HIPAA Security Rule

Tulane University Authorization and/or Supervision Policy

Department: Technology Services	**Policy Description:** Authorization and/or Supervision (A)
Standard: Workforce Security	**Section:** 164.308(a)(3)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-6

PURPOSE

The purpose of this policy is to implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it may be accessed.

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 security safeguards ensure that all members of the workforce who have access to e-PHI, including operations and maintenance employees:

- *Need the access they have* – Tulane University does not allow workforce members to access e-PHI or areas where e-PHI might be accessed without the proper authorization. Tulane University takes reasonable steps (e.g. random audits of access, oversight by supervisor) to ensure that those workforce members who have the ability to access e-PHI are properly authorized.
- *Have the access they need* – Tulane University's information system owners or chosen representatives knowledgeable about security issues review access levels annually and make revisions to ensure that workforce members have appropriate access.
- *Understand the limits of access to e-PHI* – Tulane University trains and supervises all workforce members with access to e-PHI and areas where e-PHI may be accessed on the extent and limitations of their access level. Where an individual requires additional access, authorization must be obtained.
- *Understand how to authenticate themselves to the system or application* – Workforce members with access to e-PHI Systems are trained on authentication procedures.

The criterion for determining authorization complies with the requirements of the ***Information Access Management*** policies and the ***Workforce Clearance*** procedure. These documents establish the basis for determining the type and extent of authorized access to e-PHI. Authorization and access is defined by job roles and corresponding profiles on the IDX system.

Where third-parties seek access to e-PHI or locations where e-PHI may be accessed, Tulane University will implement security controls and require that agreements are signed defining the terms of any authorization granted to a third-party. Authorization of access to a third-party depends on such factors as the type of access requested, the sensitivity of e-PHI, the security controls on the e-PHI System, physical security measures in place to protect e-PHI, and whether the party has a business associate agreement with Tulane University. Any authorization agreements must include: (1) restrictions regarding use and disclosure of e-PHI; (2) Tulane University's ability to revoke authorization where necessary; and (3) provisions requiring the third party to comply with Tulane University's security policies and procedures.

The determination of whether any access needs to be supervised is based on the results and recommendations of the Risk Analysis Report.

RESPONSIBILITIES:

The Security Officer is responsible for ensuring the implementation of requirements related to the ***Authorizations and/or Supervision*** policy. The activities may include:

- Supervision of some members of the workforce
- Proper access authorizations on the basis of job roles or functions
- Clearance procedures
- Maintenance of access authorization records

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:
(3)(i) Standard: **Workforce security**. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
(ii) Implementation specifications:
(A) **Authorization and/or supervision** (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.