HIPAA Security Rule

Tulane University Testing and Revision Procedure

Department: Technology Services	**Policy Description:** Testing and Revision Procedure(A)
Standard: Contingency Plan	**Section:** 164.308(a)(7)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-20

PURPOSE

The purpose of this policy is to implement procedures for periodic testing and revision of contingency plans.

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 periodically tests its written contingency plans to discover weaknesses and revises the documentation of these plans based on the results of the tests. These testing and feedback mechanisms are the key to successful contingency planning.

The following types of tests are performed as part of Tulane University's contingency plans:

- *Limited scope test* – Test of one or more components of the ***Disaster Recovery*** plan to identify and mitigate weaknesses (e.g. backup of e-PHI on a specific system, bring backup system online and attempt to restore data and new connection)
- *Paper test* – detailed walk through of ***Disaster Recovery*** plan

Tulane University ensures that the ***Disaster Recovery*** and ***Emergency Mode Operation*** plans remain current, active and effective. In addition, all equipment necessary to the smooth operation of the contingency plan is tested.

The Security Officer organizes sufficient awareness and training of all personnel on how to react in the event of a disaster or other business interruption. This training is updated as necessary to reflect revisions in the contingency plans.

Testing results are reported to the Security Officer, who reviews the results and recommends revisions to the plans, as necessary, to address any issues. In addition, other events such as changes to the physical or technical infrastructure; employee responsibilities and/or internal or external threats may necessitate modifications to the contingency plan.

Base on our Risk Analysis, this policy only applies to the IDX system.

RESPONSIBILITIES:

The Security Officer will be responsible for implementing the requirements of the ***Testing and Revision*** procedures.

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:
(D) **Testing and revision procedures** (Addressable). Implement procedures for periodic testing and revision of contingency plans.