HIPAA Security Rule

Tulane University Facility Security Plan

Department: Technology Services	**Policy Description:** Facility Security Plan (A)
Standard: Facility Access Controls	**Section:** 164.310(a)(1)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-25

PURPOSE

The purpose of this policy is to document the procedures necessary to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

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's ***Risk Analysis*** defines the level of risk to Tulane University facilities and e-PHI Systems and, as such, provides the basis of the ***Facility Security*** plan.

Tulane University protects its facilities and e-PHI Systems from unauthorized access, tampering or theft in order to protect the confidentiality, integrity and availability of e-PHI. The facilities at issue are the TUMG's offices and their satellite clinics. Tulane University ensures that all external doors are adequately secured against unauthorized access by installing locks, alarms, or other access control devices.

Internally, within buildings and facilities, doors and windows must be locked whenever practicable. Keypad entry systems are installed at each facility which only allows authorized personnel entry to sensitive areas. Further, intrusion detection capabilities are installed to secure privileged internal areas, and physical barriers are in place from the floor to the ceiling. Only authorized workforce members, as defined in the ***Contingency Operations*** policy, have access to these secured locations during an emergency.

Any workforce member who becomes aware of any unauthorized access, tampering or theft attempts should notify Campus Security.

The ***Facility Security*** plan is reviewed and, if necessary, updated after each ***Risk Analysis*** or, at a minimum, at least once every year.

RESPONSIBILITIES:

The Security Officer is ultimately responsible for ensuring the implementation of the requirements of the

Facility Security plan. The Security Officer is responsible for reviewing and updating the plan as necessary.

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:
(ii) **Facility security plan** (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.