HIPAA Security Rule

Tulane University Audit Controls Policy

Department: Technology Services	**Policy Description:** Audit Controls (R)
Standard: Audit Controls	**Section:** 164.312(b)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-38

PURPOSE

The purpose of this policy is to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use e-PHI.

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 enabled event auditing capabilities on all Information Systems that process, transmit, and/or store e-PHI. Currently, Tulane University controls only one Information System with e-PHI, which is the IDX billing system, and this policy applies only to that Information System. In the event that additional Information Systems with e-PHI are created or identified, additional procedures will be developed to govern the auditing of those Information Systems.

Auditing mechanisms provide the following information via the IDX Security Module:

- Users accessing the system with invalid username, passwords, and unknown usernames
- Frequency of access by users with errors

Audits are conducted to ensure confidentiality, integrity, and availability of e-PHI, investigate possible security incidents, ensure conformance to Tulane University security policies and monitor user or system activity where appropriate.

Tulane University's Information Systems have the appropriate hardware, software or personal auditing mechanisms to generate reports of auditable events. Based on Tulane University's ***Risk Analysis***, an auditable event has been determined to include such events as:

- Failed and successful authentication attempts (i.e. logins)
- Use of audit software programs or utilities
- Access of sensitive e-PHI
- Use of privileged accounts (e.g., system administrative accounts)

- Deletions and modifications involving e-PHI
- Security Incidents

Tulane University reviews the logs created by the audit mechanisms weekly. The following workforce members review audit logs and report suspicious auditable events to FPP Information Systems Administrator:

IDX Business Applications Analyst Security

All audit reports and log files are retained for six years.

When requested, and for the purpose of performing an audit, the Security Officer may provide authorized workforce members of Tulane University's security team with the following access to Information Systems:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, and so on) that may be produced, transmitted, or stored on Tulane University's equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on Tulane University's networks

RESPONSIBILITIES:

The Security Officer is ultimately responsible for ensuring the implementation of the ***Audit Controls*** policy.

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:
(b) Standard: **Audit controls**. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.