HIPAA Security Rule

Tulane University Data Backup Plan

Department: Technology Services	**Policy Description:** Data Backup Plan (R)
Standard: Contingency Plan	**Section:** 164.308(a)(7)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-17

PURPOSE

The purpose of this policy is to establish and implement procedures to create and maintain retrievable exact copies of e-PHI.

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 backs up e-PHI Systems to create exact and retrievable copies of e-PHI daily. E-PHI Systems for which the data backup plan procedure applies include:

- Hardware – Tulane University Medical Group Faculty Plans IDX System

Tulane University ensures that exact up-to-date copies of e-PHI can be recovered in the event that e-PHI Systems are damaged by or during a disaster or other emergency. Backup procedures are described in FPP-14, IDX Policy for System Back-up Tapes. The tapes are reformatted for re-use until they reach maximum lifetime according to the manufacture's specification. They are then destroyed in the manner set forth in the ***Disposal*** policy.

Users of personal computers and other portable devices such as laptops and PDAs must backup all e-PHI located on these workstations daily as set forth in the ***Workstation Security*** document**.**

RESPONSIBILITIES:

The Security Officer is responsible for implementing the requirements of the ***Data Backup*** plan. Authorized workforce members, as defined above, are responsible for ensuring that e-PHI Systems are backed-up according to schedule, disposing of backup systems after an appropriate amount of time and testing backup data and the restoration procedures. Authorized workforce members are trained in all procedures necessary to comply with 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 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:

§ 164.308 Administrative safeguards.

(a) A covered entity must, in accordance with § 164.306:
(7)(i) Standard: **Contingency plan**. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
(ii) Implementation specifications:
(A) **Data backup plan** (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.