College of Osteopathic Medicine
SAM HOUSTON STATE UNIVERSITY

Element 1.4: Governance and Program Policies

- **1.4-2c Supporting Documentation**
  - Policies for Confidentiality of Employment, Student, and Medical Records
    - SHSU Academic Policy Statement 810106 – link
    - SHSU Data Classification Policy IT-06 – link
    - SHSU HIPAA Breach Notification IT-31 – link

1. PURPOSE

This policy is established to assure compliance with the Family Educational Rights and Privacy Act of 1974 (FERPA).

2. DEFINITIONS

For purposes of this policy, Sam Houston State University ("University") provides the following definitions:

2.01 *Student* - An individual who is receiving or has received instruction in a University course, including an activity which is evaluated toward a grade such as classroom instruction, an academic internship, or a student teaching assignment.

2.02 *Educational Record* - Any record maintained by the University, an employee of the University, or an agent of the University, which is directly related to a student or former student, EXCEPT:

a. A personal record kept by a University staff person or agent, which is in the sole possession of the person who made it.

b. Employment records used only in relation to a student's employment by the University. However, the records of a student's employment are educational records when:

(1) The position in which the student is employed depends on their status as a University student; or

(2) The student receives a grade or credit based on the student's performance as an employee.

c. Records maintained by the University used only for the provision of medical, psychiatric, psychological or other recognized professional treatments that are otherwise protected by a privilege recognized by State law. In order to maintain these records separate from educational records, the University will enforce the following conditions:

(1) No person other than the physicians, psychiatrists, psychologists, or other recognized professionals providing treatment will have access to information contained in the University health records. Such records, however, may be disclosed to other persons under the procedures to meet a health and safety emergency as described in the FERPA and this policy.

(2) Personal Identifiers will be protected. This includes the individual's name; the name of the individual's parents or other family members; the individual's addresses (permanent or present); the individual's social security number; any other number or symbol which identifies the individual; a list of the individual's personal characteristics; or any other information which would make the individual's identity known and can be used to label a record as the individual's.

3. ANNUAL NOTIFICATION

The University publishes in the S*tudent Guidelines*, available on the Dean of Students' Office website, a notice to students of their rights under the FERPA. Additionally, each fall semester a notice is sent to all enrolled University students via institutional email in coordination with advising and registration. The notice will include, but not be limited to, the rights listed in section 4.02 of this policy and as follows:

3.01 The right of the student to inspect and review the student's own educational records, including reference to this policy for the procedure for exercising the right to inspect and review education records.

3.02 The right of the student to consent to disclosures of personally identifiable information contained within the student's education records, including the intent of the University to limit the disclosure of information contained in a student's educational record to the following circumstances:

a. With prior written (includes electronic) consent from the student;

b. As an item of directory information, which the student has not refused to permit the University to disclose; or

c. Under any FERPA provisions which allow the University to disclose information without the student's prior consent, including disclosure of personally identifiable information from a student's education record to other school "officials" within the

University whom the University has determined to have a "legitimate educational interest" as those terms are defined in this policy.

3.03 The right of a student to petition the University to amend or correct any part of the student's educational record, which may be inaccurate, misleading, or in violation of privacy or other rights of the student, including reference to this policy for the procedure for requesting amendment of records. When the University decides it will not amend or correct a student's record, the student's right to a hearing to present evidence that the record is inaccurate, misleading, or in violation of privacy or other rights.

3.04 The right to file a complaint with the Family Policy Compliance Office of the U.S. Department of Education concerning alleged failures by the the University to comply with the FERPA.

3.05 How to obtain a copy of this policy and the locations where a student may obtain a copy.

4. STATEMENT OF RIGHTS

4.01 The University encourages students to be aware of all of their rights under the FERPA and this policy.

Since educational records will be used repeatedly by University officials and others to make important decisions affecting students' academic programs, documentation of enrollment, and academic performance, each student should assume a personal responsibility to make certain that the student's record is complete and accurate.

4.02 This policy is intended to inform students about the University's procedures to provide students with rights to:

a. Inspect and review the student's educational records;

b. Exercise control (with some limitations as provided in 3.02) over disclosure of information contained in the student's educational records;

c. Seek to correct educational records in a hearing, if necessary, when a student believes the student's records are inaccurate, misleading, or in violation of the privacy or other rights;

d. Report violations of the FERPA to the Family Policy Compliance Office of the U.S. Department of Education; and

e. Be informed about their FERPA rights.

4.03 The President of the University has delegated authority for the oversight of educational records to designated custodians. Each custodian is responsible for the administration of this policy. Students who have concerns or questions related to this policy should contact the appropriate educational record custodian for assistance.

5. LOCATIONS OF EDUCATIONAL RECORDS

Types	Office	Custodian
Admissions Records	Admissions Office	Director, Undergraduate Admissions
Cumulative Academic Records	Registrar's Office	Registrar
Health Records	Health Center	Administrator, University Health Center
Financial Aid Records	Financial Aid Office	Director, Financial Aid
Public Safety Service Records	Public Safety Services	Director, Public Safety Services
Financial Records	Student Account Services	Director, Student Account Services
Placement Records	Career Success	Director, Career Success
Counseling Records	Counseling Center	Director, Counseling Center
Disciplinary Records	Student Life Office	Dean of Students
Advising Records	Student Advising and Mentoring Center	Director/SAM Center

6. PROCEDURE TO INSPECT EDUCATIONAL RECORDS

6.01 Students who wish to inspect and review their records should submit a written request to the record custodian. The request should identify as accurately as possible the specific records the student wishes to inspect and review, the "Location of Educational Records" as listed in section 5 above, or the custodianship of specific University officials identified by title.

6.02 If it is mutually convenient, the record custodian will allow the student to inspect the records at once. If the student cannot inspect the records immediately, the official responsible for responding to the request will arrange a time convenient to both the student and the custodian for inspecting the records. In no case will the time designated for inspection be more than 45 days after the request for inspection has been made.

6.03 When a record contains personally-identifiable information about more than one student, a requesting student may inspect only the requesting student's own information.

6.04 The University reserves the right to refuse to permit a student to inspect and review the following educational records:

a. The financial statement of the student's parents or legal guardian.

b. Statements and letters of recommendation prepared by University officials or others that were placed in the student's records before January 1, 1975, or for which the student has waived their rights of access, provided the letters and statements are related the student's admission, employment application, or receipt of an honor.

c. Those records that are excluded from the FERPA definition of educational records (see "Definitions" in Section 2).

7. FEES FOR COPIES OF RECORDS

7.01 For those educational records for which the FERPA allows the parent or student to review, the University may charge a parent or student a fee for copies of the student's educational records, unless the imposition of the fee effectively prevents the parent or student from exercising the right to inspect and review the student's education records.

For official transcripts, students will be charged per University policy. Further information can be found on the University Registrar's webpage.

7.02 Sam Houston State University reserves the right to deny transcripts or copies of records not required by the FERPA in any of the following situations:

a. The student has an unpaid financial obligation to the University;
b. There is an unresolved disciplinary action against the student; or
c. There is unresolved litigation between the student and the University.

8. DIRECTORY INFORMATION

8.01 The University designates the personally-identifiable information contained in a student's educational record listed below as "directory information" and the University may, at its discretion, disclose this information without a student's further prior written consent:

a. The student's name
b. The student's permanent address
c. The student's major
d. The student's minor
e. The student's home telephone numbers
f. The student's degrees, diplomas, and certificates and dates of award
g. The student's honors and awards
h. The student's classification
i. The student's extracurricular activities
j. Weight, height, and related information of athletic team members
k. The student's SHSU e-mail address

8.02 Students have the first twelve (12) class days in a long term or the first four (4) days in a summer term to change their directory information release status via the Buckley Amendment form located on the University Registrar's webpage.

8.03 When a student refuses to permit the University to designate an item of information for release for the directory, the Registrar shall mark the item in the student's electronic file as "confidential" and no custodian shall make disclosures without the student's prior written consent.

8.04 The appropriate custodians of records are authorized to disclose directory information.

9. USE OF STUDENT EDUCATIONAL RECORDS

9.01 All University officials will follow a strict policy that information contained in a student's educational record is confidential and may not be disclosed to third parties without the student's prior consent except as otherwise provided in this policy.

9.02 The University maintains student educational records in order for the administrative staff and the faculty to perform their proper functions to serve the student body. To

carry out their responsibilities, these officials will have access to student educational records for legitimate educational purposes.

9.03 A "University official" includes:

a. A member of The Texas State University System Board of Regents.

b. Any and all persons employed by The Texas State University System or Sam Houston State University.

c. A person under contract to The Texas State University System or Sam Houston State University to perform a specific task where, by law or contract, the System or the University has the right to control access to the educational records.

9.04 University officials who meet the criteria listed above will have access to personally-identifiable information contained in student educational records if they have a legitimate educational interest in doing so. A "legitimate educational interest" is the person's need for information to:

a. Perform an administrative task which is outlined in the official position description or contract of the individual or which is otherwise related to the individual's position and duties;

b. Perform a supervisory or instructional task directly related to the student's education; and/or

c. Perform a service or benefit for the student such as health care, counseling, student job placement, or student financial aid.

9.05 Within the general policy that University officials must secure a student's prior written consent before they disclose personally-identifiable information contained in the student's educational records, the University reserves the right for its officials to make such disclosures without the student's consent in the following circumstances:

a. To another college, university, or other academic institution of higher education in which the student seeks or intends to enroll.

b. To certain federal and state officials who request information to audit or enforce legal conditions related to federally-supported educational programs in the University.

c. To parties who provide or may provide financial aid to the student to:

(1) Establish the student's eligibility for the financial aid.

(2) Determine the amount of financial aid.

(3) Establish the conditions for the receipt of the financial aid.

(4) Enforce the terms of the agreement between the provider and the receiver of the financial aid.

d. To state and local officials or authorities to whom information is specifically required to be reported or disclosed pursuant to any state status adopted prior to November 19, 1974.

e. To organizations conducting studies for, or on behalf of, educational agencies or institutions for the purpose of developing, validating, or administering predictive tests, administering student aid programs, and improving instruction; provided that the studies are conducted in a manner which will not permit the personal identification of students and their parents by individuals other than representatives of the organization, and the information will be destroyed when no longer needed for the purposes for which the study was conducted.

f. To accrediting organizations to carry out their accrediting functions.

g. To parents/legal guardians of a student if the parents claim the student as a dependent under the Internal Revenue Code of 1954. The University will exercise this option only on the condition that evidence of such dependency is furnished to the custodian of records. It is generally held that the FERPA rights of eligible students lapse or expire upon the death of the student.

h. To comply with a judicial order or lawfully issued subpoena. The University will make a reasonable effort to notify the student before it makes a disclosure under this provision.

9.06 University officials may release education records to parties after the redaction of all personally identifiable information from the records, provided that the University official has made a reasonable determination that a student’s identity is not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information.

9.07 The University authorizes its officials to make the needed disclosures from student educational records in a health or safety emergency if the official deems:

a. The disclosure to be warranted by the seriousness of the threat to the health or safety of the student or other persons;

b. The information to be necessary and needed to meet the emergency; and
c. Time to be an important and limiting factor in dealing with the emergency.

9.08 University officials may not disclose personally-identifiable information contained in a student's educational record, except directory information or under the circumstances listed above, without with the student's prior written consent. The written consent must include:

a. A specification of the information the student consents to be disclosed;

b. The purpose for which the disclosure may be made;

c. The person or organization or the class of persons or organizations to whom the disclosure may be made; and

d. The date of the consent and, if appropriate, a date when the consent is to be terminated.

9.09 The student may obtain a copy of any record the University discloses pursuant to the student's prior written consent.

9.10 The University will not release information contained in a student's educational records, except directory information, to any third parties except its own officials, unless those parties agree that they will not disclose the information without the student's prior written consent.

10. GUIDELINES TO BE FOLLOWED WHEN HARD COPY STUDENT ACADEMIC RECORDS ARE PRINTED FROM THE UNIVERSITY'S INFORMATION RESOURCES

10.01 Access codes will be restricted to authorized University officials.

10.02 Students may obtain official transcripts from the Registrar's Office for an appropriate fee provided there is no hold on their receipt of such transcript (e.g., delinquent student loan); further, students are entitled under the State Public Information Act to an unofficial transcript.

10.03 The following third-party message appears on the hard copy of any student's academic record retained in the office of University officials in order to relieve the President and the Registrar from liability should the record fall into unauthorized hands and legal action result.

> "Confidential. Release of information contained on this document without the written consent of the person(s) identified on the document is in violation of Sec. 438 Public Law 90-247, the Family Educational Rights and Privacy Act and the Texas Public Information Act, Government Code, Chapter 552."

10.04 Said records must be destroyed when no longer needed.

11. RECORDS OF REQUEST FOR ACCESS AND DISCLOSURES MADE FROM EDUCATIONAL RECORDS

The University will maintain a record of each request granted or rejected and each disclosure of personally-identifiable information from the educational records of the student that indicates:

a. The name of the person or agency that made the request;

b. The interest the person or agency had in the information;

c. The date the person or agency made the request; and

d. Whether the request was granted and, if it was, the date access was permitted or the disclosure was made.

The University will maintain this record of disclosure as long as it maintains the student's educational record.

12. PROCEDURES TO CORRECT EDUCATIONAL RECORDS

12.01 Request for Correction - The University will permit a student to challenge the content of their educational records to ensure that records are not inaccurate, misleading, or otherwise in violation of the privacy or other rights the student. (Note: Under the FERPA, the University is permitted to refuse to consider a student's request to change the grade an instructor assigns for a course).

12.02 For purposes the procedure to seek to correct educational records, the term "incorrect" will be used to describe a record that is inaccurate, misleading, or in violation of privacy or other rights of a student. Also, in this section, the term "requester" will be used to describe a student or former student who seeks record correction.

12.03 If a student or former student discovers incorrect information in their educational records, they should informally discuss the problem with the record custodian. If the custodian finds the record is incorrect because of an obvious error, and it is a simple matter to correct it to the satisfaction of the requester, the custodian may make the change.

12.04 If the custodian does not change the record to the requester's satisfaction or the record does not appear to be obviously incorrect, the custodian will:

a. Provide the requester a copy of the questioned record at no cost; and
b. Ask the requester to initiate a written request for the change with the custodian.

12.05 The written request should at least identify the item the requester believes is incorrect and state whether it:

a. Is inaccurate, and the basis for any such contention;
b. Is misleading, and the basis for any such contention; or
c. Violates the privacy or other rights of students, and the basis for any such contention.

12.06 The record custodian will then amend the educational record of the student or refuse to amend it in whole or in part. The record custodian shall notify the requester of any refusal and advise the requester of the right to a hearing.

12.07 Upon completion of each of the steps in this section and upon timely notice of a request for hearing, the hearing will be held within a reasonable period of time, and it will be conducted by an impartial University official appointed by the President. The requester may have anyone of their choice, including an attorney, at the hearing. If the requester is not satisfied with the result of the hearing, they may file a grievance with the Family

Policy Compliance Office of the U.S. Department of Education. If the requester does not agree with the University's decision as to the interpretation of the records, the requester may file their own interpretation with the University. The requester's interpretation will be placed with their educational record and maintained by the University. The University will provide the interpretation of the student and the interpretation of the University with the educational record of the student.

APPROVED: <signed>
Alisa White, Ph.D., President

DATE: 01/03/2023

CERTIFICATION STATEMENT

This academic policy statement (APS) has been approved by the reviewer listed below and represents SHSU's Division of Academic Affairs' policy from the date of this document until superseded.

Original:	August 6, 1981	Review Cycle:	Five years*
Reviewer:	Academic Affairs Council	Review Date:	Spring 2027

Approved: <signed> Date: 12/19/2022
Michael T. Stephenson, Ph.D.
Provost and Sr. Vice President
for Academic Affairs

*****Effective January 2018, Academic Policy Statements will be reviewed on a rotating 5-year schedule. To transition to a distributed review load, some policies may be reviewed prior to the 5-year timeframe, with subsequent reviews transitioning to the 5-year schedule.

Sam Houston State University
A Member of The Texas State University System
Information Technology Services (IT@Sam)

Data Classification Policy: IT-06

PURPOSE:

Data Classification provides a framework for managing data assets based on value and associated risks and for applying the appropriate levels of protection as required by state and federal law as well as proprietary, ethical, operational, and privacy considerations. All SHSU data, whether electronic or printed, must be classified as Confidential, Protected, or Public. Consistent use of data classification reinforces with users the expected level of protection of SHSU data assets in accordance with SHSU policies.

The purpose of the Data Classification Policy is to provide a foundation for the development and implementation of necessary security controls to protect information according to its value and/or risk. Security standards, which define these security controls and requirements, may include document marking/labeling, release procedures, privacy, transmission requirements, printing protection, computer display protections, storage requirements, destruction methods, physical security requirements, access controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures.

SCOPE:

The SHSU Data Classification policy applies equally to all Data Owners and Data Custodians.

POLICY STATEMENT:

Data Owners and/or Data Custodians must classify data as follows:

1. Confidential: Sensitive data that must be protected from unauthorized disclosure or public release based on state or federal law, (e.g. the Texas Public Information Act, FERPA, HIPPA) and other constitutional, statutory, judicial, and legal agreements. Examples of Confidential data may include, but are not limited to:

    a. Personally identifiable information such as a name in combination with Social Security Number (SSN) and/or financial account numbers
    b. Student education records such as posting student identifiers and grades
    c. Intellectual property such as copyrights, patents and trade secrets
    d. Medical records

2. Protected: Sensitive data that may be subject to disclosure or release under the Texas Public Information Act but requires additional levels of protection. Examples of Protected data may include but are not limited to SHSU:

    a. Operational information
    b. Personnel records
    c. Information security procedures
    d. University-related research
    e. SHSU internal communications

3. Public: Information intended or required for public release as described in the Texas Public Information Act.

DEFINITIONS:

Confidential Data: Information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g. the Texas Public Information Act, and other constitutional, statutory, judicial, and legal agreement requirements).

Data Classification: Classifying data according to their category of Confidential, Protected or Public.

Data Custodian: The person responsible for overseeing and implementing physical, technical, and procedural safeguards specified by the data owner.

Data Owner: Departmental position responsible for classifying business data, approving access to data, and protecting data by ensuring controls are in place.

Protected Data: Sensitive data that requires a level of protection but may be subject to disclosure or release – Public Information Act.

Public Data: Information intended or required for public release.

Related Policies, References and Attachments:

An index of approved IT@Sam policies can be found on the SHSU Information Technology Services Policies website at http://www.shsu.edu/intranet/policies/information_technology_policies/index.html. Reference materials, legal compliance guidelines, and policy enforcement are available in the IT-00 Policy Compliance Document. The SHSU Information Security Program and SHSU Information Security User Guide are also available on the Information Technology Services Policies website.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 30, 2015
Approved by: President's Cabinet, June 27, 2011
Next Review: November 1, 2016

IT Policy IT-31

HIPAA BREACH NOTIFICATION POLICY

1. GENERAL

Sam Houston State University (SHSU), a HIPAA Hybrid Entity, and its Health Care Components (HCCs) are accountable to the Department of Health and Human Services and to individuals for the proper safeguarding of the private information entrusted to their care.

2. PURPOSE

To enable HCCs in accordance with 45 C.F.R. § 164.400 et seq. to comply with applicable state and federal laws and regulations governing notice to affected individuals in the event of a breach of patient privacy.

3. DEFINITIONS

3.01 Business Associate. A person or entity that performs a function or service that creates, receives, maintains, or transmits protected health information for a HIPAA covered entity. A Business Associate may be a department within SHSU or an unaffiliated third party.

3.02 Covered Functions. Performance of activities that makes an entity a health plan, health care provider, or health care clearinghouse.

3.03 Covered Entity. Entities, to include designated SHSU Health Care Components, that operate a health plan, health care clearinghouse, or provide health care services and transmits protected health care information in electronic form.

3.04 SHSU Health Care Component (HCC). A department that either performs covered functions or would meet the definitions of a covered entity or business associate if it were a separate legal entity.

3.05 Hybrid Entity. A single legal entity whose activities include both covered and non-covered functions and that designates one or more departments as HCCs.

3.06 Protected Health Information (PHI). Individually identifiable health information created, received, maintained or electronically transmitted by a covered entity. Protected health information excludes individually identifiable health information:

a) in education records covered by the Family Educational Rights and Privacy Act (FERPA).

b) in employment records held by a HCC in its role as employer; and

c) regarding a person who has been deceased for more than 50 years.

(See 45 C.F.R. § 160.103 and § 164.105).

4. APPLICATION

4.01 HCC Personnel. This Policy applies to all HCC personnel, including HCC administration, medical staff, clinical and administrative personnel, volunteers, and HCC's business associates.

4.02 Breaches of (PHI). This Policy applies only if there is a breach of a patient's individually identifiable health information. For purposes of this Policy, a breach is presumed if there is an unauthorized access, acquisition, use or disclosure of unsecured PHI unless (1) the HCC can

demonstrate that there is a low probability that the information was compromised based a risk assessment of certain factors described below, or (2) the situation fits within one of the following exceptions to the breach notification rule:

a) Any unintentional acquisition, access, or use of PHI by a member of the HCC's workforce or a person acting under HCC's authority if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in violation of the HIPAA privacy rules.

b) Any inadvertent disclosure by a person who is authorized to access PHI at the HCC to another person authorized to access patient information at the HCC or its business associate and the PHI disclosed is not further used or disclosed in violation of the HIPAA privacy rules.

c) A disclosure of PHI if the HCC has a good faith belief that the person to whom the disclosure was made would not reasonably have been able to retain such information.

d) The use or disclosure involves PHI that has been "secured" according to standards published by HHS. Currently, this only applies to electronic patient information that has been properly encrypted consistent with standards published by HHS. HHS will publish future guidance for securing patient information on its website, https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html. (45 C.F.R. § 164.404-408).

5. PROCEDURE

5.01 Mitigating Potential Breaches. If HCC personnel improperly access, acquire, use or disclose PHI and immediate action may cure or mitigate the effects of such use or disclosure, HCC personnel should take such action. For example, if HCC personnel improperly access or acquire PHI, they should immediately stop, close, and/or return the information. If HCC personnel mistakenly disclose PHI to the wrong person, they should immediately request the return of the information and confirm that no further improper disclosures will be made. If the potential breach is significant or requires further action to mitigate its effects, HCC personnel should immediately contact their supervisor or the SHSU Privacy and Security Officer for assistance and direction.

5.02 Reporting Potential Breaches to the SHSU Privacy and Security Officer. HCC personnel shall immediately report any suspected breach of PHI in violation of the HIPAA Rules or the HCC's privacy policies to the SHSU Privacy and Security Officer. Failure to timely report suspected breaches may result in sanctions as described below.

5.03 Investigating Potential Breaches. The SHSU Privacy and Security Officer shall promptly investigate any reported privacy breach or related patient complaint to determine whether there has been a "breach" of PHI as defined above, and if so, how notice should be given. The SHSU Security and Privacy Officer shall document his or her investigation and conclusions, including facts relevant to the risk assessment. (45 C.F.R. §§ 164.414 and 164.530). To determine whether a breach has occurred, the SHSU Privacy and Security Officer shall consider:

a) Whether the alleged breach involved PHI. (45 C.F.R. § 164.402)

b) Whether the alleged breach violates the HIPAA Privacy Rule. Disclosures that are incidental to an otherwise permissible use or disclosure (e.g., a patient overhears a physician speaking with another patient, or sees information about another patient on a whiteboard or sign-in sheet) do not violate the privacy rule so long as

the HCC implemented reasonable safeguards to avoid improper disclosures. (45 C.F.R. § 164.502)

c) Whether there is a low probability that the protected health information has been compromised considering relevant factors, including at least the following: (1) the nature and extent of the information involved; (2) the unauthorized person who used or received the information; (3) whether the information was actually acquired or viewed; and (4) the extent to which the risk to the information has been mitigated. (45 C.F.R. § 164.402)

d) Whether the alleged breach fits within one of the exceptions identified in Section 4.0.2, above. (45 C.F.R. § 164.402)

5.04 Notice – In General. If the SHSU Security and Privacy Officer determines that a breach of unsecured PHI has occurred, the affected HCC Administration shall notify the patient, HHS, and the media (if required) consistent with this Policy and the requirements of 45 C.F.R. §§ 164.404- .408 et seq. Any notice provided pursuant to this Policy must be approved and directed by SHSU Security and Privacy Officer and/or the affected HCC Administration. No other HCC personnel are authorized to provide the notice required by this Policy unless expressly directed by the SHSU Security and Privacy Officer and/or the affected HCC Administration.

5.05 Notice to Individuals. If a breach of PHI has occurred, the affected HCC Administration shall notify the affected patient(s) without unreasonable delay and in no case later than 60 days after the breach is discovered. The notice shall include to the extent possible: (1) a brief description of what happened (e.g., the date(s) of the breach and its discovery); (2) a description of the types of information affected (e.g., whether the breach involved names, social security numbers, birthdates, addresses, diagnoses, etc.); (3) steps that affected patients should take to protect themselves from potential harm resulting from the breach; (4) a brief description of what the HCC is doing to investigate, mitigate, and protect against further harm or breaches; and (5) contact procedures for affected persons to ask questions and receive information, which shall include a toll-free telephone number, e-mail address, website, or postal address at which the person may obtain more information. The notice shall be written in plain language. (45 C.F.R. § 164.404)

a) Notice by Mail or Email. The affected HCC Administration shall notify the patient by first-class mail to the patient's last known address. If the patient agrees, the notice may be sent by e-mail. The notice may be sent by one or more mailings as information is available. (45 C.F.R § 164.404(d))

b) Substitute Notice. If the affected HCC lacks sufficient contact information to provide direct written notice by mail to the patient, the affected HCC Administration must use a substitute form of notice reasonably calculated to reach the patient. (45 C.F.R. § 164.404(d))

1) Fewer than 10 affected patients. If there is insufficient contact information for fewer than 10 affected patients, the affected HCC Administration shall provide notice by telephone, e-mail, or other means of written notice. If the affected HCC lacks sufficient information to provide any such substitute notice, the SHSU Security and Privacy Officer shall document same. (45 CFR § 164.404(d)(2)(i))

2) 10 or more affected patients. If there is insufficient contact information for 10 or more affected patients, The affected HCC Administration shall do one of the following: (1) post a conspicuous notice on the home page of affected HCC's website for 90 days with a hyperlink to the additional

information required to be given to individuals as provided above; or (2) publish a conspicuous notice in major print or broadcast media in the area where affected patients reside. The notice must include a toll-free number that remains active for at least 90 days so individuals may call to learn whether their PHI was breached. (45 C.F.R. § 164.404(d)(2)(ii))

c) Immediate Notice. If the SHSU Security and Privacy Officer believes that PHI is subject to imminent misuse, the affected HCC Administration may provide immediate notice to the patient by telephone or other means. Such notice shall be in addition to the written notice described above. (45 C.F.R. § 164.404(d)(3))

5.06 Deceased Patient; Notice to Next of Kin. If the patient is deceased and the affected HCC knows the address for the patient's next of kin or personal representative, the affected HCC Administration shall mail the written notice described above to the next of kin or personal representative. If the affected HCC does not know the address for the next of kin or personal representative, then the affected HCC is not required to provide any notice to the next of kin or personal representative. The SHSU Security and Privacy Officer shall document the lack of sufficient contact information. (45 C.F.R. § 164.404(d)(1))

5.07 Notice to HHS. If the SHSU Security and Privacy Officer determines that a breach of PHI has occurred, the affected HCC Administration shall also notify HHS of the breach as described below.

a) Fewer than 500 Affected Patients. If the breach involves the PHI of fewer than 500 persons, the affected HCC Administration may either (1) report the breach immediately to HHS as described in subsection (b), or (2) maintain a log of such breaches and submit the log to HHS annually within 60 days of the end of the calendar year. Instructions for maintaining and submitting the log are posted on the HHS website. (45 C.F.R. § 164.408(c))

b) 500 or More Affected Patients. If the breach involves 500 or more persons, the affected HCC Administration shall notify HHS of the breach at the same time the affected HCC Administration notifies the patient or next of kin. Instructions for maintaining and submitting the log are posted on the HHS website. (45 C.F.R. § 164.408(b))

5.08 Notice to Media. If a breach of PHI involves more than 500 residents in a state, the affected HCC Administration will also notify prominent media outlets in such state. The notice shall be provided without unreasonable delay but no later than 60 days after discovery of the breach. The notice shall contain the same elements of information as required for the notice to the patient described above. The SHSU Security and Privacy Officer shall work with affected HCC Administration to develop an appropriate press release concerning the breach. (45 C.F.R. § 164.406)

5.09 Notice from Business Associate. If an HCC's business associate discovers a breach of PHI, the business associate shall immediately notify the SHSU Security and Privacy Officer of the breach. The business associate shall, to the extent possible, identify each person whose information was breached and provide such other information as needed by the HCC to comply with this Policy. Unless the SHSU Security and Privacy Officer directs otherwise, the affected HCC Administration shall notify the patient, HHS, and, in appropriate cases, the media as described above. (45 C.F.R. § 164.410)

5.10 Delay of Notice Per Law Enforcement's Request. The affected HCC Administration shall delay notice to the patient, HHS, and the media if a law enforcement official states that the notice would impede a criminal investigation or threaten national security. If the law enforcement official's statement is in writing and specifies the time for which the delay is required, the

affected HCC Administration shall delay the notice for the required time. If the law enforcement official's statement is verbal, the SHSU Security and Privacy Officer shall document the statement and the identity of the law enforcement official, and the affected HCC Administration shall delay the notice for no more than 30 days from the date of the statement unless the officer provides a written statement confirming the need and time for delay. (45 C.F.R. § 164.412)

5.11 Training Employees. The HCC shall train its workforce members concerning this Policy, including members' obligation to immediately report suspected privacy violations. The SHSU Security and Privacy Officer shall ensure that this Policy is included in training given to new workforce members, and thereafter in periodic training as relevant to the workforce members' job duties. (45 C.F.R. § 164.530)

5.12 Sanctions. HCC personnel may be sanctioned for a violation of this Policy, including but not limited to the failure to timely report a suspected privacy violation. HCC may impose the sanctions it deems appropriate under the circumstances, including but not limited to termination of employment and report the sanctions to the SHSU Security and Privacy Officer. (45 C.F.R. § 164.530)

5.13 Documentation. The SHSU Security and Privacy Officer shall prepare and maintain documentation required by this Policy for a period of six (6) years, including but not limited to reports or complaints of privacy violations; results of investigations, including facts and conclusions relating to the risk assessment; required notices; logs of privacy breaches to submit to HHS; sanctions imposed; etc. (45 C.F.R. § 164.530)

6. POLICY REVIEW

SHSU shall regularly review this policy at least every two (2) years. The Policy shall be reviewed for consistency with other University policies and the policies of The Texas State University System, which shall govern in the event of a conflict.

Approved by: President's Cabinet
Date: October 7, 2019