# HIPAA Security Rule

## Tulane University Disaster Recovery Plan

| | |
|---|---|
| **Department:** Technology Services | **Policy Description:** Disaster Recovery Plan (R) |
| **Standard:** Contingency Plan | **Section:** 164.308(a)(7) |
| **Approved:** April 19, 2005 | **Revised:** |
| **Effective Date:** April 20, 2005 | **Policy Number:** TS-18 |

**PURPOSE**

The purpose of this policy is to establish and implement as needed procedures to restore any loss of data.

**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 developed and instituted this ***Disaster Recovery*** plan relating to the recovery of any lost, damaged or corrupted e-PHI for the IDX system in the event of a disaster or other emergency. Tulane University provides training and awareness on this ***Disaster Recovery*** plan to the necessary workforce members on an ongoing basis and maintains a copy of the plan at the secured location where the backup e-PHI systems are stored. The specific locations/sites and critical systems that are a part of the ***Disaster Recovery*** plan are detailed in the ***Data Backup*** plan.

*Assumptions*
The ***Disaster Recovery*** plan is based on the following assumptions, derived from the results of the ***Risk Analysis***:

- That the needed personnel and resources are available for disaster preparation and response;
- That this document and all vital records are stored in a secure off-site location and not only survive the disaster but are accessible immediately following the disaster;
- That primary or alternate vendors have a contractual commitment to assist in the recovery process.

*Team Members*
The team that is responsible for recovering lost, damaged or corrupted e-PHI data in the case of an emergency consists of workforce members from Tulane University's FPP Information Systems and the Information Technology Department. Workforce members' roles in executing the ***Disaster Recovery*** plan are as follows:

- TUMG Director of Information Systems – Coordination of the recovery effort
- IDX Security/Web Analysis – Performance of security and data integrity check
- TUMG Unix System Administrator – Restoration of Operating System and data
- Director of Network Services – Assistance with network issues

- Information Security Officer – Assistance with security issues and requirements

*Activation*
The ***Disaster Recovery*** plan may be activated under the following conditions:

- An incident has disabled, or is expected to disable, the systems and/or the communications network to the degree that normal operations will be significantly impacted for a period of 24 hours or more.
- An occurrence beyond the scope of daily operations has impaired the use of the systems or communication facilities in a manner that will substantially impact the normal operation of the University.
- An incident caused by problems with computers, networks, and/or telecommunications managed by Technology Services or by the TUMG Information Systems Group has resulted in the injury of one or more persons at the University.

*Notification*
In the event of such a disaster or emergency, phones, cell phones and pagers will be used to notify the team member. A call cascading list is established and distributed to each team member.

*Damage Assessment and Reporting*
Once all team members have been notified, the extent of damage to systems and sites must be analyzed and recommendations must be documented and reported to management. At the completion of the damage assessment, the TUMG Director of Information Systems reports the damage assessment and recommends the recovery action to the Director of Faculty Practice Plan. The Director of Information Systems invokes and supervises the recovery plan upon approval.

*Recovery Operations*
Once the extent of the damage has been analyzed, team members must recover critical systems to the extent possible. The TUMG Director of Information Systems must ensure that the following restoration steps are followed:

- Contact hardware and software Professional Services for recovery assistance if necessary
- Load Operating System
- Load data from the most current Backup tape
- Check systems and data integrity
- Perform quality assurance

*Return to Normal Operations*
Once it has been determined that it is safe to fully restore e-PHI Systems to normal, the TUMG Director of Information Systems will declare the end of a disaster state. He then will seek approval to return to normal operations from the Director of Faculty Practice Plan.

Tulane University has determined that it would not be reasonable or appropriate to apply these data restoration procedures to other systems on which e-PHI may be stored other than the IDX system, such as personal computers or other portable devices (e.g., laptops and PDAs). As described in the ***Information Security Strategy*** policy, Tulane University has determined that the e-PHI maintained on these systems generally is not as critical to the day-to-day operation of the Tulane University as the e-PHI on the IDX system to warrant recovery preparations similar to those used for the IDX system. In the event of a disaster impacting one of these systems, such as the personal computers operated in an independent physician practice location, e-PHI should be restored as quickly and as thoroughly as possible from the most recent backup or from the paper record, if one exists.

Policies and procedures for data backup and storage of e-PHI, including e-PHI stored in locations other than the IDX system, are set forth in Tulane University's ***Data Backup*** plan and ***Data Backup and Storage*** policy.

**RESPONSIBILITIES:**

The Security Officer will be responsible for implementing the requirements of the ***Disaster Recovery*** plan. The TUMG Director of Information Systems will be responsible for damage assessment and recommending the recovery actions.

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:
(B) **Disaster recovery plan** (Required). Establish (and implement as needed) procedures to restore any loss of data.