HIPAA Security Rule

Tulane University Information System Activity Review Policy

Department: Technology Services	**Policy Description:** Information System Activity Review (R)
Standard: Security Management Process	**Section:** 164.308(a)(1)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-4

PURPOSE

The purpose of this policy is to ensure that Tulane University regularly reviews records of information system activity, such as audit logs, access reports, and security incident tracking reports.

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 clearly identified all e-PHI Systems. To enable regular review of information security activity, Tulane University has implemented appropriate auditing mechanisms on all e-PHI Systems as determined necessary by the ***Risk Analysis***. Based on the *Risk Analysis* results, the risk management review will be repeated bi-annually.

Where possible, the information that will be maintained in audit logs and access reports must include:

- Identification of User performing activity
- Dates and time of log-on and log-off
- Origin of activity (e.g., terminal identity, IP address and/or location, if possible)
- Records of successful and rejected system access attempts
- Use of privileged accounts (e.g., system administrator accounts)
- Security incidents
- Access of sensitive e-PHI

The Security Officer will maintain safeguards to protect against unauthorized changes and operational problems including:

- The logging facility being deactivated
- Alterations to the message types that are recorded
- Log files being edited or deleted
- Log file media becoming exhausted, and either failing to record events or overwriting itself

Records of significant activity will be maintained in a secured location for a length of time to be determined by the Security Officer.

RESPONSIBILITIES:

The Security Officer will clearly identify:

- The systems that must be reviewed
- The information on these systems that must be reviewed
- The types of access reports that are to be generated (i.e. the types of activities that are significant)
- The security incident tracking reports that are to be generated to analyze security violations
- The individual(s) responsible for reviewing all logs and reports ensuring that there is a separation of roles between the person(s) undertaking the review and those whose activities are being monitored.

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:
(ii) Implementation specifications:
(D) **Information system activity review** (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.