SAFEGUARDS FOR PROTECTED HEALTH INFORMATION (PHI)

Policy

The Health Science Center (HSC) values its member’s privacy rights and is committed to safeguarding protected health information. HIPAA Rules require that the University have reasonable administrative, technical and physical safeguards in place to protect PHI from any intentional or unintentional use or disclosure and to limit incidental uses or disclosures. The University will make reasonable efforts to use or disclose only the minimum amount of PHI necessary for treatment, payment, or health care operations.

Definitions

ADMINISTRATIVE SAFEGUARDS: Is the administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of the Universities workforce in relation to the protection of that information

PHYSICAL SAFEGUARDS: Generally are physical measures, policies and procedures to protect and secure all forms of protected health information from unauthorized access, accidental or intentional use, disclosure, transmission, or alteration, and inadvertent or incidental disclosure.

TECHNICAL SAFEGUARDS: Is the technology and the policy and procedures relating to electronic storage, maintenance, and transmittal of PHI, including authentication requirements, password controls, audit trails, email encryption, and Internet use.

Administrative, Physical, and Technical Safeguards

- University employees will discuss PHI with other employees only when the other person is authorized to have access to PHI for purposes of performing job responsibilities related to treatment, payment or health care operations, or other authorized purposes.

- University employees must avoid unnecessary disclosures of PHI through oral communications.
• Conversations, both phone and face-to-face, involving PHI shall take place in low tones, to the extent possible, and in closed offices or cubicles when possible.

• When having a conversation in a public area with a patient, the patient’s family members, or other conversations in which PHI is discussed, conduct the conversation in a lowered voice, to the extent possible, and avoid using patients’ names or the names of patients’ family members when persons who are not authorized to receive the information are present.

• PHI may be released over the telephone in the same manner that it may be released in person, in accordance with the policies regarding disclosures of PHI, and will be documented as appropriate. When handling a call that involves PHI, efforts to verify the identity and authority of the caller will be made prior to discussing the PHI. (See Section 11.1.6 of the Handbook of Operating Procedures (HOP), “Confidentiality of Patient Health Information”)

• PHI mailed must be in sealed envelopes and no PHI can be visible. Preferably, using a window envelope to allow the recipient’s address to be printed on the paper contained within.

• The transmission of PHI via facsimile (fax) is permitted in accordance with the accounting of disclosures (See Section 11.3.1 of the HOP, “Accounting of Disclosures of Protected Health Information”), provided that an approved Facsimile Cover Sheet, containing confidentiality language is used. The sender ensures that an appropriate person is available to receive the fax as it arrives, and that the fax is being sent to a secure location. (See Section 11.1.8 of the HOP, “Fax Transmittal of Protected Health Information”)

• PHI may not be included in an electronically transmitted message over a public network. i.e. Internet, except as permitted by and in accordance with the Universities e-mail policy (See Section 11.1.12 of the HOP, “E-mailing Protected Health Information”). E-mail destined for an address outside of the UTHSCSA.edu (e-mail) network that contains PHI should be processed through the Health
Science Center’s secure e-mail gateway (see Secure Email instructions located at http://infosec.uthscsa.edu/secure-email?utm_source=imssecuritydirectory&utm_medium=pageredirect&utm_campaign=imssecurity), which will encrypt the communication in a form that can be decrypted by the intended recipient.

- Computer screens and monitors will be located in areas or at angles that minimize viewing by persons who do not need the information or utilize privacy screens.

- Whiteboards and scheduling boards that display PHI will be located in areas that minimize viewing by persons who do not need the information or the information will be de-identified of PHI.

- PHI should not be printed or copied indiscriminately or left unattended and open to compromise.

- All employees must store paper PHI in areas that are not accessible to unauthorized individuals, preferably in a locked room or filing cabinet.

- The original media should be used (e.g., hardcopy medical record, EPIC, My Chart) and only reproduced when absolutely necessary.

- Printers and copiers used for printing of PHI should be in a secure location.

- If the equipment is in a non-secure location, the information being printed or copied is required to be strictly monitored. PHI printed to a shared printer should be promptly removed.

- PHI in hardcopy format must be disposed of in accordance with the records retention schedules managed by the custodian of the medical records. (http://library.uthscsa.edu/rrs/recordrrs.php)

- Disposal of patient information, when no longer needed or required by law, will be properly disposed of, or destroyed, so that it is unrecoverable. This may be accomplished by shredding or other
methods that render the document non-readable. These documents include sign-in logs, lab or diagnostic reports, patient schedules, billing and health records and duplicate cash receipts.

- The designated custodian of the medical record has the sole authority to disclose PHI when a patient authorization is required.

- When transporting medical records, they should never be left unattended and records should be covered or turned over so that PHI is not visible to casual observers.

- PHI stored in medical equipment (e.g. EKG, Ultrasound) must be kept secure and disposed in a way that preserves the confidentiality of the patient information.

- For additional guidance relating to securing and storing PHI on mobile devices see Section 11.1.14 of the HOP, “Securing Protected Health Information and Mobile Devices”.

- For additional guidance on security of confidential information see Section 5.8 of the HOP “Information Security”.

### Notification by a Business Associate

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the University, without unreasonable delay and in no case later than 30 days, following the discovery of the breach. To the extent possible, the business associate should provide the University with the identification of each individual affected by the breach, as well as any information required to be provided by the University in its notification to affected individuals. [http://uthscsa.edu/hipaa/assoc-contract.asp](http://uthscsa.edu/hipaa/assoc-contract.asp)

### Mitigation

The University, and or its business associates, to the extent practicable, maintains policies and procedure to mitigate harmful effects in the event of a violation of this policy or an improper use/disclosure of PHI. The duty to mitigate includes, but is not limited to:

- Taking operational and procedural corrective measures to remedy violations.
• Taking employment actions, reprimand, or discipline employees as necessary, up to and including termination.

• Addressing problems with business associates once the University is aware of a breach of privacy.

• Addressing and investigating the Universities facility workforce violations.