



HIPAA Security Rule

Tulane University Assigned Security Responsibility Policy

Department: Technology Services	Policy Description: Assigned Security Responsibility (R)
Standard: Assigned Security Responsibility	Section: 164.308(a)(2)
Approved: April 19, 2005	Revised:
Effective Date: April 20, 2005	Policy Number: TS-5

PURPOSE

The purpose of this policy is to identify the job responsibilities of the information Security Officer who is responsible for the development and implementation of the policies and procedures required by the Security Rule.

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

The Information Security Officer must:

- Confirm that e-PHI Systems do not compromise the confidentiality, integrity and availability of any e-PHI. Approve and oversee the administration, implementation and selection of Tulane University's security controls for e-PHI Systems.
- Ensure that all policies, procedures, and plans required by the Security Rule and other federal, state and local laws pertaining to security of e-PHI are developed, implemented, and maintained as necessary.
- Monitor changes in legislation that may affect Tulane University and its security position.
- Monitor changes and advances in technology that may affect Tulane University and its security position.
- Confirm that a periodic risk analysis of e-PHI Systems is completed on an ongoing basis in accordance with Tulane University's **Risk Analysis**.
- Perform technical and non-technical evaluations or audits on security processes in order to find and correct weaknesses and guard against potential threats to security in accordance with Tulane University's **Information System Activity Review** policy.
- Act as an internal consultant for Tulane University in all issues related to security. Work with Tulane University's Privacy Official to confirm that security policies, procedures and controls support compliance with the HIPAA Privacy Regulations.
- Ensure that a system for reporting and responding to security incidents (as well as violations of Security Rule) is in place and functioning in accordance with Tulane University's **Risk Management**

- activities.
- Deliver, on an ongoing basis, security awareness training to all members of the workforce.

The Tulane University Technology Services Component shall designate an appropriate individual to serve as the Information Security Officer.

RESPONSIBILITIES:

All individuals, groups, and organizations identified in the scope of this policy are responsible for:

- Supporting and providing assistance to the Information Security Officer whenever necessary when the Information Security Officer is acting in the role described under the policy section

The Tulane University's Information Security Officer, as defined by the ***Assigned Security Responsibility*** policy, is responsible for:

- All aforementioned responsibilities described in the policy section

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:

(2) Standard: **Assigned security responsibility** (Required). Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.