

1. 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 “System”) to adhere to these guidelines. Additionally, each employee/student of the System and its component institutions who have access to protected health information are required to adhere to these guidelines.

HIPAA and the HITECH ACT (collectively “HIPAA”) are federal laws that protect the privacy of a patient’s protected health information. Patients have specific, protected rights regarding the release and handling of such records and HIPAA requires “covered entities” (as defined below) to adhere strictly to these guidelines. Therefore, it is imperative that faculty/staff/students with access to protected health information have knowledge of HIPAA guidelines.

2. HIPAA Guidelines:

2.1 Covered Entities: If you are a health care provider (physicians, hospitals, clinics, etc.) and transmit health information in electronic form (i.e. claims, benefit eligibility, referral authorization, enrollment, claim status, healthcare and premium payments, coordination of benefits), then you are a HIPAA Covered Entity.

2.2 Protected Health Information: “Protected health information” (PHI) includes any information that can possibly identify the particular patient to which the information applies. This information can be written, verbal, or electronic, including 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.

2.3 Important Exceptions: Health information on students is NOT PHI when it constitutes either an education or a “treatment record” (student health information used only for treatment and not disclosed to anyone else) under the Family Education Rights and Privacy Act (FERPA). Please contact the University General Counsel with questions about the interplay between FERPA and HIPAA.

2.4 Responsibilities of Health Care Providers: Each applicable clinic or department must: (i) identify a Privacy Officer; (ii) document its policies/procedures used to protect PHI, authorizations, restrictions, and complaints; (iii) keep documentation for 6 years;

and (v) train faculty, staff, and students on HIPAA. The HIPAA training should be provided to each new staff or faculty member and student clinician, as well as on an annual basis to such individuals and to each person who changes job functions.

2.5 Notice of Privacy Practices: This document states how patients' health information may be used and disclosed and specifies patients' rights with respect to the information. This notice must be provided to each patient at the time of first contact with the patient, be posted at the clinic, and be available on its website. Patients must acknowledge receipt of the form. If the patient refuses to sign, note refusal on acknowledgement form and place in patient's file.

2.6 Consents for Treatment – Use and Disclosure: Utilize separate consent forms for: video/audio taping and observation of the patient for training purposes.

2.7 Causes of HIPAA Incidents: Careless handling of patient information, unauthorized access or disclosure of patient information, sharing passwords or enabling others to work under the same user ID, accessing electronic patient information without first logging on with your own unique identification or password, failing to log off, shut off, or otherwise protect computer, gossiping about a patient's health information, faxing documents containing patient information to the wrong recipient or fax number, mailing reports or billing statements containing patient information to the wrong patient or wrong address, giving patient information or documents to the wrong patient, leaving printed documents containing patient or other confidential information unattended in a public place, having cameras or data storage devices with unencrypted patient data or pictures lost or stolen, sharing sensitive patient information while visitors are present in the patient's room without giving the patient an opportunity to object or consent.

2.8 Sharing Patient Information: You must obtain authorization before using or disclosing patient information *EXCEPT* to provide treatment or services for the patient, to bill or collect payment for services, as required in order to do your job as part of defined health care operations, as required or allowed by law (e.g., court order, subpoena, in response to any law enforcement body), or with appropriate authorization by the patient or the patient's legal representative. Except for treatment purposes, only share the minimum necessary information. Any court order, subpoena, Texas Public Information Act request or other similar request for protected health information should be immediately brought to the attention of the Privacy Officer and UH General Counsel before taking action.

2.9 Authorizations received from other entities: Make sure any authorization form you receive from other entities contain the language required under HIPAA or state law to cover YOUR release of the patient's PHI! Best to check with your Privacy Officer, department head, or UH General Counsel.

2.10 Minimum Necessary Disclosure: Only use the "minimum necessary" disclosure of PHI. Only employees *authorized* to use and disclose PHI are permitted to do so. The health provider must not use or disclose a patient's PHI without the written permission of

the patient, except as described in its Notice of Privacy Practices. Examples of Minimum Necessary: your best friend's brother comes into your clinic for care. If you are NOT providing his care, you should NOT be reading his records. The receptionist/appointment maker/file clerk should NOT be reading the contents of a patient's file in most situations. If someone authorized to receive information requests the dates of treatments, provide the dates but no more information than requested.

2.11 De-Identifying PHI: Remove all 18 Personal Identifiers to avoid being subject to HIPAA : **Names** (patient, relatives, household members & employers), **Address** (street address, city, county, state, precinct and all geographic subdivisions smaller than a state), **Zip Code, Dates** (birth, visit, admission, discharge, death and all ages over 89), **Visual** (pictures, voice prints, finger prints), **Numbers** (accounts, SS, licenses, health plan numbers, serial numbers, etc.), **Phone numbers, fax numbers, e-mail addresses, Web URLs, IP address numbers, Any other unique identifying number, characteristics, or code.**

2.12 Marketing & Fundraising: HIPAA and Texas state law each have specific requirements for marketing purposes. Specific patient authorization is required. The authorization must include a way for patient to opt out of receiving material subsequent to first contact and a separate authorization for each use. Any marketing or fund raising in relation to protected health information must be approved by the Department Chair, Privacy Officer and General Counsel. Please note that the Texas Medical Records Privacy Act defines "covered entity" to include anyone who collects, analyzes, uses, or sends protected health information, regardless of whether or not the protected health information is electronically transmitted.

2.13 Research: You cannot access PHI to recruit participants or conduct research unless the University Internal Review Board (Human Subjects Board) approves the authorization or IRB has waived the authorization requirement.

2.14 Business Associates: We require a business associate agreement with any entity that provides a function for our health providers, and under certain circumstances, certain University departments performing functions for HIPAA-covered entities may constitute a business associate of those entities. Business associates, not ordinarily covered by HIPAA, are now required to comply with HIPAA requirements as well. HIPAA imposes obligations on business associates to terminate agreements and/or report violations of covered entities. We also are responsible for HIPAA violations of business associates. Faculty/Staff/Students should notify the Privacy Officer if they become aware of an oversight by any business associate. All business associate agreements should come through OGC for review.

2.15 Patients' Rights: A patient has the right to have PHI protected, receive privacy notice, obtain and review copies of records, request an amendment to PHI, limit use and disclosure of PHI, request accounting of uses and disclosures, request restrictions on certain uses and disclosures of PHI. Patients may ask the health care provider not to disclose PHI to family members or personal representatives, but the health care provider

may act on its own if the patient is unable to state a preference. A patient may revoke in writing their previous consent to use and disclose certain types of PHI. In the case of a Legal Guardian or Power of Attorney, we must make a copy of the documentation and keep in the patient file.

2.16 Patient Access To Own Records: Patient may access all information in a designated records set upon specific written request. The request must specify the items being requested. We have up to 30 days to grant the request. We can deny the request under limited situations (e.g. danger to someone else). The patient can challenge denial.

2.17 Amendments: Patient can request an amendment to their record. Request must be in writing and must be specific. We have 60 days to grant or deny. We can refuse if we believe the record is accurate as is, or if record was not created by you or originator is no longer available. We must notify patient of decision and/or when record is amended. Additional procedures must be followed and should be addressed with the Privacy Officer.

2.18 Patient Requests to Restrict Disclosures: Patient can request that we restrict uses or disclosures of PHI. All such requests **must** be brought to the Privacy Officer's attention and extensively documented. If patient requests, covered entities must not disclose PHI to a health plan for payment or health care operations purposes if the PHI relates solely to an item or service fully paid for out of pocket. *Make sure to always check the file:* Has patient restricted access to certain family members? Has patient specified preferred method of contact? Use reasonable judgment in disclosing PHI to patient's family and friends (give patient opportunity to object). Whenever possible, allow the patient to determine which family members or others involved in their care are communicated with regarding the patient's care and services. Do not assume that the patient agrees for a visitor or family member to see or hear any personal health information). Use professional judgment to determine whether the disclosure is in the best interest of patient and, if so, disclose only the PHI directly relevant.

2.19 Accounting: All disclosures of patient's information must be recorded in each file on a designated form. Under the HITECH Act, this includes all disclosures made to third parties (including healthcare providers and business associates) for treatment, payment, and operations (TPO) when disclosed through "electronic health records". Each request must be in writing. Also applies to business associates.

2.20 Breach Notifications: The HITECH Act and regulations require breach notification and reporting when a patient's PHI is accessed, used, or disclosed in a way that violates HIPAA and poses a significant to risk of reputational, financial, or other harm to the individual. *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). The Privacy Officer will consult with UH General Counsel to investigate and manage the incident.

3. Additional Guidelines and Best Practices for Faculty and Staff

3.1 Protecting Privacy of Patient Information: Only share patient information with other faculty and staff who need the information to do their job. Avoid accessing a patient's record unless you need to do so for your job or you have written permission from the patient. Do not access the record of your co-worker, spouse, or family member unless there is written authorization in the patient's record.

3.2 E-MAIL: Never send unencrypted information over the Internet that you would not place on a billboard. You cannot control how a message you generate is forwarded or shared after you hit the "Send" button! Never use the full nine-digit social security number in an electronic message unless the message has been encrypted or otherwise secured! Do not use a patient's full name associated with specific health information (e.g. reason for visit, diagnosis, procedures, or test results).

3.3 Telephone and Fax Precautions: Only speak to the patient (or parent); do not leave message with identifying information; do not give your personal phone number; check fax number (more than once); fax with a permission form; use a cover sheet; check to see if the fax was received; do not fax plans, logs, reports to supervisors unless absolutely necessary and only if info is de-identified.

3.4 Files: Store patient files, CDs/USB drives containing PHI and video/audiotapes in a locked file cabinet. Never store PHI on personal hard drives. *Never* take from clinic unless to off-site assessment and then you must immediately return the files.

3.5 Best Practices: Do not use patient's whole name in earshot of others; cover charts so patient name is not visible; do not leave records & other PHI unattended; screen computers or locate so others cannot read the screen; keep secure patient reports and appt 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 patient file at the clinic for archival purposes.

3.6 State Law: Texas and other states also separately regulate the privacy of healthcare information. HIPAA preempts state law unless state law imposes stricter requirements. The Texas Medical Records Privacy Act defines "covered entity" more broadly to include virtually anyone or any entity coming into contact with PHI. This definition comes into play particularly with marketing and reidentification, both of which require individual consent under Texas law.

3.7 Sanctions and Penalties. Potential University sanctions, in order of ascending severity: verbal/written warnings, probation, suspension, transfer, or termination of employment. **Penalties:** Monetary penalty amounts, imposed by the U.S. Office of Civil Rights and/or Texas Attorney General can be huge. Individuals, including employees of covered entities or business associates, may be criminally liable or subject to imprisonment.