Information Security Management Program
HIPAA Policy: Security 01

Summary: Establishes requirements for HIPAA security

Affected Individuals: Employees in covered entities; IT staff

Purpose of Policy

The purpose of this policy is to establish the high level requirements for the University of Mississippi (UM) Information Security Management Program (ISMP). The ISMP reduces risk by protecting and supporting the confidentiality, availability, and integrity of information assets.

UM is committed to conducting business in keeping with its core organizational values and in compliance with all applicable laws, regulations, and policies. In particular, UM is committed to compliance within the covered health care component areas with the regulatory requirements established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regarding the security of protected health information (PHI), also known as the "Security Rule" and all subsequent Security Rule updates, as well as all state-level regulatory compliance requirements that apply to its area of operations.

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 workforce members, including third parties, are required to comply with this policy.

Policy

A. Information Security Management Program Policy

1. Protecting UM's confidential data and reducing information security risks is the responsibility of all workforce members and third parties.

2. UM establishes formal information security, privacy, and risk management programs. These programs work together with the common goal of reducing risk to UM from within their specific areas of responsibility.
3. These programs are reviewed and updated annually.
4. UM designs, implements, and maintains a comprehensive and effective ISMP to ensure acceptable levels of risk throughout UM. The ISMP is continuously assessed and improved upon through governance, risk management, information security protective operations, awareness and training, and incident response activities.
5. UM implements a formal ISMP to ensure the confidentiality, availability, and integrity of information assets. The ISMP must be designed to the specific characteristics of UM and established and managed via continuous monitoring, maintenance and improvement.
6. The ISMP is formally documented and actively monitored by the CISO.
7. The ISMP is reviewed and updated on an annual basis to ensure program objectives continue to meet the needs of UM.

B. Information Security Management Program Strategy

The ISMP is manned, organized, and supported by the CISO to ensure it is capable of accomplishing its primary tasks of information security:

- Governance
- Risk management
- Information security protection operations
- Training, and awareness
- Incident response activities

C. Information Security Management Program Content

1. At a minimum, the ISMP includes:

- UM approved information security policies and procedures
- Mission, vision, structure and objectives of the information security program
- Governance structure
- HITRUST common security framework
- Annual risk assessment
- Risk management measures and actions
- Education, training, and awareness plan and materials
- Information security plans for (minimum set):
- Information systems
- End user devices
- Applications
- Networks, including wireless
- IT security devices and systems
- Business continuity
- Disaster recovery
- These security plans meet applicable legal, regulatory and appropriate best security practices as determined by the CISO. Security plans are periodically reviewed and communicated to relevant stakeholders.

D. Commitment to Information Security

1. UM Security Committee actively supports information security through clear direction, demonstrated commitment, incorporation into strategic planning, and acknowledgment of information security responsibilities.
2. A CISO is appointed and accountable for ensuring information security leadership and processes are in place, compliance with applicable laws and regulations is assured, and security risks are evaluated and accepted for UM.
3. Formal governance is chartered to ensure institutional oversight, coordination, and synchronization of information security at UM.

4. The Security Committee reviews the effectiveness of the ISMP and evaluates and accepts security risks.
5. Capital planning and investment requests consider information security. They include resources necessary for implementing information security capabilities necessary to address any risks associated with such capital plans and requests. UM ensures such resources are available for expenditure and applied appropriately.

E. Information Security Coordination

1. Reducing information security risks is the responsibility of all workforce members and third parties. These risk reduction activities are coordinated and communicated by representatives from different parts of UM respective to their roles and job functions.
2. Security activities (e.g., implementing controls, correcting non-conformities) are coordinated in advance and communicated across UM.
3. Security requirements for information systems are identified and resources are allocated as either capital or operating resources in a separate budget line item.

F. Information Security Responsibilities

1. All information security responsibilities are formally defined in writing in the *Information Security Roles and Responsibilities* document.
2. The CISO is a senior-level employee who oversees the ISMP.

G. Authorization Process

1. A management authorization process for acquiring new information assets (e.g., systems and applications), and facilities (e.g., data centers or offices where covered information is processed), including their maintenance, is defined and implemented according to the *Information Systems, Acquisition, Development and Maintenance Policy*.

H. Contact with Authorities

1. The CISO develops and maintains a contact list for reporting security incidents to law enforcement if it is suspected that laws may have been broken.
2. The CISO develops and maintains a contact list of third parties for reporting security incidents in case of a reportable security incident.

Policy Compliance

Enforcement

The designated Chief Information Security Officer (CISO) 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 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.

Exceptions

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

Information Security Management Program
HIPAA Policy: Security 01

Regulatory and Standards References

The following regulations and standards are applicable to this policy:

- **HIPAA Regulatory References**: HIPAA § 164.308(a)(2), HIPAA §164.308(a)(1)(i), HIPAA §164.308(a)(1)(ii)(A), HIPAA §164.308(a)(1)(ii)(B), HIPAA §164.308(a)(1)(ii)(D), HIPAA §164.308(a)(2), HIPAA §164.308(a)(5)(ii)(A), HIPAA §164.308(a)(8), HIPAA §164.310(a)(2)(ii), HIPAA §164.316(a), HIPAA §164.316(b)(1), HIPAA §164.316(b)(1)(i), HIPAA §164.316(b)(2)(iii), HIPAA §164.316(b)(2)(iii)
- **PCI References**: PCI DSS v3, PCI DSS v3 12.4, PCI DSS v3 12.5, PCI DSS v3 12.5.1, PCI DSS v3 12.5.2, PCI DSS v3 12.5.3, PCI DSS v3 12.5.4, PCI DSS v3 12.5.5

Related Documents:

- Glossary
- Information Security Management Program Plan
- Information Security Roles and Responsibilities
- Risk Management Plan

Approval

Chief Information Security Officer	<date>