HIPAA Security Rule

Tulane University Workstation Use Policy

Department: Technology Services	**Policy Description:** Workstation Use Policy (R)
Standard: Workstation Use	**Section:** 164.310(b)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-28

PURPOSE

The purpose of this policy is to specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access 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

The workstations and other computing devices at Tulane University are to be used for work related purposes only. This includes, but is not limited to, Internet and Web access and the use of e-mail at Tulane University. Workforce members should not expect any level of privacy as their activities, e-mails, files, and logs may be viewed at any time by the Security Officer or other members of management in support of this and other policies and procedures. Workforce members are advised of this policy. The following activities are considered examples of unauthorized uses of workstations:

- Violating any of Tulane University's security policies and procedures
- Violating the privacy rights of Tulane University's patients or any person or company protected by intellectual property laws
- Unauthorized copying of copyrighted material
- Intentionally introducing malicious software onto workstation or network
- Procuring or transmitting material in violation of Tulane University's harassment policies
- Intentionally causing a security incident
- Intercepting data not intended for the workforce member

Tulane University may revoke the access rights of any individual at any time in order to protect or secure the confidentiality, integrity, and availability of sensitive information or to preserve the functionality of electronic information systems.

Tulane University implements reasonable and appropriate measures to secure its computing devices from unauthorized access to sensitive information. Examples of such measures include:

- All user and administrator accounts are protected by use of a password, as set forth in the ***Access Authentication*** policy and ***Password Management*** policy. Password-based access control systems mask or obscure passwords so that unauthorized persons are not able to view them. Workforce members are instructed not to share passwords with others and to report any suspected misuse of their user IDs or passwords promptly to Tulane University's Security Officer.
- All users accessing Tulane University computing devices are provided with a unique user ID as set forth in the ***Access Authentication*** policy. Tulane University verifies that no redundant user IDs are issued.
- Each workstation has an automatic locking mechanism that activates when left unattended for 15 minutes. Workforce members are instructed to log off their workstations when their shift is complete.
- Workstation access privileges are immediately removed from workforce members once employment has been terminated in accordance with the ***Termination Procedures*** policy.
- Security updates and software patches are performed automatically as needed.
- All unnecessary and unused services (or ports) are disabled.

Special measures are taken to physically protect computers that are located in public areas, computers used to access e-PHI and portable computers (e.g., laptops and PDAs) that can be taken off the premises:

- Computers located in public areas are situated to block unauthorized viewing and have screen savers that black out the screen when left unattended.
- Workstations that access e-PHI are physically located in such a manner as to minimize the risk of access by unauthorized individuals, as addressed in the ***Workstation Security*** document. Display screens are positioned or protected to prevent unauthorized viewing.
- E-PHI may not be stored on portable workstations or PDAs unless passwords and other appropriate security measures are implemented. Users must ensure that portable workstations are backed-up on a network device and that PDAs are synchronized with computers as often as practical. Additionally, portable workstations and PDAs should be carried as carry-on baggage on public transportation, and should be concealed and locked on private transportation. Users should contact the Security Officer with any questions about appropriate security measures relating to the storage of e-PHI on portable workstations or PDAs.

RESPONSIBILITIES:

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

§ 164.310 Physical safeguards.

(a) A covered entity must, in accordance with § 164.306:
(b) Standard: **Workstation use** . Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health

information.