HIPAA Security Rule

Tulane University Disposal Policy

Department: Technology Services	**Policy Description:** Disposal Policy (R)
Standard: Device and Media Controls	**Section:** 164.310(d)(1)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-30

PURPOSE

The purpose of this policy is to implement procedures to address the final disposition of e-PHI, and the hardware or electronic media on which it is stored.

SCOPE

This policy applies to Tulane University Medical Group, its participating physicians and clinicians, and all University employees and business units who provide management, administrative, financial, legal, and operational support to or on behalf of Tulane University Medical Group and have been designated as part of the Tulane University HIPAA Health Care Component.

POLICIES AND PROCEDURES

Tulane University disposes of e-PHI when no longer needed, as well as the hardware and electronic media on which it is stored, by completely and irreversibly deleting e-PHI and preventing future access to it. Types of hardware and electronic media that require adequate secure disposal include:

- Computers (desktops and laptops)
- Floppy disks
- Backup tapes
- CD-ROMs
- Zip drives
- Hard drives
- Flash memory
- Other portable storage devices

Tulane University conducts a periodic inventory to identify hardware and electronic media which contains e-PHI, creating a master inventory list. The inventory list is stored in a secure manner with the Security Officer and updated upon the disposal of any components containing e-PHI. The final disposal of e-PHI and hardware and electronic media on which e-PHI is stored is logged and tracked, including the following information:

- Date and time of disposal
- Who administered the disposal
- Description of the e-PHI being disposed of
- Description of any hardware and electronic media being disposed of

- Description of what method was used for the disposal

Tulane University takes reasonable and appropriate steps, prior to disposal, to completely and permanently remove e-PHI prior to reusing any hardware or electronic media on which e-PHI is stored. The Security Officer must approve any erasable tools to be used in this process, and workforce members must take reasonable steps to ensure that these tools are used properly as specified in Tulane University's ***Media Re-use*** policy.

Where hardware and electronic media on which e-PHI is stored is to be disposed of permanently, Tulane University ensures that the data are physically destroyed and that any steps taken are documented as laid out above. All labels are removed from such data prior to disposal.

RESPONSIBILITIES:

The Security Officer is ultimately responsible for ensuring the implementation of the requirements of the ***Disposal*** 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 Security 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.

IMPLEMENTATION SPECIFICATION:

§ 164.310 Physical safeguards.

(a) A covered entity must, in accordance with § 164.306:
(d)(1) Standard: **Device and media controls**. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.
(2) Implementation specifications:
(i) **Disposal** (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.