HIPAA Security Rule

Tulane University Data Backup and Storage Policy

Department: Technology Services	**Policy Description:** Data Backup and Storage (A)
Standard: Device and Media Controls	**Section:** 164.310(d)(1)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-33

PURPOSE

The purpose of this policy is to create a retrievable, exact copy of e-PHI, when needed, before the movement of equipment.

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

In addition to the routine backup of information as part of the ***Data Backup*** plan, Tulane University makes exact, retrievable backup copies of e-PHI as needed before movement of equipment. In addition, all reasonable steps are taken to ensure that e-PHI that is backed up in connection with the movement of any required systems can be recovered following a disaster or other emergency or a failure of the equipment during movement.

Tulane University stores critical backed-up data and records of the backup copies and restoration procedures in a secure remote location, within sufficient distance from the facilities to allow for prompt retrieval in the event of a disaster or other emergency. Tulane University ensures that the appropriate access controls are implemented to only allow authorized access to all such backed-up data. All backup copies of e-PHI are provided with appropriate physical and environmental protections while stored at the remote location.

Tulane University keeps 10 days of full backup tapes in a secure storage within the data center. In addition, the most current full backup tapes are kept in a vault at the Security Center near the facility.

Tulane University tests the copy of the data to make sure the copy of the data is exact and retrievable. In addition, Tulane University runs periodic tests of all backup and restoration procedures for equipment on which e-PHI is stored.

Owners of personal computers and other portable devices such as laptops and PDAs must backup all e-PHI located on these workstations and devices daily and store the backup media in a safe place so that the backup can be accessed easily in an emergency.

RESPONSIBILITIES:

The Security Officer is ultimately responsible for ensuring the implementation of the ***Data Backup and Storage*** 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:
(iv) **Data backup and storage** (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.