



HIPAA Security Rule

Tulane University Applications and Data Criticality Analysis

Department: Technology Services	Implementation Specification: Applications and Data Criticality Analysis(A)
Standard: Contingency Plan	Section: 164.308(a)(7)

Under the Security Rule, Tulane University is required to assess the relative criticality of specific applications and data in support of other contingency plan components. Tulane University completed the initial assessment on July 2004. This assessment, which will be repeated periodically, concerns the impact of a disaster or emergency to Tulane University's services, processes and business objectives if e-PHI were to be unavailable for various amounts of time. This assessment serves as the basis for the security prioritization of e-PHI and e-PHI Systems, as documented in the **Risk Management** memorandum.

Tulane University assessed the "critical" areas of its operations, including the critical business functions, infrastructure and e-PHI or records. As part of this assessment, key applications and systems used to support critical business processes were identified and analyzed.

The focus of this analysis was on the impact to the confidentiality, integrity and availability of e-PHI if e-PHI Systems were unavailable for various amounts of time. The analysis was performed by the HIPAA Security Consultant and FPP Information Systems Administrator. As part of the analysis, network architecture diagrams and system flowcharts were created to show the current structure, equipment addresses, communication providers and system interdependencies of Tulane University's e-PHI Systems. Copies of these documents are attached to this memorandum. In addition, the network infrastructure was tested to ensure the existence of adequate redundancies to reduce or eliminate single points of failure.