HIPAA Security Rule

Tulane University Access Control and Validation Procedures

Department: Technology Services	**Policy Description:** Access Control and Validation Procedures (A)
Standard: Facility Access Controls	**Section:** 164.310(a)(1)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-26

PURPOSE

The purpose of this policy is to establish procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control access to software programs for testing and revision.

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 ensures that only personnel with appropriate clearance or need-to-know have access to facilities that contain e-PHI.

All workforce members are required to wear visible identification or carry identification cards throughout the facilities. Visitors or equipment repair Contractors must be escorted at all times by an authorized employee.

In addition, Tulane University verifies need for access prior to authorizing physical access to any facilities. Workforce members are instructed not to attempt to gain physical access to facilities containing e-PHI Systems for which they are not authorized.

Tulane University logs and tracks physical access to facilities or areas and maintains such logs in a secure manner. The information documented includes:

- Date and time of access
- Name or user ID of workforce member gaining access
- Name of workforce member that granted the access

Workforce members are encouraged to report the loss or theft of any device that enables them to gain access to facilities, as well as any unknown persons in the facilities not wearing an identification badge.

RESPONSIBILITIES:

The Security Officer is ultimately responsible for ensuring the implementation of the requirements of the ***Access Control and Validation*** 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:

§ 164.310 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:
(iii) **Access control and validation procedures** (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.