Element1.4: Governance and Program Policies

- x 1.4-2cSupporting Documentation
  - o Policies for Confidentiality of Employment, Student, and Medical Records
    - ¾ SHSU Academic Policy Statement 810106 – link
    - ¾ SHSU Data Classification Policy IT-06 – link
    - ¾ ^ , ^ h , / W ZŒE } š]v / d r ï í – 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 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

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
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.

8. DIRECTORY INFORMATION

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

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.

Sam Houston State University
Academic Policy Statement 810806

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.

10.01 Access codes will be restricted to authorized University officials.

12.01 Request for Correction - The University will permit a student to challenge the content

Policy Compliance Office of the U.S. Department of Education.

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 ² 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: 3UHVLGHQW

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

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

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 ev