HIPAA Security Rule

Tulane University Integrity Controls Policy

Department: Technology Services	**Policy Description:** Integrity Controls (A)
Standard: Transmission Security	**Section:** 164.312(e)(1)
Approved: April 19, 2005	**Revised:**
Effective Date: April 20, 2005	**Policy Number:** TS-41

PURPOSE

The purpose of this policy is to implement security measures to ensure that electronically transmitted e-PHI is not improperly modified without detection until disposed of.

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

In accordance with its risk analysis, Tulane University determined that the following types of e-PHI merit special protection when being transmitted over electronic communication networks:

- Billing information

In making this determination, Tulane University considered:

- Sensitivity of the e-PHI (high, medium or low)
- Risks to the e-PHI (e.g. malicious alteration or corruption)
- Expected effectiveness of specific integrity controls in mitigating such risks
- Expected impact to Tulane University's functionality and workflow by implementing integrity controls
- Ability of recipient to validate integrity of any e-PHI received

Tulane University maintains integrity controls to protect the integrity of e-PHI transmitted over electronic communication networks as follows:

- VPN tunnel

Based on its assessment of the risks of communication interception and modification and on its assessment of the costs and benefits of available encryption technologies, Tulane University has determined that it would not be reasonable and appropriate to implement technical solutions to guard against the improper modification of e-PHI transmissions not relating to the IDX system. If a workforce member sends e-PHI that he or she believes requires additional protections based on amount, sensitivity, or other considerations, he or

she should contact the Security Officer for guidance on encryption options.

RESPONSIBILITIES:

The Security Officer is ultimately responsible for ensuring the implementation of the ***Integrity Controls*** 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:

§ 164.312 Technical safeguards.

(a) A covered entity must, in accordance with § 164.306:
(e)(1) Standard: **Transmission security**. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
(2) Implementation specifications:
(i) **Integrity controls** (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.