SHSU Physicians Policy XXXXX

PATIENT PRIVACY AND HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

1. GENERAL

SHSU Physicians is a Health Care Component of Sam Houston State University (SHSU), a Hybrid Health Insurance Portability and Accountability Act Entity. This policy pertains to all SHSU employees assigned to SHSU Physicians (SHSU Physicians or Clinic) and to those who facilitate transactions involving protected health information (PHI), as well as Clinic non-employee workforce, vendors, or contractors that have access to patient records. SHSU Physicians is required to maintain the privacy of PHI of patients and to provide notice about legal duties and privacy practices concerning PHI. The Clinic is also required to accommodate reasonable requests made to communicate PHI by alternative means or at alternative locations. The Clinic shall follow this Policy when using or disclosing PHI.

2. PURPOSE

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and their implementing regulations, as amended, protects PHI and prohibits its unauthorized access, use, or disclosure. HIPAA and HITECH and implementing regulations are referred to collectively herein as HIPAA. Further, unauthorized access, use, or disclosure of such information could cause irreparable harm to SHSU Physicians, its workforce, students, affiliated entities, vendors, the community, and others, and could subject SHSU Physicians and its workforce to fines, criminal penalties, other sanctions, civil liability, and/or damage to reputation and standing.

SHSU Physicians, its workforce, and vendors shall protect such information as required by HIPAA, this policy, and applicable SHSU and Texas State University System (TSUS) Rules and Regulations and policies, SHSU Physicians policies and procedures. SHSU Physicians workforce, SHSU employees that facilitate Clinic covered transactions, and vendors are required to know and follow this policy and SHSU Physicians procedures.

3. DEFINITIONS

3.01 Breach. The acquisition, access, use, or disclosure of protected health information that compromises the security or privacy of the information when such disclosure is not otherwise permitted by law. More detail on what events constitute a breach may be found in the SHSU HIPAA Breach Notification Policy.

3.02 Business Associate. A person or entity other than a member of a SHSU health care component workforce that performs a function or service that creates, receives, maintains, or transmits protected health information for a HIPAA covered entity.

3.03 Information Security. The preservation of confidentiality, integrity, and availability of protected health information; in addition, other properties, such as authenticity, accountability, nonrepudiation, and reliability can also be involved.

3.04 Protected Health Information (PHI). Individually identifiable health Information, in any form or media, created, received, maintained or electronically transmitted by a covered entity or its business associate.

3.05 Workforce. 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 SHSU Physicians or a business associate. For purposes of this policy, references to employees shall include members of the SHSU ~~Physician's~~ Physicians workforce.

4. NOTIFYING PATIENTS OF PRIVACY PRACTICES

SHSU Physicians shall comply with all requirements of the HIPAA Privacy Rule, including:

4.01 Notice of Privacy Practices (NPP) is a document patients sign acknowledging that SHSU Physicians has provided Notice of Privacy Practices and that SHSU Physicians will protect their information as set forth in the HIPAA Act. (See Notice of Privacy).

4.02 Copies of the NPP will be kept at various locations throughout the facility. A copy will be available for each patient to review and sign upon Clinic check-in. SHSU Physicians will provide a paper copy to patients who request a copy.

4.03 Patients may make a written request for amendment of their PHI contained in medical records created and maintained by SHSU Physicians, provided the request is accompanied by a supporting reason. If a patient orally requests an amendment be made, or does not provide a reason, the patient will be provided with a "Request for Amendment of Protected Health Information" form to facilitate their ability to make a written, complete request.

4.04 Before SHSU Physicians uses or discloses patient PHI for any purpose involving treatment, payment, or health care operations, the Clinic must make a good faith effort to obtain an NPP Acknowledgment from the patient. Any signed NPP Acknowledgement is to be kept in the patient's chart (electronic or paper).

4.05 If a patient refuses to sign the NPP, a notation will be made in the chart (electronic or paper) that the patient was provided the NPP, but refused to sign.

4.06 Patients 18 years of age or older or emancipated minors can sign the NPP. Otherwise, the parent or guardian accompanying the child to the appointment as required by SHSU Physicians policies will sign for the child or dependent.

4.07 Red Flag Rule-SHSU Physicians will make an effort to identify each patient with his/her medical records, to protect patients from theft of identity, PHI and other sensitive information including, credit card information, social security numbers, insurance claim information, and employer information.

4.08 New and established patients may be asked for photo identification to be scanned into the computer. Any minor patient's identification will be verified by a photo ID of the guarantor on account. All sensitive information will be kept in a secure location for a minimum of ten (10) years.

5. RELEASE AND DISCLOSURE OF PHI

5.01 A signed release of medical records must be obtained when records are requested from ANY outside source, except those directly associated with treatment and billing purposes (patients' insurance company, referring physician, hospital or surgery center, laboratories, pharmacies). Some authorizations may be done on a case-by-case basis each time disclosure is made.

5.02 A patient has the right to have access to and a copy of their own PHI, to know what uses are being made of their information, and to whom it is being disclosed. A patient may request an accounting of their PHI disclosure through a written request. This request will be saved in the patient’s record (paper or electronic).

5.03 A patient must sign a Release of Information or Authorization for any disclosure outside of direct treatment and billing purposes. SHSU Physicians will identify the person signing the request by a form of an official government picture ID.

5.04 SHSU Physicians share PHI with business associates and may allow the business associate to create and receive PHI on behalf of the Clinic. A signed contract with the business associate must be obtained to ensure safeguard of the information, compliance with this policy, and the requirements of HIPAA.

5.05 SHSU Physicians will provide the "minimum necessary" amount of information to accomplish the intended purpose of the use or disclosure to be released, except when PHI is disclosed for treatment purposes. The law contemplates that providers and covered

entities will use their common sense and good judgment to determine the minimum amount of private information that is needed to accomplish the intended purpose.

6. COMPREHENSIVE SAFEGUARDS TO PROTECT PHI

6.01 SHSU Physicians will make every reasonable effort to implement safeguards to protect the confidentiality, integrity, and availability of electronic or hard copy of PHI.

6.02 SHSU Physicians appoints the Director of Clinic Operations as the Clinic Privacy and Security Official to manage the security of the PHI and oversee the development, implementation, training, maintenance of, and adherence to, all privacy policies and procedures regarding the safe use and handling of PHI in accordance with SHSU's policies, the SHSU Physician policies and procedures, applicable TSUS Rules and Regulations, and applicable state and federal law.

6.03 Workforce Training. All SHSU Physicians employees, interns, and volunteers are required to successfully complete an initial HIPAA training with assessment within 45 days of hire or appointment to intern or volunteer position. Training will be documented and maintained by the Clinic Privacy and Security Official in the SHSU Physicians HIPAA training log and/or Talent Management system, the SHSU learning and training management system.

6.04 All employees separating from SHSU Physicians are required to immediately return issued keys and/or access cards and the individual's computer login access will be disabled.

6.05 If a departing workforce member has used cryptography (i.e. encryption) on PHI, the member shall make the cryptographic keys available to appropriate management.

6.06 In the event of an emergency, SHSU Physicians shall respond in accordance with the HCC's and SHSU's Business Continuity Plans. Electronic PHI shall be protected in accordance with the SHSU Information Technology Data Backup and Recovery Policy. To the extent that PHI is maintained by a Business Associate, the Agreement with such Business Associate shall include emergency procedures.

7. PHYSICAL SAFEGUARDS TO PROTECT PHI

7.01 SHSU Physicians will monitor any accessible areas of storage and computer workstations during normal Clinic hours to guard against inadvertent or unauthorized access of PHI by those visiting the Clinic.

7.02 All access to computers is password protected, with a renewal every six (6) months. A screensaver or sleep mode will activate after fifteen (15) minutes of non-use.

7.03 SHSU Physicians employees will lock computer screens whenever their screen is not within their sight.

7.04 All SHSU Physicians portable workstations shall be securely maintained when in the possession of workforce members in accordance with SHSU IT-26 Portable Computing Policy.

7.05 Documents containing PHI will not be left visible on desks or posted where easily viewed. These documents must be secured before employees leave for the day.

7.06 Documents containing PHI will be maintained in accordance with the SHSU Record Retention Schedule and destroyed by shredding upon expiration of the period or when duplicated and no longer necessary. In the event of a conflict between this clause and another clause in this policy, this clause shall prevail.

7.07 The ~~SHSU Physician's~~ Clinic office requires an individually issued key or controlled access card.

7.08 As appropriate, all physical security access codes used to protect PHI that are known by a departing workforce member shall be deactivated or changed. For example, the PIN to a keypad lock that restricts entry to a facility containing PHI shall be changed if a workforce member who knows the PIN departs.

8. TECHNICAL SAFEGUARDS TO PROTECT PHI

8.01 SHSU Physicians securely stores and transmits all electronic and paper records with PHI.

8.02 A personal logon is required for Electronic Health Records. Passwords will not be shared among employees, and each individual has a unique login credential.

8.03 Back up data files will be generated every day and stored at an off-site location. In the event of a fire, disaster, loss or system failure occurs; the backup files will be used to restore data for clinic use.

8.04 All electronic PHI is encrypted or destroyed, as appropriate and required by law.

8.05 Any electronic communication that contains PHI will be sent via fax or encrypted email. The messages sent within the Electronic Medical Record housed by a Business Associate will; by regulation and contract conform to the HIPAA security requirements.

8.06 All computers will be cleansed to ensure all PHI is removed before it is re-used or destroyed in accordance with SHSU Media Sanitization Policy, IT-15.

9. AUDITS TO SECURE SAFEGUARDS ARE IN PLACE AND CURRENT

9.01 SHSU Physicians will have monthly and yearly audits to ensure security and safeguards are in place and up to date.

9.02 Monthly audits will be conducted by the Clinic Privacy and Security Official and logged to ensure all activity and access is appropriate and in keeping with the intent of this policy.

9.03 Each server will be protected by a firewall, virus protection, and reviewed by IT@Sam annually.

9.04 All Logs will be reviewed and maintained by the Clinic Privacy and Security Official yearly.

10. SECURITY BREACH NOTIFICATION AND MITIGATION

10.01 SHSU Physicians shall make every effort to secure an individual's PHI, including the use of encryption whenever possible.

10.02 SHSU Physicians and any Business Associates shall investigate and mitigate any security or other incidents that involve potential unauthorized access of PHI.

10.03 A breach must be immediately reported to the Clinic Privacy and Security Official who shall notify the SHSU Privacy and Security Officer. The Clinic Privacy and Security Official will maintain a record of all breach notifications and actions taken to investigate and address the breach.

10.04 In the event of a breach, SHSU Physicians shall follow the SHSU HIPAA Breach Notification Policy.

11. DOCUMENTATION OF COMPLIANCE

11.01 SHSU Physicians will maintain a current HIPAA Compliance Manual that keeps all policies, procedures, logs, and forms on-site.

11.02 Incident Reports/Complaints - Per HIPAA, SHSU Physicians patients may file a complaint regarding SHSU Physicians use and disclosure of the patient's PHI. All patient complaints will be submitted to the Clinic Privacy and Security Official for investigation and resolution.

a) The Clinic Privacy and Security Official will immediately work to resolve technical issues and disputes on specific incidents before filing a complaint form.

b) The Clinic Privacy and Security Official will log the complaint onto the Complaint Log (see Complaint Log).

c) The Clinic Privacy and Security Official will then take the necessary action to investigate and resolve the complaint to the satisfaction of the patient. If the complaint cannot be satisfactorily resolved, it will be forwarded to the Medical Director and SHSU Privacy and Security Officer for resolution.

d) Patients may file a complaint with the Secretary of HHS, and upon request shall be directed to and follow the steps provided on the Office for Civil Rights website (www.hhs.gov/ocr/hipaa).

12. PROGRAM IMPROVEMENT

12.01 The Clinic Privacy and Security Official, the SHSU Privacy and Security Officer, and the SHSU Compliance Officer shall periodically address improvement of the HIPAA Information Security and Privacy Program by ensuring that the Program is appropriate and efficient, current compliance obligations remain accurate and up-to-date, and new compliance obligations are examined and included where required or appropriate.

13. SANCTIONS

13.01 Any SHSU Physicians employee who violates this policy, any other SHSU policies or procedures or applicable System Rules and Regulations concerning PHI, or any federal or state law related to PHI, may be sanctioned. Sanctions may include additional training, curtailing or otherwise altering job responsibilities, or other disciplinary action up to and including termination of employment, termination of contract, or expulsion from school, as applicable. To determine appropriate sanctions for staff, the Clinic Privacy Official will consult with the SHSU Compliance Office and the Office of Human Resources.

13.02 SHSU shall not tolerate retaliation against any person reporting a HIPAA violation.

13.03 HIPAA is enforced by the Office for Civil Rights of the U.S. Department of Health andHuman Services and the state Attorney General. Violations may result in civil and/or criminal penalties.

Approved by:
Date:

Reviewed by:
Date: