Business Continuity Management
HIPAA Policy: Security 04

Summary: Outlines emergency management requirements for HIPAA systems

Affected Individuals: HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to ensure that strategies and plans are in place to counteract interruptions to the University of Mississippi's (UM) activities and to protect critical business processes from the effects of major failures of information systems or disasters (e.g., fire, power or communications blackout, tornado, hurricane, flood, earthquake, civil disturbance, hacking or other security attacks etc.) and to ensure their timely resumption.

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.

This policy applies to all workforce members, users, and all personnel affiliated with third parties who access or use UM's information assets, regardless of physical location.

Information assets include all UM owned, licensed, leased, or managed hardware and software, and use of the UM network via a physical or wireless connection, regardless of the ownership of the computing device connected to the network.

Policy

A. Business Continuity Management Policy

1. UM develops, implements, tests, and maintains a Business Continuity Plan (BCP) that covers all information assets that deliver or support core critical business functions.
2. The BCP ensures that UM maintains compliance with statutory requirements (e.g., HIPAA, HITRUST, PCI, applicable state regulations, etc.) during and after a business disruption.

B. Business Impact Analysis

1. UM conducts a risk assessment of events that can cause interruptions to its operational processes and identifies, estimates, and prioritizes risks to these processes.
2. UM conducts a business impact analysis to identify critical operational processes and to determine recovery criticality.
   - UM identifies outage impacts and estimated downtime.
   - UM shall identify resource requirements.
   - UM shall identify recovery priorities for critical systems.
   - System criticality should be determined and documented based on tolerance and impact to your business unit / department for unplanned interruptions of normal business operations. The reference scales below should be used for a baseline:

     The business unit / department impact will be felt within:
     - **1 hours** of an interruption = **Critical**
     - **8 hours** of an interruption = **Important**
     - **24 hours** of an interruption = **Non-critical**

System Type	Impact
Telecom / Network	Critical
Data Center	Critical
EHR	Important
Medical Devices	Important
Workstations	Non-critical
Scheduling / Billing	Non-critical
Other	Non-critical

3. UM identifies mitigation options, steps, and costs.

C. Design and Develop the Business Continuity Plan

1. UM develops and implements the BCP to ensure UM can restore operations and establish availability of information in the required time frame following interruption to, or failure of, critical operational business processes.
2. UM identifies roles and responsibilities and designates the BCP owner.
3. UM develops backup and recovery strategies for information assets according to the *Information Backup and Storage Policy*.
4. UM ensures the secure protection of confidential data, and ensures that confidentiality, accessibility and integrity are preserved.
5. UM identifies and implements an alternate, geographically-separated site for back-up and recovery continuity support, including equipment and budget for the site.
6. UM develops BCP activation criteria including notification and escalation plans.
7. UM develops BCP deactivation criteria including notification of the return to normal operations and clean up procedures.

D. Implement the Business Continuity Plan

1. UM prepares emergency response procedures and checklists.
2. UM prepares detailed recovery procedures and checklists.
3. UM stores the BCP in a geographically separate remote location.
4. UM develops a BCP distribution list and distributes copies of the BCP to key contingency personnel.
5. UM provides business continuity and crisis management awareness to all workforce members on an annual basis.

E. Testing the Business Continuity Plan

1. UM tests the BCP annually at a minimum, to ensure that it is up-to-date and effective.
2. UM defines testing exercises and testing scenarios.
3. UM ensures that all workforce members can perform their roles and carry out their responsibilities when the BCP is activated.
4. UM evaluates the results of BCP tests and provides a report to the Leadership Team, including improvement recommendations and resource requirements.

F. Maintaining the Business Continuity Plan

1. UM reviews and updates the BCP at a minimum annually.
2. UM updates the BCP with lessons learned during the testing exercises.
3. UM updates the BCP upon acquisition of new equipment, upgrading of systems, or other business events including but not limited to the following:
    - Changes in personnel, location, facilities, or resources
    - Revisions in legislation

- Updated processes and procedures
- Changes to operational and financial risk

4. UM distributes the updated BCP to key contingency personnel on the BCP distribution list.

Policy Compliance

Enforcement

The 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 (approved by committee) 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.

Business Continuity Management
HIPAA Policy: Security 04

Regulatory and Standards References

The following regulations and standards are applicable to this policy:

- **HIPAA Regulatory Reference**: HIPAA § 164.308(a)(1)(ii)(A), HIPAA § 164.308(a)(7)(i), HIPAA § 164.308(a)(7)(ii)(A), HIPAA § 164.308(a)(7)(ii)(B), HIPAA § 164.308(a)(7)(ii)(C), HIPAA § 164.308(a)(7)(ii)(D), HIPAA § 164.308(a)(7)(ii)(E), HIPAA § 164.310(a)(2)(i), HIPAA § 164.310(d)(2)(iv), HIPAA § 164.312(a)(2)(ii), HIPAA § 164.312(c)(1)
- **HITRUST Reference**: 12.a Including Information Security in the Business Continuity Management Process, 12.b Business Continuity and Risk Assessment, 12.c Developing and Implementing Continuity Plans Including Information Security, 12.d Business Continuity Planning Framework,
  12.e Testing, Maintaining and Re-Assessing Business Continuity Plans
- **PCI Reference**: PCI DSS v3 12.10.1

Related Documents:

- Business Continuity Plan
- Business Impact Analysis
- Disaster Recovery Plan
- Glossary
- Information Backup and Storage Policy

Approval

Chief Information Security Officer	<date>