

**THE TEXAS A&M UNIVERSITY SYSTEM
HEALTH SCIENCE CENTER INTERNAL POLICIES**

**16.99.99.Z0.30 Disposal of Documents and Media Containing
Electronic Protected Health Information Internal Policy**

Approved January 26, 2011

1. GENERAL/OVERVIEW

This policy applies to TAMHSC health care providers, its participating physicians and clinicians, employees and business units who provide management, administrative, financial, legal, and operational support to or on behalf of the health care provider and has been designated as a member of the TAMHSC Health Care Component. This policy pertains to protected health information covered by the TAMHSC Health Care Component's Notice of Privacy.

2. INTERNAL POLICY/RESPONSIBILITIES

The TAMHSC Health Care Component has a duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. The purpose of the policy is to comply with the HIPAA Privacy & Security Rule's requirements pertaining to the destruction¹ of documents and other materials containing PHI and the receipt, tracking and removal of hardware and electronic media that contain ePHI.

3. PROCESS

This policy defines the guidelines and procedures that must be followed when disposing of information containing PHI and ePHI. All supervisors are responsible for enforcing this policy.

3.3 Destruction of Paper Copies and Original Documents (Day-to-Day Disposal).

- 3.1.1 Any printed material (e.g., faxes, printed emails, informal notes about patients; patient identification stickers) containing PHI must not be discarded in trash bins, unsecured recycle bins or other publicly accessible locations. Instead this information must be personally shredded or placed in secured shredder bins. The TAMHSC Health Care Provider shall provide users with access to shredders or secured shredder bins for proper disposal of confidential printouts containing PHI disposal of Documents/Materials Containing PHI.

- 3.1.2 The user may elect to use either shredding or secured shredder bins, as long as the destruction is in accordance with this policy. It is the individual's responsibility to ensure that the document has been secured or destroyed. It is the supervisor's responsibility to ensure that their employees are adhering to the policy.
- 3.1.3 After documents have reached their retention period according to the State of Texas Record Retention Schedule, all PHI must be securely destroyed.
- 3.1.4 The TAMHSC Health Care Provider shall dispose of patient identification cards and wrist bands according to stated protocol.

3.2 Destruction of X-ray film.

- 3.2.1 The State of Texas Record Retention Schedule is used to determine the schedule for X-ray film destruction.
- 3.2.2 X-rays to be destroyed are handled by the TAMHSC Health Care Provider designee and an outside firm does final destruction using secure methods.

3.3 PHI Disposal in Regulated Medical Waste.

- 3.3.1 Red Bag Waste must be placed in regulated medical waste bins.
- 3.3.2 All regulated medical waste trash is incinerated using secure methods.

3.4 Documentation of PHI Disposal.

- 3.4.1 Unless destroyed by the TAMHSC Health Care Provider, the destruction of PHI shall be performed by certified destruction service who must provide a certificate of destruction.
- 3.4.2 If TAMHSC Health Care Provider personnel undertake the destruction of the records, TAMHSC Health Care Provider personnel must use the TAMHSC Health Care Component records destruction form.
- 3.4.3 The record schedule must be found in the Records Retention Manual for the department requesting destruction of the records. If the record retention schedule is not found, please contact the TAMHSC Health Care Provider Records designee.
- 3.4.4 Records cannot be destroyed without the approval of the State Records Administrator. Please contact the Office of Vice President of Finance and Administration.

3.4.5 If a certified shredding company is utilized for the final destruction of the records, the company must provide the TAMHSC Health Care Provider with a manifest of destruction that contains the following information:

3.4.5.1 Date of destruction;

3.4.5.2 Method of destruction;

3.4.5.3 Description of the disposed records;

3.4.5.4 Inclusive dates covered;

3.4.5.5 A statement that the records have been destroyed in the normal course of business;

3.4.5.6 The signatures of the individuals supervising and witnessing the destruction; and

3.4.5.7 The TAMHSC Health Care Provider and Privacy Officer will maintain destruction documents permanently.

3.5 Hardware.

3.5.1 The TAMHSC Health Care Provider shall follow procedures established by the information Security Officer and the Office of Information Technologies related to receipt, removal, storage, re-use and disposal of hardware.

3.5.2 Hardware shall be controlled and accounted for at all times in accordance with TAMHSC protocol.

3.5.3 All hardware shall be assigned an owner.

3.5.4 There shall be a record of the movements of all hardware containing ePHI, the owner and the designated individual(s) responsible for the movement.

3.5.5 The movement of hardware shall be authorized and logged by the TAMHSC Health Care Component designee prior to the hardware and electronic media entering or leaving a facility.

3.5.6 The TAMHSC Health Care Provider designee shall be accountable for hardware while in transit between facilities.

3.5.7 Hardware shall be properly logged and disposed of when no longer used.

3.5.8 ePHI shall be removed from hardware before it is made available for reuse.

3.5.9 A retrievable, exact copy of ePHI, (when needed or requested) shall be created before any movement of hardware.

3.6 Electronic Media.

3.6.1 Electronic media containing PHI shall be physically destroyed when no longer used or no longer needed.

3.6.2 An inventory shall be maintained by the TAMHSC Health Care Provider.

4 VIOLATIONS

The Privacy Officer has general responsibility for implementation of this policy. Employees who violate this policy 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 policy 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 policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment.

OFFICE OF RESPONSIBILITY

Vice President of Finance and Administration

ⁱ HIPAA Code: §164.310(d) (1), §164.310(d) (2)