Physical and Environmental Security
HIPAA Policy: Security 05

Summary: Outlines required physical protections for PHI in HIPAA covered entities

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to ensure that the University of Mississippi (UM) provides adequate physical and environmental safeguards to avoid damage or unauthorized access to confidential data and information assets.

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 UM facilities and to all UM information assets regardless of physical location.

1. Policy

A. Physical and Environmental Security Policy

1. UM prevents unauthorized physical access, damage, and interference with UM's premises and information assets.
2. UM develops and implements processes, procedures, and guidelines for implementing the physical and environmental protection policy.

B. Physical Security Perimeters

1. UM designs and implements physical security perimeters (e.g., controlled entrances) to protect areas that contain confidential data and information assets.
2. Walls are physically sound and of solid construction.

3. All external doors are protected against unauthorized entry with control mechanisms (e.g., alarms, locks etc.).
4. Doors to internal secure areas (e.g., data center, communications closets, etc.) make use of additional security measures as deemed appropriate by the Chief Information Security Officer (CISO). Examples of additional security measures include automatic locks, door delay alarms, and electronic locks (e.g., keypad, card swipe, etc.).
5. Windows that can be opened are kept locked and additional protection is considered for all accessible windows.

C. Physical Entry Controls

1. UM defines and protects secure areas with physical authentication controls to ensure that only authorized workforce members are allowed access.
2. UM develops and maintains a list of authorized workforce members based on individual job functions.
3. UM issues authorization credentials.
4. UM reviews and updates the access list and authorization credentials at a minimum every 90 days.
5. Where feasible, UM enforces physical access controls and maintains an audit trail of all access according to the *Audit, Logging, and Monitoring Policy*.
6. Third party support personnel are granted restricted access to secure areas. This access must be authorized and monitored.
7. All physical access devices (e.g., keys, access cards, combinations, etc.) must be returned, disabled, or changed when access is no longer authorized.
8. UM inventories physical access devices annually.

9. Combinations and keys are changed when keys are lost or combinations are compromised. If this is not feasible, a risk assessment is performed and documented.

D. Facility Security Maintenance Records Policy

1. UM maintains facility security maintenance records to document repairs and changes to physical elements of a facility related to security.
2. UM establishes procedures for maintaining such records in appropriate form.

E. Protecting Against External and Environmental Threats

1. UM designs and implements physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster.
2. UM designs and implements formal procedures to support physical and environmental protection controls.
3. Fire suppression systems (e.g., sprinklers, gas, etc.) and fire detection systems (e.g., smoke or heat activated) are installed, protected and maintained according to applicable laws and regulations.

F. Equipment Siting and Protection

1. Information assets are physically located to minimize potential damage from physical and environmental threats and hazards, and to minimize the opportunities for unauthorized access.
2. Guidelines for eating, drinking, and smoking in proximity to information assets are established.
3. Hazardous or combustible materials are stored at a safe distance from a secure area.
4. Bulk supplies such as printer paper, etc. are not stored within a secure area.

5. Backup information assets and media are stored at a safe distance from the main site to avoid damage from disaster affecting the main site.
6. Where feasible, lightning protection is applied to all buildings, and lightning protection filters (e.g., surge protectors) are fitted to all incoming power and communications lines.
7. Where feasible, information assets processing confidential data are positioned, and the viewing angle restricted, to reduce the risk of information being viewed by unauthorized persons.
8. Where deemed appropriate by the CISO, device locks (e.g., slot locks, port controls, peripheral switch controls, cable traps, etc.) are implemented for information assets containing confidential data.
9. Where feasible, UM restricts physical access to wireless access points, networking and communications hardware, and telecommunication lines.

G. Supporting Utilities

1. Information assets supporting critical business operations are protected from power failures and other disruptions caused by failures in supporting utilities (e.g., electricity, water supply, steam pipes, sewage, heating/ventilation, and air conditioning).
2. All supporting utilities are adequate for the systems they are supporting.
3. Supporting utilities are regularly inspected and tested to ensure their proper functioning and to reduce any risk from malfunction or failure.
4. A suitable electrical supply is provided that conforms to the equipment manufacturer's specifications.
5. An uninterruptable power supply (UPS) is required for information assets that support critical business operations to support orderly close down or transition to generators.
6. Power contingency plans cover the action to be taken on failure of the UPS.

7. UPS equipment and generators are regularly tested in accordance with the manufacturer's recommendations to ensure they have adequate capacity.
8. The water supply is stable and adequate to supply air conditioning, humidification equipment, and fire suppression systems.

H. Cabling Security

1. Where feasible, power and telecommunications cabling carrying data or supporting information services is protected from interception or damage.
2. Access to patch panels and cable rooms is controlled.
3. A patch list is developed and implemented to reduce the possibility of errors.
4. Clearly identifiable cable and equipment markings are used to minimize handling errors, such as accidental patching of wrong network cables.

I. Information Asset Maintenance

1. UM maintains its information assets to ensure continued availability and integrity.
2. UM develops and implements processes and procedures for information asset maintenance.
3. Information assets are maintained in accordance with the supplier's recommended service intervals and specifications.
4. Only authorized maintenance personnel carry out repairs and service information assets.
5. Appropriate controls (e.g., authorization levels) are implemented and take into account whether the maintenance is performed by workforce members or third parties.
6. UM establishes a process for requesting and approving access for maintenance personnel.

7. UM maintains a list of approved maintenance organizations and authorized maintenance personnel.
8. UM must ensure that maintenance personnel have authorization or UM must designate personnel with authorization to supervise maintenance.
9. Electronic and physical media containing covered information is securely sanitized prior to reuse, or if it cannot be sanitized, is destroyed prior to disposal.
10. UM complies with all requirements imposed by insurance policies regarding its information assets.

J. Remote Maintenance

1. UM approves and monitors remote maintenance and diagnostic activities.
2. UM employs strong identification and authentication techniques when establishing remote maintenance and diagnostic sessions.
3. UM does not allow the use of generic accounts by third parties unless noted by exception.
4. UM only allows the use of remote maintenance and diagnostic tools consistent with policy.
5. UM maintains records of remote maintenance and diagnostic activities.
6. UM terminates all remote sessions and network connections when maintenance is complete.

K. Security of Information Assets Off-Premises

1. Security is applied to off-site information assets taking into account the different risks of working outside of UM premises.

2. Regardless of ownership, the use of any information asset outside of UM's premises is authorized by the Leadership Team. This includes information assets used by remote workers, even where such use is permanent (i.e., a core feature of the employee's role).
3. Information assets and media taken off the premises are not left unattended in public places.
4. Portable computing devices (laptops, tablets, etc.) are carried as hand luggage and disguised where possible when travelling.
5. Manufacturers' instructions for protecting information assets is observed at all times (e.g., protection against exposure to strong electromagnetic fields).
6. Adequate insurance coverage is in place to protect information assets off-site.
7. Security risks (e.g., damage, theft or eavesdropping) may vary considerably between locations and is taken into account when determining appropriate controls.

L. Visitors

1. Escort visitors and third parties while on premises.
2. Accompany visitors at all times. Only allow visitors access to common areas or areas necessary to perform the function for which the visitor is in the facility.

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:

- **HIPAA Regulatory References**: HIPAA §164.308(a)(3)(ii)(A), HIPAA §164.310(a)(1), HIPAA §164.310(a)(2)(i), HIPAA §164.310(a)(2)(ii), HIPAA §164.310(a)(2)(iii), HIPAA §164.310(a)(2)(iv), HIPAA §164.310(b), HIPAA §164.310(c), HIPAA §164.310(d)(1), HIPAA §164.310(d)(2)(iii), HIPAA §164.312(c)(1)
- **HITRUST References**: 08.a Physical Security Perimeter, 08.b Physical Entry Controls, 08.c Securing Offices, Rooms, and Facilities, 08.d Protecting Against External and Environmental Threats, 08.e Working in Secure Areas, 08.f Public Access, Delivery, and Loading Areas, 08.g Equipment Siting and Protection, 08.h Supporting Utilities, 08.i Cabling Security, 08.j Equipment Maintenance, 08.k Security of Equipment Off-Premises, 08.m Removal of Property

Physical and Environmental Security
HIPAA Policy: Security 05

- **PCI References**: PCI DSS v3 9.1, PCI DSS v3 9.1.3, PCI DSS v3 9.2, PCI DSS v3 9.3, PCI DSS v3 9.4, PCI DSS v3 9.4.1, PCI DSS v3 9.4.2, PCI DSS v3 9.4.3, PCI DSS v3 9.4.4, PCI DSS v3 9.9, PCI DSS v3 9.9.2

Related Documents:

- Audit, Logging, and Monitoring Policy
- Clear Desk and Clear Screen Policy
- Glossary
- Incident Management Policy
- Record Retention Policy
- Secure Disposal Policy

Approval

Chief Information Security Officer	<date>