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