HIPAA Security Rule

Tulane University Log-in Monitoring Policy

Department: Technology Services	**Policy Description:** Log-in Monitoring (A)
Standard: Security Awareness and Training	**Section:** 164.308(a)(5)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-14

PURPOSE

The purpose of this policy is to implement procedures for monitoring log-in attempts and reporting discrepancies.

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 provides authorized individuals access to e-PHI Systems through a secure log-in process. The system is designed to automatically lock out any individual after three unsuccessful log-in attempts, at which point a report is generated. All critical components of systems that process, store or transmit e-PHI are configured to record log-in attempts – both successful and unsuccessful.

The security training and awareness sessions include information on the following topics:

- How to detect a log-in discrepancy
- How to report a log-in discrepancy
- How to use the secure log-in process, including how to check last log-in information
- The importance of monitoring log-in success or failure

RESPONSIBILITIES:

The Security Officer is responsible for ensuring the implementation of the ***Log-in Monitoring*** policy. The Security Officer has identified all critical systems that will record log-in attempts – both successes and failures. The Security Officer ensures the monitoring of logs that record such information by authorized individuals on a regular basis.

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:
(5)(i) Standard: **Security awareness and training**. Implement a security awareness and training program for all members of its workforce (including management).
(ii) Implementation specifications. Implement:
(C) **Log-in monitoring** (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.