HIPAA Security Rule

Tulane University Emergency Mode Operation Plan

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

PURPOSE

The purpose of this policy is to establish and implement as needed procedures to enable continuation of critical business processes for protection of the security of electronic protected health information (e-PHI) while operating in an emergency mode.

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 Medical Group follows TUHC Policy 4.18, Computer Downtime Policy and Procedure, updated 12/1/04 as its emergency mode operation plan for the IDX system.

As described in the ***Information Security Strategy*** policy, Tulane University has determined that the e-PHI stored in locations other than the IDX system, such as personal computers or other portable devices (e.g., laptops and PDAs), generally is not as critical to the day-to-day operation of Tulane University as the e-PHI on the IDX system. Access to e-PHI stored in locations other than the IDX system would not be necessary to enable continuation of critical business processes during an emergency.

RESPONSIBILITIES:

The Security Officer will be responsible for implementing the requirements of the ***Emergency Mode Operation*** plan.

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:
(C) **Emergency mode operation plan** (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.