HIPAA Security Rule

Tulane University Evaluation Policy

Department: Technology Services	**Policy Description:** Evaluation Policy(R)
Standard: Evaluation	**Section:** 164.308(a)(8)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-22

PURPOSE

As of April 20, 2005, all of Tulane University's security policies and procedures are compliant with the Security Rule. The purpose of this policy is to document Tulane University's technical and non-technical evaluation procedures for determining the extent to which Tulane University's security policies and procedures must be revised going forward to meet the requirements of the Security Rule, in light of environmental or operational changes affecting the security of 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 conducts periodic technical and non-technical evaluations of its security policies and procedures. These evaluations are conducted on an "as needed" basis, but not less than once a year. The purpose of this evaluation will be to determine and document the effectiveness of the policies as well as to ensure compliance with state and federal laws and regulations, including the Security Rule.

These evaluations are completed by the Security Officer, TUMG Information Systems Administrator, and TU Internal Audit as appropriate. Each evaluation includes, as needed:

- A review of Tulane University's security polices and procedures to evaluate their appropriateness and effectiveness at protecting against any reasonably anticipated threats or hazards to the confidentiality, integrity and availability of e-PHI.
- An updated ***Risk Analysis*** and ***Risk Management*** to identify and mitigate threats and risks to e-PHI and e-PHI Systems.
- An updated ***Applications and Data Criticality Analysis*** to assess and prioritize the impact to the confidentiality, integrity and availability of e-PHI if various e-PHI Systems become unavailable as a result of a disaster or other emergency.
- An updated gap analysis to compare Tulane University's security policies and procedures against actual practices.
- An assessment of whether Tulane University's security controls and processes are reasonable and appropriate protections against the risks identified for e-PHI Systems.

- Testing and evaluation of Tulane University's security controls and processes to determine whether they have been implemented properly and whether they appropriately protect e-PHI.

Should a policy or procedure be found ineffective, missing, or otherwise flawed, Tulane University takes appropriate steps to mitigate the problem. Such steps may include:

- Amending or adding the policy or procedure it in a timely manner
- Communicating the new policy or procedure to the affected workforce members and ensuring that they understand the changes

Changes that may trigger a reevaluation of Tulane University's security safeguards on an "as needed" basis include without limitation:

- Known security incidents
- New threats or risks that impact the security of e-PHI
- Changes to Tulane University's organizational or technical infrastructure
- Changes to Tulane University's information security requirements or responsibilities
- New security technologies that are available
- Changes to any state or federal law or regulation, or the addition of a new law or regulation, that may affect the security policies

The results of each evaluation, including recommendations for changes to existing policies and procedures, are documented and reported to the Security Officer.

RESPONSIBILITIES:

The Security Officer has ultimate responsibility for ensuring the implementation of the requirements of the ***Evaluation*** 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:

§ 164.308 Administrative safeguards.

(a) A covered entity must, in accordance with § 164.306:
(8) Standard: **Evaluation** (Required). Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.