HIPAA Security Rule

Tulane University Accountability Policy

Department: Technology Services	**Policy Description:** Accountability (A)
Standard: Device and Media Controls	**Section:** 164.310(d)(1)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-32

PURPOSE

The purpose of this policy is to maintain a record of the movements of hardware and electronic media and any person responsible therefore.

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 has established and maintains a complete, accurate and current inventory of hardware and electronic media on which e-PHI is stored and uses that inventory to log and track the movement of such hardware and electronic media. Protection of organizational assets is maintained through each asset's life cycle, beginning with purchasing and ending with final disposal. Data Center operators keep the log of e-PHI equipment movement.

The movement of hardware, electronic media and devices includes the receipt, removal, storage and/or disposal of e-PHI Systems. Tulane University documents the identity of workforce members who move the hardware or electronic media on which e-PHI is stored into, out of and within Tulane University.

Hardware and electronic media on which e-PHI is stored that is logged and tracked pursuant to this policy includes:

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

RESPONSIBILITIES:

The Security Officer is ultimately responsible for ensuring the implementation of the requirements of the ***Accountability*** 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:
(iii) **Accountability** (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.