STANDARD ADMINISTRATIVE PROCEDURE

16.99.99.M0.15 Breach or Unauthorized Disclosure of Protected Health Information

Approved April 27, 2020
Next scheduled review: April 27, 2025

SAP Statement

This standard administrative procedure applies to the Texas A&M University (TAMU) components that have been designated as a TAMU HIPAA Health Care Component (TAMU HIPAA HCC) in Standard Administrative Procedure 16.99.99.M0.01, *Designation as a Hybrid Entity*.

Definitions

Click to view Definitions

Official Procedure

1. RESPONSIBILITIES

    1.1. TAMU HIPAA HCCs are required by law to protect the privacy of health information that may reveal the identity of a patient. If a breach of certain types of individually identifiable health information occurs, the TAMU HIPAA HCC at issue is required to provide notification to certain individuals and entities pursuant to Subtitle D of the Health Information Technology for Economic and Clinical Health Act, which is Title XIII of the American Recovery and Reinvestment Act of 2009 and any regulations promulgated thereunder (HITECH). The TAMU HIPAA HCC may have additional reporting obligations under other federal laws and state breach notification laws. Those obligations are not addressed in this procedure.

2. PROCESS

    2.1. Background

2.1.1. Breach or unauthorized disclosure means the acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA and which compromises the security or privacy of the PHI.

2.1.1.1. Exclusions

- Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a Hybrid Entity or a Business Associate, 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 a manner not permitted under HIPAA.
- Any inadvertent disclosure by a person who is authorized to access PHI at a Hybrid Entity or Business Associate to another person authorized to access PHI at the same Hybrid Entity or Business Associate, or organized health care arrangement in which the Hybrid Entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA.
- A disclosure of PHI where a Hybrid Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2.1.1.2. Risk Assessment

- An impermissible acquisition, access, use, or disclosure of PHI is presumed to be a breach or unauthorized disclosure unless the Hybrid Entity or Business Associate demonstrates that there is a low probability that PHI has been compromised based on a risk assessment of at least the following factors:
  - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
  - The unauthorized person who used the PHI or to whom the disclosure was made;
  - Whether the PHI was actually acquired or viewed; and
  - The extent to which the risk to the PHI has been mitigated.

2.1.1.3. Breach or Unauthorized Disclosure

- TAMU HIPAA HCCs will implement procedures and practices to protect against breaches of PHI.

- In the event of a breach or Unauthorized Disclosure of PHI, TAMU HIPAA HCCs **must**:

    - Immediately notify the TAMU Privacy Officer;
    - Cooperate with the TAMU Privacy Officer, and others in the course of the investigation of the breach or unauthorized disclosure; and;
    - In coordination with the TAMU Privacy Officer, initiate corrective action plans or other remediation or mitigation to prevent recurrence of the breach or similar breaches.
- When applicable, the HIPAA Breach Team (see below) will implement the breach protocol (Protocol), which outlines the necessary steps to take in the event that any confidential or restricted data is compromised.
- This Protocol includes assembling key TAMU stakeholders and is also used to perform the risk assessment as identified under 45 CFR § 164.402
- Unless the PHI in question is indecipherable, unreadable, or unusable, the TAMU Privacy Officer will determine through a risk assessment whether the incident meets the definition of breach under 45 CFR § 164.402.
- The HIPAA Breach Team shall consist of, at a minimum:
    - TAMU Privacy Officer and/or his/her designees;
    - CISO and/or his/her designees;
    - Representative(s) from the TAMUS Office of General Counsel (OGC); and
    - Any other individuals identified as necessary participants.

2.1.1.4. Reporting

- To OCR: When necessary, the TAMU Privacy Officer will report breaches involving TAMU HIPAA HCCs to the Secretary of the Department of Health and Human Services (HHS) and coordinate any or all investigations the Secretary may perform or cause to be performed.
- To Others: The TAMU Privacy Officer will work with the CISO or designated TAMU point-of-contact for breach notifications to notify the TAMU Communications to coordinate notification to individuals and notification to the media, as necessary.

<u>Breaches affecting less than 500 individuals:</u>

- Breach information must be added to the breach log by the TAMU Privacy Officer;
- The TAMU Privacy Officer will work with designated TAMU point-of-contact for breach notifications to affected individuals within sixty (60) calendar days after discovery of a breach; and
- The TAMU Privacy Officer must submit the breach log to OCR no later than February 1 of each calendar year.

Breaches affecting more than 500 individuals:

- Breach information must be added to the breach log by the TAMU Privacy Officer;
- The TAMU Privacy Officer will work with designated TAMU point-of-contact for breach notifications to affected individuals;
- The TAMU Privacy Officer will work with the designated TAMU point-of-contact for breach notifications to notify the TAMU Communications to coordinate notification to the media; and
- Notice shall be provided to the Secretary of HHS by the TAMU Privacy Officer without unreasonable delay and in no case later than sixty (60) calendar days in the case of a single Breach event involving 500 or more individuals, regardless of the location of the patients.

2.1.1.5. Role of the TAMU Privacy Officer:

- The TAMU Privacy Officer will work with the TAMU HIPAA HCC and the CISO to investigate the circumstances of the breach and make recommendations regarding a corrective action plan or other remediation.

2.1.1.6. Role of Information Security Office:

- The Information Security Office collaborates with the TAU HIPAA HCC and with the TAMU Privacy Officer to investigate the circumstances of the breach and make recommendations regarding a corrective action plan or other remediation. The Information Security Office may recommend appropriate remediation action, provide additional training to staff and recommend other process improvements as necessary to remediate the breach and prevent recurrences.

3. VIOLATIONS

The Privacy Officer has general responsibility for implementation of this procedure. Employees who violate this procedure will be subject to disciplinary action up to and including termination of employment. Anyone who knows or has reason to believe that another person has violated this procedure should report the matter promptly to his or her supervisor or the Privacy Officer. All reported matters will be investigated and, where appropriate, steps will be taken to remedy the situation. Where possible, every effort will be made to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this procedure will itself be considered a violation of this procedure that may result in disciplinary action up to and including termination of employment.

Contact Office

Office of University Risk, Ethics, and Compliance