HIPAA Security Rule

Tulane University Contingency Operations Policy

Department: Technology Services	**Policy Description:** Contingency Operations (A)
Standard: Facility Access Controls	**Section:** 164.310(a)(1)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-24

PURPOSE

The purpose of this policy is to establish and implement as needed procedures that allow facility access in support of restoration of lost data under the ***Disaster Recovery*** plan and ***Emergency Mode Operations*** plan in the event of an emergency.

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

Under Tulane University's ***Disaster Recovery*** plan and ***Emergency Mode Operations*** plan, authorized workforce members must be able to access Tulane University's facilities to support restoration of lost data and to enable continuation of processes and controls that protect the confidentiality, integrity and availability of e-PHI while operating in the emergency mode. In the event of such an emergency, only authorized workforce members are permitted to administer or modify processes and controls that protect the security of e-PHI, as indicated in the ***Emergency Mode Operations*** plan.

Tulane University ensures that only those workforce members who are authorized have access to the facilities, information systems, workstations and backup media during emergency situations. Authorization is given only to those workforce members who are identified as essential personnel in the unit's disaster recovery or emergency operations plan.

Tulane University monitors and reviews access authorizations in the unit's disaster recovery or emergency operations plan to prevent abuse and access violations.

All emergency response staff and facility access management staff receive training on these procedures and this policy has been communicated to and coordinated with any third parties (e.g., landlords) who may control facility access.

RESPONSIBILITIES:

The Security Officer is ultimately responsible for ensuring the implementation of the ***Contingency***

Operations policy, as well as determining which workforce members must have access to certain secured locations.

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:
(a)(1) Standard: **Facility access controls**. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
(2) Implementation specifications:
(i) **Contingency operations** (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.