HIPAA Security Rule

Tulane University Access Establishment and Modification Policy

Department: Technology Services	**Policy Description:** Access Establishment and Modification (A)
Standard: Information Access Management	**Section:** 164.308(a)(4)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-11

PURPOSE

The purpose of this policy is to establish procedures that, based upon Tulane University's ***Access Authorization*** policy, establish, document, review, and modify a user's right of access to a workstation, transaction, program or process.

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 workforce members are properly authorized and trained to access e-PHI. Tulane University creates and maintains access control lists (ACLs) and other access control related capabilities to ensure that access is limited according to the rights approved for each individual employee under the ***Access Authorization*** policy.

ACLs and other access control related capabilities are utilized to ensure that status changes such as termination or change in job role are reflected in rights granted to individuals or entities. Reviews are triggered by the submission of a Payroll Action Form to ensure that access rights for each individual or entity are consistent with established policies and job roles and functions. Any modifications of workforce members' access rights are logged and tracked, documentation of which is securely maintained. Tracking and logging includes the following information:

- Date and time rights is being modified;
- Identification of workforce members whose access is being modified;
- Description of modified access rights;
- Reason for modification of access rights.

Security controls or methods that establish access to e-PHI include:

- The removal of access methods for workforce members who no longer require access to e-PHI;
- Unique user IDs that enable workforce members to be uniquely identified and ensure that redundant user IDs are not created;
- Where possible, common or shared identifiers will not be used to access e-PHI.

RESPONSIBILITIES:

The Security Officer is responsible for ensuring the implementation of the ***Access Establishment and Modification*** policy. The Security Officer must review the access rights of individuals to ascertain that they are aligned with the individual's job's role or function.

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:
(4)(i) Standard: **Information access management**. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.
(ii) Implementation specifications:
(C) **Access establishment and modification** (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a User's right of access to a workstation, transaction, program, or process.