HIPAA Security Rule

Tulane University Documentation Policy

Department: Technology Services	**Policy Description:** Documentation Standard
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-A3

PURPOSE

The purpose of this policy is to maintain the policies and procedures implemented to comply with the Security Rule in written (or electronic) form and, if an action, activity or assessment is required to be documented, to maintain a written electronic record.

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 maintains documentation of the policies and procedures that it implements under the Security Rule in written (paper or electronic) format. Where the Security Rule requires an action, activity or assessment to be documented, Tulane University maintains a written record of it. Such records include, but are not limited to:

- Correction action plans
- Executive memorandums
- Quality improvement evaluations
- Risk analysis findings and results in accordance with Tulane University's ***Risk Analysis*** policy
- Documentation of assignment of security responsibility in accordance with Tulane University's ***Assigned Security Responsibility*** policy
- Documentation of security reminders provided to workforce members in accordance with Tulane University's ***Security Reminders*** policy
- Documentation of security incidents and their outcomes in accordance with Tulane University's ***Security Incident*** policy
- Documentation for establishing, reviewing and modifying access in accordance with Tulane University's ***Access Establishment and Modification*** policy.
- Documentation of application and data criticality analysis conducted in accordance with Tulane University's ***Applications and Data Criticality Analysis*** policy
- Documentation of technical and non-technical evaluations of its security controls and processes conducted in accordance with Tulane University's ***Evaluation*** policy
- Documentation of movements of hardware and electronic media, and the persons responsible therefore in accordance with Tulane University's ***Accountability*** policy

- Documentation of repairs and modifications to the physical components of its facilities that are related to security in accordance with Tulane University's ***Maintenance Records*** policy.
- Business associate contracts
- Any documentation required relating to decisions to not implement Addressable Implementation Specifications

Tulane University retains such documentation for 6 years from the date of its creation or the date when it was last in effect, whichever is later.

Tulane University makes such documentation available to those persons responsible for implementing the procedures to which the documentation pertains. Workforce members are provided with copies of relevant policies and procedures.

Tulane University reviews the documentation periodically, and updates it as needed, in response to environmental or operational changes affecting the security of the e-PHI.

RESPONSIBILITIES:

The Security Officer is ultimately responsible for ensuring the implementation of the requirements of the ***Documentation*** 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:

§ 164.316 Policies and procedures and documentation requirements.

A covered entity must, in accordance with § 164.306:
(b)(1) Standard: **Documentation**.
(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and
(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.
(2) Implementation specifications:
(i) **Time limit** (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.
(ii) **Availability** (Required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
(iii) **Updates** (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.