UH IT Security should be contacted with questions or concerns relating to the HIPAA Security Rule.

9. Minimum Necessary Standard *means t*he least information reasonably necessary to accomplish the intended purpose of the use, disclosure, or request of PHI. It also means that only those ***authorized*** to use and disclose PHI of a specific patient are permitted to do so.

10. Payment means any activities undertaken either by a health plan or by a health care provider to obtain or provide reimbursement for the provision of health care. These activities include but are not limited to:

    a. Determining eligibility for and other matters relating to health benefit claims;
    b. Billing, claims management, collection activities, obtaining payment from insurance, and related health care data processing;
    c. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; and
    d. Utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services.

11. Protected Health Information (PHI) means any individually identifiable health information created or received by a health care provider, health plan, employer, or health care clearinghouse that is transmitted or maintained in oral, written, and/or electronic form. Key identifiers can include the name, address, social security number, phone number, photograph, zip code, treatment date, employer, names of spouse and children, and any other information that can potentially identify the subject such as rare conditions, unique characteristics, etc.

    Exceptions to PHI. The following health information records do not constitute PHI: (i) education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) records on a student who is eighteen years of age or older, made or maintained by a health care provider and which are made, maintained, or used only for treatment purposes only and not disclosed for other purposes[1]; (iii) employment records held by a covered entity in its role as employer; and (iv) individually identifiable health information regarding a person who has been deceased for more than 50 years. PHI is defined the same under both the federal and Texas health privacy statutes.

[1] 20 U.S.C. 1232g(a)(4)(B)(iv). This information would be protected under FERPA once it is released within the educational institution for other uses or purposes and appropriate authorization must be obtained unless use or disclosure of such information is otherwise permitted under FERPA.

12. Treatment. "Treatment" means the provision, coordination, or management of health care and 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 the referral of a patient for health care from one health care provider to another.

13. Workforce. "Workforce" means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

V. Responsibilities of Covered Entities Under Both Federal and Texas Law

A. Each applicable clinic or department must: (i) identify a Privacy Officer and Contact person (ii) develop and document necessary procedures, forms and training necessary to carry out the requirements of these guidelines; (iii) document authorizations, restrictions, complaints, training, inadvertent disclosures, and breaches; (iv) maintain documentation for at least 6 years or longer as applicable; (v) train all pertinent staff, faculty, students, volunteers, trainees, paid or unpaid, on HIPAA; and (vi) continually assess compliance practices.

B. Each applicable clinic or department must maintain the policies and procedures required by this policy in written or electronic form. Whenever a communication is required to be in writing, UHS 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, the health care components shall maintain a written or electronic record of such action, activity, or designation.

C. Privacy Officer and Contact: Each department handling Protected Health Information must designate an individual responsible for ensuring that your department is complying with these guidelines and applicable law and an individual responsible who may be contacted with questions and concerns. This may be one individual. The Privacy Officer shall**:**

1. document the department's policies/procedures used to protect PHI;
2. ensure training is conducted, completed, and documented;
3. document authorizations and restrictions for the use and disclosure or PHI;
4. monitor compliance through random checks; and
5. maintain appropriate documentation to establish compliance for at least 7 years.

The Privacy Officer shall provide a summary annual report of the Health Care Components' training activities and any breaches of PHI to the UHS Privacy Officer.

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

D. Signed Employee Confidentiality Statement. All workforce members who come into contact with PHI in performing their job function shall acknowledge in writing that they agree to access only the minimum amount of PHI necessary to do their job, and will comply with the provisions of federal and Texas law, University policy, and the health care component's policies and procedures. The health care component shall provide a form for this purpose and shall keep it on file.

E. Determining workforce access to PHI. Access to PHI shall be granted to persons based on their role, as determined by their supervisor, manager, and unit head. **The UHS health care component shall identify:**

(1) Those persons or classes of persons in the UHS workforce, including students, trainees, and volunteers, who need access to PHI to carry out their duties, and

(2) 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.

F. Security. Pursuant to UHS Policy (SAM 07.A.08-Data Classification and Protection), medical records, whether protected under FERPA or the Health Privacy Laws, are classified as Level 1 information requiring a high level of security controls. *See also* SAM 01.D.06 (Confidential Information). In all instances involving electronic PHI ("e-PHI"), UH IT Security must be contacted to ensure that only authorized systems for processing, storing or entering PHI are used and that PHI is securely transmitted, or encrypted. An authorized user who wishes to encrypt Protected Health Information must ensure that the encryption code is not based on information about the patient whose information is being de-identified, and that the code cannot be translated so as to identify the individual.

G. Security Officer. Each department shall assign a security officer who, with UH IT Security, is tasked to work with UH IT Security to:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information 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

(4) Ensure compliance with security requirements by the department's Workforce; and

(5) Implement security policies and procedures and ensure compliance with University and the Health Care Component' security policies and procedures.

H. Uses and Disclosures of Protected Health Information

(1) **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.**

(2) *Authorizations.* Except as otherwise permitted by this section, UHS and its health care components may not use or disclose PHI without a valid authorization from the individual. All authorizations must contain certain legally required language. Please contact the Office of General Counsel for assistance in developing a valid authorization for your department's use.

(a) *Individuals request release of their own PHI*. An individual requesting the release of the individual's own PHI must complete and sign the authorization form developed by the health care component. UHS's release of PHI must comply with the directives stated in the authorization. The UHS health care component must save all signed authorizations in the individual's record. PHI may be disclosed without an authorization if the law requires such disclosure. The UHS health care component from which PHI is released must document the disclosure in its database used for this purpose.

(b) *Authorizations from other entities*. All Workforce members must confirm that any authorization form received from other entities contains the necessary language to cover the Health Care Component' release of the patient's Protected Health Information.

(c) *Exceptions*. Authorizations for the use or disclosure of PHI are not required for the following treatment, payment or health care operations ("TPO"):

1. Use or disclosure for the purpose of UHS's own treatment, payment or health care operations.
2. Disclosure for treatment activities of another health care provider.
3. Disclosure to another covered entity or a health care provider for the payment activities of the entity receiving the information.
4. Disclosure to another covered entity for the health care operations of the entity receiving the information, as long as UHS 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.

(3) *Student Health Information/FERPA.* Both HIPAA and the Texas Medical Records Privacy Act exempt health information on students when it is either an education record under the Family Education Rights and Privacy Act (FERPA), or when health information for adult students is used only for treatment and not disclosed to anyone else. To cover all records maintained by UHS health care components, UHS suggests that UHS workforce members obtain from each patient a signed Consent for the Use and Disclosure of PHI prior to any use or disclosure of PHI to carry out treatment, payment or operations.

(4) *Employment Information.* Medical information held by the System in its role as employer is generally exempt from both HIPAA and the Texas Medical Records Privacy Act. In other words, PHI contained in the following records generally is not encompassed by the statutes: Workers Compensation Insurance; Employee Benefit Plan; Employment records held by employers *(e.g. leave information, return to work documentation, FMLA documents, accommodation records).* However, under Texas law, the following prohibitions apply to employers as well as all other departments handling Protected health Information:

1. Do not disclose PHI electronically without notice to or authorization from the individual to whom PHI applies.
2. Do not send PHI electronically without proper notice and authorization.
3. If you electronic disclose PHI, you must post a written notice to that effect in your offices, on your website, or anywhere affected individuals are likely to see it. You may need an authorization before providing an individual's PHI to another person. Authorization can be written, electronic, or oral if documented in writing.
4. Do not attempt to re-identify information without the individual's consent or authorization.
5. Do not use PHI for marketing/fundraising purposes.
6. Do not sell or receive compensation for providing PHI.

5. *Specially Protected Medical Records*. The following medical records are subject to special confidentiality protection and shall only be disclosed with an explicit authorization or as otherwise permitted by law. Health Care Components should contact the UHS Office of General Counsel with questions on using or disclosing these records.

- Drug Alcohol or Substance Abuse Records
- Psychotherapy Notes
- Mental Health Records
- HIV/Aids Records
- Genetic Information

(6) *Minimum Necessary Requirement.* When using or disclosing PHI or when requesting PHI from another covered entity or business associate, UHS must limit the use, disclosure or request to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. For instance:

- no one should be accessing or reviewing documents containing PHI unless it is in the scope of their duties to do so.
- medical record custodians must not use, disclose, or request the entire medical record except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

- Persons handling payment for PHI may not disclose information about an individual's diagnosis or treatment.

(7) *Educational Purposes.* Faculty, staff, students, and trainees must use de-identified information when in a classroom setting.

(8) *Requests for uses and disclosures of entire medical records*. Medical record custodians must not use, disclose, or request the entire medical record except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

(9) *De-Identification of PHI.* Because PHI is rendered anonymous whenever its identifying characteristics are completely removed, the University strongly encourages the use of de-identified information where practicable to adhere to the minimum necessary standard and to ensure the privacy of the individuals whose PHI is being used. All Workforce members must strictly observe the following standards for de-identification of PHI.

a) PHI must be de-identified prior to disclosure to non-authorized users.

b) To be considered de-identified, the following identifiers of the individual or of relatives, employers or household members of the individual must be removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to 000.

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

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) addresses numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code; and

The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

A person may not re-identify or attempt to re-identify an individual who is the subject of any PHI without obtaining the individual's consent or authorization if required under the Health Privacy Laws.

Only de-identified information should be used in the classroom.

(10) *Encryption*. If the PHI is not de-identified, the user must encrypt PH. The encryption code used must not be based on information about the individual whose information is being de-identified, and the code cannot be translated so as to identify the individual.

(11) *Marketing.* "Marketing" means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

(a) HIPAA and Texas state law have specific requirements for marketing purposes, mandate specific client authorizations, and contain special mailing requirements. .

Any marketing in relation to protected health information must be approved by the Department Chair, Privacy Officer and General Counsel.

(b) The authorization must include a way for client to opt out of receiving material subsequent to first contact and a separate authorization for each use. If the marketing involves payment to the Health Care Component from a third party, the authorization must state that such remuneration is involved.

(c) Authorizations are not required if the communication is for:

1. Providing information on health-related products and services in a face-to-face encounter with a patient or client.
2. 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 UHS in exchange for making the communication is reasonably related to the cost of making the communication.
3. Providing treatment of an individual by a health care provider, except where UHS receives financial remuneration from a third party in exchange for making the communication.
4. Providing promotional gifts of nominal value (pens, calendars, etc.).

(b) If the 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 the Health Care Component receives the request.

(12) *Sale of PHI.* "Sale of PHI" means a disclosure of PHI by a covered entity or business associate where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI. A covered entity may not disclose an individual's protected health information to any other person in exchange for direct or indirect remuneration, except that a covered entity may disclose an individual's protected health information for treatment, payment, operations for remuneration to cover the covered entity's reasonable costs of preparing or transmitting the protected health information.

The University strongly discourages the sale of PHI to a third party. Any proposed use of PHI for this purpose must first be approved by the Department Chair, Privacy Officer and General Counsel.

(13) *Fundraising***.** Any fundraising materials sent to a patient will have clear and conspicuous instructions on how a patient may opt out of receiving such communications in the future. Any fundraising in relation to protected health information is discouraged and must first be approved by the Department Chair, Privacy Officer and General Counsel.

(14) *Requirements for Electronic Disclosure.* If patients' protected health information may be disclosed via electronic means, a notice to that effect must be displayed in a clear and prominent location, posted on the practices' website, and/or elsewhere where affected individuals are likely to see the notice. The patient or client must specifically authorize the Health Care Component to disclose protected health information via electronic means to another person or entity. The authorization for electronic disclosure of protected health information can be written, electronic, or oral and must be documents by the Covered Entity. No authorization is required for electronic disclosure of PHI if it is made to another covered entity for treatment, payment, health care operations, and insurance functions.

(15) *Training Requirements.* The Privacy Officer of each health care component shall be responsible for ensuring that members of the component's Workforce (as defined above) are properly trained in the requirements of federal and Texas law. 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.

a. Training shall meet the following requirements:

i. All current members of the workforce shall complete training within 60 days following the date when they start their duties and every two years thereafter.
ii. The supervisor of the workforce member shall be responsible for initiating training.
iii. Workforce members whose duties are affected by a material change in the privacy laws or policies shall be retrained with 60 days after the change becomes effective.
iv. Workforce members who have violated privacy laws, policies, or procedures shall be retrained within thirty days of the determination.

b. Each individual receiving training shall certify completion of the training. The Privacy Officer shall document each training session and the names of the workforce members who completed training. Such documentation shall be maintained within the Health Care Component's privacy records for at least seven years from the date of training.

c. **The Privacy Officer shall provide a summary annual report of the component's training activities to the UHS HIPAA Compliance Officer.**

d. Texas Medical Records Privacy Act training is available at Human Resources. HIPAA training is available through the office of General Counsel or via external sources.

(16) *Research.* The University strongly encourages the use of *de-identified* PHI for research. Individuals planning to use PHI to recruit participants or conduct research must first contact the University Department of Research to determine whether specific

authorizations are required.

(a) In some instances, and particularly those for research, public health, or health care operations, a third party may provide a limited data set of identifiable patient information to a Primary Investigator for research purposes. If that information comes from a HIPAA covered entity, that entity or one of its business associates may request the University to enter into specific agreements to maintain the confidentiality of that information. All such agreements shall be routed to the Department of Research for handling. The Department of Research will forward the information to the Office of General Counsel and the University Privacy Officer as necessary.

(b) A Health Care Component at UH also may be asked to disclose PHI to a third party or another department for their research purposes. In that instance, the Covered Entity should discuss with the Department of Research to determine the steps to undertake to protect any data or PHI it provides for research purposes.

(17) *Confidential Communication Methods with Patients. A* Health Care Component will accommodate requests from patients regarding how they wish us to communicate with them regarding their Protected Health Information, subject to the terms of this policy.

(a) If possible, the Health Care Component will accommodate reasonable requests from a patient to use a particular manner or method of communication with them in order to preserve the confidentiality of their information.

(b) Such requests shall be made in writing.

(c) The Health Care Component will not ask or require a patient to explain why they want a particular communication method.

(d) The Health Care Component's Privacy Officer is responsible for receiving and acting upon these patient requests.

(18) *Personal representatives of patients.* Properly authorized personal representatives of a patient can exercise all the rights that the patient could exercise regarding the use and disclosure of Protected Health Information and can provide any required permission for a use or disclosure of Protected Health Information.

(a) Before a health care component agrees to work with a person claiming to be a personal representative of a patient, the Health Care Component must examine its authority to do so. This can include examining the patient file, verifying the individual's identification, and/or examining court or other legal documents in consultation with the Office of General Counsel.

(b) In some instances, the Health Care Component may choose not to work with a patient's personal representatives. This can happen when:

i. The Health Care Component feels that a person claiming to be a personal representative has or may have committed domestic violence, abuse, or neglect against the patient, and it is not in the patient's best interest to treat that person as the personal representative.

ii. The Health Care Component feels that treating such person as a personal representative could endanger a patient, and it is not in the patient's best interest to treat that person as the personal representative.

(c) If someone claiming to be a family member or friend of the patient initiates contact with the Health Care Component seeking information regarding a patient's Protected Health Information, the Health Care Component will:

i. verify the identity of the caller and their relationship to the patient;
ii. determine if they are involved in the patient's care;
iii. determine if the patient is available (by phone, email, FAX or other communication method) to either agree or object to the disclosure. If so, the Health Care Component will give the patient the chance to agree or object.
iv. If the patient is not available by any reasonable means, the health care component should determine:
    1. whether the patient has previously authorized this individual to receive his PHI; or
    2. If the patient has specifically requested that *no* information be provided to this individual;, or
v. alternatively use its best professional judgment to determine whether disclosure of information is in the patient's best interest, and if so, provide only the minimum necessary.

(19) *Patients' rights to access own medical records under HIPAA and Texas law.* A patient may request information maintained in the designated record set of the Health Care Component. The individual must make the request in writing, using the appropriate form. If the patient has an approved personal representative, the personal representative can inspect or copy the patients Protected Health Information on behalf of the patient.

a) If the Health Care Component does not maintain the requested PHI but knows where the requested information is maintained, then it must inform the individual where to obtain the information.

b) The following information is exempt from a patient's right to access (to the extent applicable):

1) Psychotherapy notes;
2) Information compiled in anticipation of use in a civil, criminal, or administrative action or proceeding;
3) PHI subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA) and the disclosure is prohibited by law; and

4) PHI exempt from CLIA, pursuant to 42 CFR 493.3(a)(2), which 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.

c) Under limited circumstances, the patient's request can be denied. Any concerns about granting the request should be addressed to the Privacy Office or the Office of General Counsel.

d) **Based on Texas law, the Health Care Component must act on the individual's request no later than the 15th calendar day after receipt of the request and payment of any necessary fee.**

VI. Additional HIPAA Requirements for HIPAA Covered Entities Only

A. *HIPAA's Four Main Functions*

1. Transactions and Code Set Standards – HIPAA standardizes electronic transactions and codes for patient health, administrative and financial data, e.g. diagnostic codes; medical providers, employer and health plan codes.

2. Security Rule – HIPAA provides uniform safeguards for health information and requires risk analysis and practices to secure electronic systems, including mobile/portable devices and remote access/use.

3. Privacy Rule – HIPAA Protects confidentiality of Protected Health Information (PHI) by limiting use and disclosure of PHI while giving patient rights on how PHI is used and to access records.

4. Breach Requirements – HIPAA sets forth notification requirements in the event of a HIPAA privacy and/or security breach.

B. *Covered Entity Responsibilities:* All staff, faculty, students, volunteers, trainees, paid or unpaid, performing work for the covered entity or a business associate must understand and follow HIPAA.

C. **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 the procedures covered in these guidelines.**

D. *Notice of Privacy Practices:* Each HIPAA covered entity must provide a Notice of Privacy Practices stating how client's health information may be used and disclosed and the client's rights with respect to the information**.** This notice must contain legally required information which may be obtained from the Office of General Counsel.

1. The Notice of Privacy Practices must be provided to each patient at the time of first contact with the patient, be posted at the clinic in a clear and prominent location, and be available on its website.

2. A good faith effort must be made to obtain the patient's acknowledgement that he has received the Notice; however, if the patient refuses to sign, the refusal must be noted on the acknowledgement form accompanying the Notice of Privacy Practices and placed in the patient's file.

3. 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.

4. If a patient or client is treated on an emergency basis, the health care component may delay providing the Notice of Privacy Practices and receiving an acknowledgement until a practical time.

5. All Workforce members reviewing or handling a patient or client's file are responsible for ensuring that the Acknowledgement or other documentation establishing receipt of the Notice of Privacy Practices is present in the patient file. If such documentation does not appear in the patient records, the Patient shall be provided another copy of the Notice of Privacy Practices, and reasonable attempts shall be made to obtain the Acknowledgement from the patient.

E. *Consent for the Use and Disclosure of Protected Health Information – Additional Requirements.* In most instances, **t**he Health Care Component must obtain written authorization from the patient prior to using and/or disclosing a patient's Protected Health Information for all purposes. However, HIPAA does not require a signed patient authorization in the following circumstances:

1. Uses and disclosures for <u>treatment</u>, <u>payment</u>, <u>or health care operations</u>. This includes, among other activities:

   a. providing health care to patients in the Health Care Component office;
   b. seeking assistance from consultants or other health care professionals;
   c. making referrals of patients for additional or follow-up care;
   d. writing, sending, and filling prescriptions for medications or medical items;
   e. preparing and submitting claims and bills to patients, third party payors, employee benefit plans, and Worker's Compensation Insurance representatives;
   f. receiving and posting payments and processing such payments with a financial institution;

g. collection efforts;
h. professional licensure and specialty certification;
i. quality assurance;
j. financial audits and management;
k. training of professional and non-professional staff, including students and other doctors;
l. office management;
m. customer service activities;
n. Due diligence to prevent fraud and abuse prevention;
o. Workforce members activities;
p. Compliance with applicable law.

2. Disclosures of Treatment to Health Plans. If a patient paid out-of-pocket in full for a specific item or service, the Health Care Component will make reasonable efforts to comply with a patient's request that it not disclose that item or service to the patient's health plan.

3. Disclosures business associates that have signed a business associate contract with the Health Care Component.

4. Public Health. Disclosures to state, local, or federal governmental public health authorities to prevent or control disease, injury, or disability, report of suspected child abuse or neglect, and reports regarding offenders with mental illness.

5. Product Safety. Disclosures to individuals or organizations under the jurisdiction of the federal Food and Drug Administration ("FDA"), such as drug or medical device manufactures, regarding the quality or safety or drugs or medical devices.

6. Health and Safety. Disclosures to avert a serious threat to a patient's health or safety or the health and safety of another person or the public.

7. Abuse, Neglect or Domestic Violence. Disclosures to local, state, or federal government agencies in order to report suspected abuse, neglect, or domestic violence regarding adults under certain situations.

8. Oversight. Disclosures for health oversight audits, investigations, or disciplinary activities, provided that the Health Care Component only disclose to a federal, state, or local government agency (or a private person or organization acting under contract with or grant of authority from the government agency) that is authorized by law to conduct oversight activities.

9. Law Enforcement. Disclosures for law enforcement activities such as in response to a court order, subpoena, warrant or similar process, or in emergency circumstances or if necessary to report a crime.

10. Organ Transplant. Disclosures to organizations involved in the procurement, banking, or transplantation of an eye to facilitate eye donation and transplant.

11. Research. Disclosures to a researcher with a waiver of authorization from an IRB or privacy board; to a researcher using the Protected Health Information only for purposes preparatory to research; or to a researcher only using the Protected Health Information of deceased patients if the researcher gives the Health Care Component the assurances required by HIPAA and applicable Texas law.

12. For National Security and Intelligence Activities.

13. Military and Veterans, as required by military command authorities or to the Department of Veterans Affairs upon the patient's separation or discharge from military services.

14. Inmates**.** If the patient is an inmate of a correctional institution or under the custody of a law enforcement official, the Health Care Component may disclose information about the patient to the correctional institution or law enforcement official.

15. Disaster Relief**.** Disclosures to a public or private entity, such as the American Red Cross, for the purpose of coordinating with that entity to assist in disaster relief efforts. If practicable, the Health Care Component will provide the patient with an opportunity to agree or object to such a disclosure.

16. Decedents. Disclosures to a coroner, medical examiner, or funeral director so that they can carry out their duties. The Health Care Component may also disclose a patient's PHI *when the disclosure relates to organ, eye or tissue donation purposes.*

17. Workers' Compensation. Disclosures to comply with laws and regulations related to Workers' Compensation.

18. Treatment Alternatives**.** Disclosures to provide information about treatment options or alternatives or other health-related benefits or services of interest to the patient.

19. Data Breach Notification Purposes**.** Disclosures to provide legally required notices of unauthorized access to or disclosure of a patient's health information.

20. As otherwise required by law.

Under any circumstances other than those covered by this privacy manual or applicable law, the Health Care Component personnel may only release a patient's Protected Health Information with a proper HIPAA authorization form.

F. *Business Associates.* A business associate is a person or entity, other than a workforce member of a UHS Health Care Component, that performs a function involving PHI for a health care component of UHS. In some instances, a University department performing functions for a UHS Health Care Component may constitute a business associate of that

department.

1. E**ach health care component must establish a business associate agreement with each of their business associates prior to using or disclosing PHI.** The business associate contract must establish the permitted and required uses and disclosures of PHI by the business associate. 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 UHS System Office of General Counsel before it is executed.

2. If the health care component becomes aware of a business associate'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 business associate's contract violations are not successful in preventing or mitigating improper use or disclosure of PHI, the health care component must terminate the contract, if feasible.

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

4. If the health care component becomes aware of a business associate'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 business associate's contract violations are not successful in preventing or mitigating improper use or disclosure of PHI, the health care component must terminate the contract, if feasible. Faculty/Staff should notify the clinic director if they become aware of an oversight by any business associate.

G. *Patients' Rights.* Patients have the following rights with respect to their PHI**:** To have PHI protected, receive a Notice of Privacy Practices, To obtain and review copies of their medical records, Ability to request an amendment to PHI, Ability to limit use and disclosure of PHI, Ability to request an accounting of uses and disclosures, and Ability to request restrictions on certain uses and disclosures of PHI.

1) Amendments: Patients have the right to request an amendment to their Protected Health Information under the conditions stated in this policy. If the patient has an approved personal representative, the approved personal representative may exercise this right on behalf of the patient.

a. All requests to amend Protected Health Information must be made in writing. If a patient calls on the telephone to request an amendment, the patient must be advised to submit the request in writing.

b. The Health Care Component' Privacy Officer is responsible for handling patient requests to amend their Protected Health Information.

c. The Health Care Component will respond to requests for amendment within 30 days after it receives the written request. The Health Care Component is allowed a 30 day extension if it notifies the patient in writing that it needs this additional time before the original time period expires.

d. The Privacy Officer may deny a request to amend only for one or more of the following reasons:

a) the information as stated is accurate and complete;
b) The Health Care Component did not create the information;
c) The information is not in a designated record set.
d) The originator of the information is no longer available.

e. If a request to amend is denied, the Privacy Officer will notify the patient in writing. The response will inform the patient of their right to either submit a statement of disagreement or have the original amendment request accompany the health care information.

f. If the request to amend is granted, The Health Care Component will:

a) notify the patient in writing of the approval to amend;
b) append or link the corrected information to the original information;
c) send the corrected information to anyone who the Health Care Component knows has previously received the original information or anyone else the patient requests;
d) clearly document the file.

2) Patient Requests to Restrict Disclosures. Patients may request that the Health Care Component restrict the way a health care component uses certain Protected Health Information for purposes of treatment, payment, or health care operations.

a. The Health Care Component's Privacy Officer will handle requests from patients to restrict its use or disclosure of their Protected Health Information.

b. Generally, the Health Care Component will not agree to such restrictions requested by patients, unless legally required or in unusual circumstances that the Privacy Officer considers meritorious. Examples

of situations where the Health Care Component must or will agree to the request include:

- where the patient does not wish certain relatives to be informed of particular Protected Health Information.

- where the patient has fully paid for an item or service out of pocket and has requested the Health Care Component not disclose the protected health information relating to that item or service to a health plan for payment or health care operations purposes;

- where the patient has specified a preferred method for the Health Care Communications with him/her.

c. If the Health Care Component agrees to the requested restriction, the Privacy Officer must document the terms of the request and agreement in a highly visible manner, and place this documentation in the Health Care Component Privacy File and patient file where it can be easily seen. The Privacy Officer will also communicate the terms of such an agreement to any other business associate or Workforce member on a need to know basis.

d. **All Workforce members must carefully review the file for any restrictions before using or disclosing protected health information. Restrictions requested on an earlier date may pertain to information that may be subject to disclosure that appears later on in the file.**

e. The Health Care Component will honor any restriction it has agreed to; however, no restriction can prevent the Health Care Component from using any Protected Health Information in an emergency treatment situation.

f. If the Health Care Component has agreed to a special restriction but can no longer honor that request, the Privacy Officer of the Health Care Component will do either of the following:

   a. contact the patient to work out a mutually agreeable termination of the restriction. Any new agreement must be documented and kept in the Health Care Component Privacy File or the patient's electronic health record.

   b. contact the patient and advise him/her that the Health Care Component is no longer able to honor the restriction. This notice to no longer adhere to the terms of the original restriction will only apply to information obtained or generated after notice to terminate is given.

g. ***A request to restrict the use and disclosure of the information, or the request for an explanation why the Health Care Component cannot honor the request cannot be the basis for denying service.***

3. *Accounting.* Upon a patient's *written* request, the Health Care Component will provide the patient with an accounting of the disclosures that it has made of the patient's Protected Health Information subject to the terms and conditions stated in this policy.

a) All disclosures of patient's information must be recorded in each file on a designated form. This includes all disclosures made to third parties (including healthcare providers and business associates) for treatment, payment, and operations when disclosed through "electronic health records".

b) The request for disclosure history may be made for any time period up to six years preceding the request.

c) The following disclosures are exempt from this requirement:

i. disclosures for treatment, payment, or health care operations (unless disclosed through electronic health records);
ii. disclosures made with signed patient authorization
iii. disclosures that are incident to other permitted disclosures;
iv. disclosures to family or friends involved in the patient's care;
v. disclosures made prior to April 14, 2003.

d. The following information regarding disclosures will be tracked and provided to the patient upon written request:

i. the date of the disclosure;
ii. the name and address (if known) of the person or organization who received the information;
iii. a description of the Protected Health Information that was disclosed;
iv. a statement of the purpose for the disclosure or copy of any request that prompted the disclosure

e. The Health Care Component will respond to a request for an accounting within 30 days from its receipt of the written request. An additional 30 day extension may be granted as long as the Health Care Component notifies the patient in writing of the need for such extension before the end of the original time period.

4) The accounting will contain all information stated in subsection d above. If repeated disclosures were made to the same person or organization for the same purpose, the accounting will provide all this information for the first

disclosure, and then indicate the frequency of the other disclosures and the date of the last disclosure.

5) The accounting also applies to business associates.

6) **Each file shall contain an area where disclosures may be documented. Workforce members shall carefully set forth all disclosures needing to be documented according to this policy.**

VII. Security Safeguards Under Both Federal and State Law

A. **Each UHS health care component must develop and implement administrative procedures 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.**

B. **Storage of PHI.** All University workforce members must strictly observe the following standards for storing Protected Health Information:

1. Workforce members must properly protect paper or electronic Protected Health Information when not in use, when left in an unattended room, and before regular working hours have ended, unless the immediate area can be secured from unauthorized access.

2. PHI stored on the computer, laptop, other mobile device, diskettes, thumb drives or other type of removable data storage media must be separately password protected or encrypted.

3. Backup copies of PHI stored off site must be stored in a secure location.

4. When PHI is being released through teleconference or video feed, the Health Care Component 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 personnel 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.

5. **PHI stored in medical equipment must be kept secure and disposed of in compliance with this policy.**

C. **E-Mail.** Never send unencrypted information over the Internet, never use the full nine-digit social security number in an electronic message unless the message has been encrypted or otherwise secured, and do not use a patient's full name associated with specific health information (e.g. reason for visit, diagnosis, procedures, or test results) without encrypting.

D. **Best Practices.** Do not use client's whole name in earshot of others**;** cover charts so client name is not visible**;** do not leave records & other PHI unattended**;** screen computers or locate so others cannot read the screen**;** keep secure client reports and appointment schedules; back up disks**;** reports prepared on home computers must be prepared in de-identified format; all reports sent as email attachments must be de-identified; video/audio tapes must be erased or destroyed before clinician graduates, unless being preserved in master client file at the clinic for archival purposes.

E. **Disposal of PHI**

1. PHI must not be discarded in trash bins, recycle bins (including those with locks), or other locations accessible to the public.
2. PHI must be personally shredded or disposed of in any reasonable way that renders documents unreadable.
3. Printed material and electronic data containing PHI shall be disposed of in a manner that ensures confidentiality.
4. 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.
5. Disposal of paper PHI shall be done by shredding using a shredder which prevents the documents from being reconstructed. The shredder should be located in a room which in not accessible to unauthorized personnel. PHI should not be discarded in a regular wastebasket. Photographs, images and reports from diagnostic equipment are considered PHI and should be handled as such.

F. **Administrative Requirements**

1. **Breach Notifications**. Federal and Texas law require breach notification and reporting with suspected or actual unauthorized access, use or disclosure of PHI. *Immediately report all known or suspected violations* to University IT Security and the Privacy Officer for assistance in determining whether the individual whose information was breached must be notified and the incident reported to the applicable covered entities, federal or state officials, and otherwise as appropriate.

2. ***Additional HIPAA Breach Notification Requirements*****:** HIPAA requires breach notification and reporting when a patient's *unsecured* PHI is impermissibly used/disclosed, unless the Covered Entity can demonstrate low probability that PHI has been compromised based on a risk assessment of several factors. *Immediately report all known or suspected violations* to the Privacy Officer for assistance in determining whether the individual whose information was breached must be notified and the incident reported to the Secretary of Health and Human Services (HHS) and/or the media. The Privacy Officer will consult with UH General Counsel to investigate and manage the incident. **The Privacy Officer will maintain a log of all breaches over the year to enable proper notification to the U.S. Department of Health and Human Services on an annual basis as required.**

3. **Mitigation of Harmful Effects from Unauthorized Use**. To the extent practicable, UHS will mitigate any harmful effect that becomes known to UHS as a consequence of the use or disclosure of PHI that violates federal or Texas laws, or the policies or procedures of UHS or of its health care components.

4. **Handling Patient Complaints about Privacy Violations.**

   i) Each health care component shall develop and implement a set of procedures that enable individuals who believe that a Health Care Component has not properly respected their medical privacy to file a complaint with the designated contact or Privacy Officer of the Health Care Component or through mysafecampus.com. Complaints about HIPAA violations may also be made to the Secretary of the U.S. Department of Health and Human Services, and otherwise as permitted by law.

   ii) All patient complaints will be addressed within 30 business days of receiving the written complaint from the patient.

   iii) Each health care component must document all complaints received, and their disposition, if any, and maintain such records for at least six years. These complaints, as well as information about the investigation and resolution of the complaint, will be kept in the Health Care Component Privacy File.

   iv) 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.

   v) The Privacy officer will investigate all complaints in the manner considered reasonable and logical in light of the nature of the complaint. Based on the results of the investigation, the Privacy Officer will determine if the patient's complaint is substantiated or not. If the complaint is not substantiated, the Privacy Officer will notify the patient in writing of that decision. If the complaint is substantiated, the Privacy Officer will take necessary steps, in consultation with the necessary personnel and administrators, to resolve the issue. If a violation occurs and a resolution put into place, the Privacy Officer will develop a way to monitor whether or not the resolution is working to improve the Health Care Component' privacy protections. If new policies or procedures are put into place as part of any resolution, the Privacy Officer will conduct mandatory training for its workforce regarding the new policies.

G. Prohibition of Retaliation. The Health Care Component 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 policy.
- Provides information to or testifies against the alleged offender or University.
- Objects to or refuses to participate in activities that they believe might violate federal or Texas laws or regulations, or this policy.
- Participates in a compliance review, audit, or peer review of health care services.
- 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 University Compliance Officer will review any allegation of retaliation and will ensure that a proper investigation is conducted.

H. Sanctions for Breaches. **Each health care component 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 UHS policies.** 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. The procedures for disciplinary action will be consistent with University policy and applicable law. The Health Care Component must document any sanctions that are applied.

In addition to University disciplinary action, violations involving Protected Health Information may also be enforced by the Secretary of the U.S. Department of Health and Human Services, the U.S. Justice Department, and the Texas Attorney General. Depending on the severity of the misconduct, individual criminal penalties may also apply.

Revised: 1/____/2016