# Risk Management
# HIPAA Policy: Security 02

**Summary:** Develops a risk management plan for HIPAA entities

**Affected Individuals:** Employees in HIPAA covered entities; IT staff

## Purpose of Policy

The purpose of this policy is to develop and implement a Risk Management Plan and Program that addresses risk assessments, risk mitigation, and risk evaluation for the University of Mississippi (UM).

## Definitions

For a complete list of definitions, refer to the *Glossary*.

## Scope

This policy applies only to covered entities as defined in the University of Mississippi (UM) HIPAA hybrid policy.

All users and workforce members, including third parties, who may have access or exposure to UM's data are required to comply with this policy.

## Policy

A. Risk Management Plan Development

1. UM develops and implements a formal, comprehensive *Risk Management Plan* to manage risk associated with the operation and use of information systems, including physical and environmental hazards, to an acceptable level.
2. Information safeguards are not applied unnecessarily (e.g., to de-identified information).

B. Risk Assessments

1. UM performs risk assessments that address all major HITRUST CSF (Common Security Framework) domains to identify and quantify risks.
2. UM performs risk assessments in a consistent way and identifies information security risks to UM. This includes the evaluation of multiple factors that may impact security as

well as the likelihood and impact from a loss of confidentiality, integrity and availability of information and systems.

3. UM accounts for risks from prior incidents, changes in the environment, and third parties.
4. Formal risk assessments are performed at planned intervals, or when major changes occur in the environment, and the results reviewed annually.

C. Risk Mitigation

1. UM reduces risk to the lowest acceptable level.
2. UM defines and documents the criteria to determine whether or not a risk is avoided, accepted, transferred or treated in the *Corrective Action Plan*.
3. UM implements a process for ensuring that corrective action plans are prioritized and maintained; and the remedial information security actions necessary to mitigate risk to operations and assets, individuals, and other organizations are documented.
4. UM reviews corrective action plans (plans of action and milestones) for consistency with the risk management strategy and UM-wide priorities for risk response actions.
5. UM updates existing remediation or corrective action plans monthly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

D. Risk Evaluation

1. UM continually evaluates and assesses risks.
2. Risk assessments are re-evaluated at least annually, or when there are significant changes in the environment.

## Policy Compliance

### Enforcement

The Chief Information Security Officer (CISO), or designee has general responsibility for the implementation and enforcement of this policy.

### Future Revisions

UM reserves the right to add, delete, or revise any provision of this Policy (with committee approval) at any time, or any other Information Security Policy without prior notice to users.

### Sanctions

Any user violating these policies or applicable local, state, or federal laws while using UM's computing environment is subject to loss of network privileges and any other disciplinary actions deemed appropriate, up to and including termination and criminal and/or civil prosecution in accordance with policy.

### Exceptions

Exceptions to this policy must follow the approved exception process as outlined in the *Information Security Waiver Policy*. All approved policy exceptions will be reviewed periodically for appropriateness by the CISO and may be revoked at any time with or without notice.

## Regulatory and Standards References

The following regulations and standards are applicable to this policy:

# Risk Management
# HIPAA Policy:  Security 02

- **HIPAA Regulatory References**: HIPAA § 164.308 (a)(1)(i), HIPAA § 164.308 (a)(1)(ii)(A), HIPAA § 164.308 (a)(1)(ii)(B), HIPAA § 164.308 (a)(2), HIPAA § 164.308 (a)(7)(ii)(E), HIPAA § 164.316(a), HIPAA § 164.402
- **HITRUST Reference**s: 03.a Risk Management Program Development, 03.b Performing Risk Assessments, 03.c Risk Mitigation, 03.d Risk Evaluation
- **PCI References**: PCI DSS v3 12.2

Related Documents:

- Data Classification and Handling Policy
- Glossary
- Corrective Action Plan

## Approval

________________________________________ ____________________

Chief Information Security Officer <date>