DATA SECURITY: RISK MANAGEMENT

Policy: The University shall ensure that it meets requirements in the HIPAA Security rule regarding the assessment and mitigation of potential risks and vulnerabilities to electronic data security related to protected health information (PHI).

Rationale: To comply with 45 CFR 164.308

POLICY STATEMENT:

The purpose of the policy is to comply with state and federal requirements pertaining to the assessment of potential risks and vulnerabilities; the reduction of such risks and vulnerabilities; the evaluation of the University's compliance with HIPAA Security requirements; and the University's IT security policies and procedures.

Agency Responsibilities

The HIPAA-Covered Component shall implement a Risk Management Framework. Risk Assessment standards shall be reviewed annually. Policies and procedures shall be updated as necessary to ensure that state and federal required control capabilities are maintained.

Compliance and Implementation

1. Data Classification shall be implemented to ensure that each HIPAA-Covered Component, on an as-required basis as follows:

    - Categorizes information and their information systems in accordance with applicable federal laws and University Policy

    - Documents the security categorization results (including supporting rationale) in the organization's security plan for information systems.

2. Each HIPAA-Covered Component shall implement a Risk Assessment methodology. The HIPAA-Covered Component shall:

    - Conduct a risk assessment. This methodology will include the likelihood and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

    - Document risk assessment results

    - Review risk assessment results

- Remediate identified risks

3. Each HIPAA-Covered Component shall conduct appropriate system vulnerability scanning. They will:

    - Periodically scan for vulnerabilities in HIPAA-Covered Component information system

    - Analyze vulnerability scan reports and results from security control assessments

    - Remediate vulnerabilities in accordance with an organizational assessment of associated risk.

Reference: 45 CFR 164.308