HIPAA Security Rule

Tulane University Protection from Malicious Software Policy

Department: Technology Services	**Policy Description:** Protection from Malicious Software (A)
Standard: Security Awareness and Training	**Section:** 164.308(a)(5)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-13

PURPOSE

The purpose of this policy is to implement procedures for guarding against, detecting, and reporting malicious software. Malicious software refers to viruses, worms, Trojan horses and backdoor programs designed to disrupt or damage an information system. The key difference between the types of malicious software is how they spread throughout the system.

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 deploys malicious software checking programs at the perimeter (edge) of the network and on individual end-user systems. Anti-virus software is installed on all e-PHI Systems and workforce members are prohibited from bypassing or disabling such software unless properly authorized to do so. Anti-virus software examines all electronic mail attachments, downloads, and electronic media to confirm they do not contain malicious software. Tulane University subscribes to updates for all malicious software checking programs, including anti-virus software.

Tulane University ensures that no unauthorized software is installed on e-PHI Systems. Authorization must be obtained prior to installing software or modifying web browser settings on e-PHI Systems.

Tulane University conducts security training that includes information on:

- Potential harm that can be caused by malicious software
- Prevention of malicious software such as viruses
- How to discover malicious software programs
- How to use anti-virus software
- Steps to take if a malicious software such as a virus is detected

RESPONSIBILITIES:

The Security Officer is responsible for ensuring that malicious software checking programs are installed both on the perimeter (edge) of the network and on individual end-user systems. The Security Officer has identified all critical systems and network components that are vulnerable to malicious software. All such identified systems have malicious software checking capability.

Members of the workforce must not configure or introduce any modifications to systems or applications to prevent the execution of malicious software checking programs. Members of the workforce that suspect any malicious software infection must immediately contact the Security Officer or their manager by phone or walk-in – not by e-mail – about the suspected threat.

Members of the workforce must participate in all security awareness training programs and apply the knowledge in preventing, detecting, containing and eradicating malicious software.

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:
(5)(i) Standard: **Security awareness and training**. Implement a security awareness and training program for all members of its workforce (including management).
(ii) Implementation specifications. Implement:
(B) **Protection from malicious software** (Addressable). Procedures for guarding against, detecting, and reporting malicious software.