HIPAA Security Rule

Tulane University Automatic Logoff Policy

Department: Technology Services	**Policy Description:** Automatic Logoff (A)
Standard: Access Control	**Section:** 164.312(a)(1)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-36

PURPOSE

The purpose of this policy is to establish electronic procedures that terminate an electronic session after a predetermined time of inactivity.

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 has implemented reasonable and appropriate electronic procedures on e-PHI Systems to terminate electronic sessions after a period of inactivity through an automatic logoff mechanism. The length of time that a user is allowed to stay logged on while idle depends on the sensitivity of the information that can be accessed from that computer and the relative security of the environment in which the system is located. In general, electronic sessions are terminated and workforce members logged out of e-PHI Systems after **five minutes** of inactivity. For highly sensitive e-PHI Systems, automatic logoff occurs **after five minutes**.

Tulane University periodically inspects systems to ensure that the automatic session logoff capability is configured correctly.

In addition to the automatic logoff mechanisms, workforce members are instructed to terminate electronic sessions on e-PHI Systems when such sessions are completed and to log off from or lock workstations when they expect to be away from their workstations for an extended period of time and at the end of each day.

RESPONSIBILITIES:

The Security Officer is ultimately responsible for ensuring the implementation of the ***Automatic Logoff*** policy. Workforce members are responsible for logging off systems when they are away from their workstations for an extended period of time and at the end of each day.

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:

§ 164.312 Technical safeguards.

(a) A covered entity must, in accordance with § 164.306:
(a)(1) Standard: **Access control**. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
(2) Implementation specifications:
(iii) **Automatic logoff** (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.