HIPAA Security Rule

Tulane University Risk Analysis

Department: Technology Services	**Implementation Specification:** Risk Analysis (R)
Standard: Security Management Process	**Section:** 164.308(a)(1)

Under the Security Rule, Tulane University is required to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI. This document is a record of the steps and procedures Tulane University has taken to assess its risks pursuant to the Security Rule.

A documented risk analysis process was used as the basis for the identification, definition and prioritization of risks to e-PHI. A Risk Analysis worksheet was developed to aid in such assessment, using the following steps:

- System characterization – Each individual e-PHI system was analyzed and characterized according to factors such as type of hardware, software, interfaces and data transmission.
- Threats and vulnerabilities – Potential threats to and vulnerabilities of individual e-PHI systems were identified and prioritized.
- Likelihood determination – The probability that a threat would exploit a vulnerability of e-PHI was determined using the following ratings:
    - ***High*** – Threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
    - ***Medium*** – Threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
    - ***Low*** – Threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.
- Impact analysis – The impact of the exploitation of a specific vulnerability on the confidentiality, integrity and availability of e-PHI was determined using the following ratings:
    - ***High*** – Exercise of the vulnerability (1) may result in the high costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, and interest; or (3) may result in human death or serious injury.
    - ***Medium*** – Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
    - ***Low*** – Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.
- Risk determination – The information in the above determinations was used to identify the level of risk to e-PHI. The level of risk was computed to be between 1 and 60 with a higher number indicating greater risk.
- Safeguard recommendations – Based on the potential threats and vulnerabilities as well as the risk determination, recommendations were made concerning the controls that should be implemented to protect the confidentiality, integrity and availability of e-PHI.
- Result documentation – The results of the risk analysis for each e-PHI system were compiled into a Risk Analysis Report, which was reviewed by the management of the e-PHI and maintained in a secure fashion. Copies of the individual Risk Analysis Reports are attached to this document.

Tulane University conducted its initial risk analysis in July 2004. The risk analysis was the first step of the ***Risk Mitigation*** process as documented separately.