HIPAA Security Rule

Tulane University Termination Procedures

Department: Technology Services	**Policy Description:** Termination Procedures (A)
Standard: Workforce Security	**Section:** 164.308(a)(3)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-8

PURPOSE

The purpose of this policy is to implement procedures for terminating access to e-PHI when the employment of a workforce member ends or where access is no longer appropriate under the ***Workforce Clearance*** procedure.

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

People are the greatest threat to the security of any organization. It is thus important that any termination of a workforce member immediately results in both the Human Resources (HR) and the Information Technology (IT) departments coordinating their activities to ensure:

- Password access is immediately revoked
- Access to all systems and applications is revoked, including e-mail
- The workforce member is removed from any systems or applications that processed e-PHI
- All digital certificates are revoked
- Any tokens or smart cards issued to the workforce member are returned
- Any keys and IDs provided to the workforce member during their employment are returned
- Any other equipment or property supplied by Tulane University, including portable computers, are returned
- The workforce member is not provided any access to their desk or office – any such access, if provided, must be limited and carefully supervised

HR conducts an exit interview and documents any issues or concerns related to the workforce member.

Where it is determined pursuant to Tulane University's ***Workforce Clearance*** procedure that access to e-PHI is no longer appropriate, the HR and IT departments ensure that access to all e-PHI Systems, including access to areas where e-PHI may be accessed, is immediately terminated.

RESPONSIBILITIES:

The Security Officer is responsible for ensuring that all activities identified in this document are followed through and implemented.

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:
(C) **Termination procedures** (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.