



HIPAA Security Rule

Tulane University Maintenance Records Policy

Department: Technology Services	Policy Description: Maintenance Records Policy (A)
Standard: Facility Access Controls	Section: 164.310(a)(1)
Approved: April 19, 2005	Revised:
Effective Date: April 20, 2005	Policy Number: TS-27

PURPOSE

The purpose of this policy is to establish procedures for documenting repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

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

Repairs and modifications to the physical components at its facilities that are related to security (such as walls, doors, locks and physical access systems) are documented and maintained in a secure manner. Tulane University's documentation includes:

- Date and time of repair or modification
- Description of physical component prior to repair or modification
- Reasons for repair or modification, including any related security incident
- Persons performing repair or modification
- Outcome of repair or modification

All building maintenance personnel receive training regarding this policy in order to take reasonable steps to ensure the Security Officer is informed when a repair or modification is made. The Security Officer or his or her designee oversees any security-relevant physical modifications or repairs.

To the extent that the physical premises of Tulane University Medical Group clinics or other facilities are managed by a third party (such as a landlord); Tulane University will attempt to ensure that it has copies of, or access to, any documentation described in this policy that is maintained by the third party.

RESPONSIBILITIES:

The Security Officer is ultimately responsible for ensuring the implementation of the ***Maintenance Records***

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:

(a)(1) Standard: **Facility access controls**. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(2) Implementation specifications:

(iv) **Maintenance records** (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).