Access Control
HIPAA Policy: Security 07

Summary: Only individuals with proper authority should be able to access PHI

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to address University of Mississippi's (UM) requirements to manage and control access to information assets and information service in support of compliance with legal regulations (e.g., HIPAA) and to protect and lower risk to business operations.

The purpose of this policy is to ensure that UM's information assets and information services are properly protected against unauthorized access, while meeting the access requirements for all authorized users.

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 and users, including third parties, who may have access or exposure to UM's information assets are required to comply with this policy.

This policy covers access to all of UM's data regardless of whether that data is stored on or provided via UM information assets or on a third-party-hosted service or equipment.

Policy

A. Access Control Policy

1. UM develops and implements a formal access control program through policies and procedures. The access control program is reviewed and updated at least annually.
2. Access control rules account for and reflect UM's policies for information dissemination and authorization. Access control rules are supported by formal procedures and clearly defined responsibilities.

3. Non-Disclosure Agreements are signed by all employees before being allowed access to information assets.
4. Access control rules and rights for each user or group of users are clearly stated.
5. Access controls are both logical and physical and these are considered together.
6. Users and service providers are given a clear statement of the business requirements to be met by access controls.

B. User Registration

1. UM develops and implements a formal, documented process for establishing, activating, modifying, reviewing, disabling, and removing accounts. This user registration and de-registration process includes workforce member transfers, third party accounts, maintenance accounts, and external access.
2. UM grants access to information systems based on need-to-know, need-to-share, and least privilege.
3. UM grants access to information systems only after users are briefed on their security role(s)/responsibilities, conform with the terms and conditions of employment.
4. Proper user identification is required prior to establishing information system accounts and prior to approval of all such requests.
5. Proper user identification is required prior to establishing information system accounts and prior to approval for emergency access.
6. UM defines account types (e.g., individual, shared/group, system, application, and guest). Guest/anonymous and shared/group, accounts must be specifically authorized and monitored.

7. Default and unnecessary accounts (e.g., system, guest, vendor or other third party accounts) are removed, disabled, or otherwise secured (e.g., change the default passwords, reduce privileges to the lowest levels of access, etc.).
8. Users are given a written statement of their access rights, which they are required to sign stating they understand the conditions of access.

C. Privilege Management

1. The allocation and use of privileged access to information systems and services is restricted and controlled. Special attention is given to the allocation of privileged access rights, which allow users to override system controls.
2. The allocation of privileges is controlled through a formal access authorization process administered by the Department of Information Services.
3. The access privileges associated with each system (e.g., servers, SQL databases, individual applications, etc.) and the users to which they need to be allocated is identified.
4. Privileges are allocated to users based upon on work roles, job function, and business requirements. Privileges are granted based upon the minimum requirement for a user's functional role, and only when needed.
5. An authorization process and a record of all privileges allocated is maintained. Privileges are not granted until the authorization process is complete. Any exceptions must be noted and documented by the Chief Information Security Officer (CISO).

D. Review of Access Rights

1. User access rights are reviewed on a quarterly basis following a formal documented process.
2. User's access rights are reviewed after any changes such as transfer or termination of employment.
3. Reviews and follow-up actions are documented and submitted to the CISO.

4. Account managers are notified when users access rights change (e.g., termination, change in position) and modify the users account accordingly.

E. Remote Access

1. Where feasible, multi-factor authentication is implemented for all remote access according to the *Remote Access Policy*.
2. Where feasible, accounts for remote maintenance and remote administration are specifically authorized and disabled or deactivated when not in use.
3. Encrypted VPN solutions are implemented for remote access to UM's network.
4. Scans to identify and review any unauthorized remote access connections are performed every six months.

F. Remote Diagnostic and Configuration Port Protection

1. Physical and logical access to diagnostic and configuration ports is controlled.
2. Where feasible, access to network equipment is physically protected (e.g., a router must be stored in a room that is only accessible by authorized workforce members or third parties) such that remote diagnostic and configuration ports are protected.
3. Logical access to remote management of network equipment is protected.
4. Ports, services, and similar applications installed on a network system, which are not specifically required for business functionality, are disabled or removed.

G. Network Segregation

1. Where feasible, groups of information services, users, and information systems are segregated on networks.

2. Firewalls are used to maintain segregation between internal network segments and external network segments (e.g., the Internet) and enforce access control policies for each of the domains.
3. UM's network is logically segmented by a defined security perimeter and traffic is controlled based on functionality required and classification of the associated data, applications, or systems.
4. Network segregation architecture and security design logic are documented and reviewed annually.

H. Network Connection Controls

1. For shared networks, especially those extending across UM boundaries, the capability of users to connect to the network is restricted, in line with the access control policy and requirements of the business applications.
2. At external network interfaces, inbound network traffic is denied by default and allowed by exception (i.e., deny all, permit by exception).
3. Network traffic is controlled through firewall and other network-related restrictions.
4. Transmitted information is secured in accordance with the *Data Classification and Handling Policy*.

I. Secure Log-on Procedures

1. Access to operating systems is controlled by a secure log-on procedure.

J. User Identification and Authentication

1. UM requires unique user IDs for all types of users (e.g., employees, contractors, third parties, etc.), and duplicate user IDs must not be issued to other users.
2. Users are uniquely identified and authenticated for both local and remote access to information systems.

3. Third party users, or processes acting on behalf of third party users, are uniquely identified and authenticated.
4. Actions that can be performed without identification and authentication are permitted by exception when done in accordance with the *Information Security Waiver Policy*.
5. Users who perform privileged functions (e.g., system administration) are to use separate accounts when performing those privileged functions. Do not perform regular user activities from privileged accounts.

K. Session Time-out

1. A screen saver locks the screen after a maximum of fifteen minutes of inactivity on workstations and auto login computers.
2. The system requires the user to re-establish access using appropriate identification and authentication procedures (*workstation*).

L. Information Access Restriction

1. Logical and physical access to information and application systems and functions by users and support personnel is restricted in accordance with the defined *Access Control Policy*.
2. Associated identification and authentication controls are developed, disseminated, and periodically reviewed and updated.

M. Termination of Access

1. Upon termination of employment for employees, contractors, third party users or other workforce arrangement, physical and logical access rights and associated materials are removed or modified to restrict access within 24 hours and delete old accounts after 90 days of opening new accounts.
2. Emergency terminations will have their physical and logical access rights removed immediately if required.

Policy Compliance

Enforcement

The 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 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 Reference**: HIPAA §164.308 (a)(3)(i), HIPAA §164.308 (a)(3)(ii)(a), HIPAA §164.308 (a)(4)(i), HIPAA §164.308 (a)(4)(ii)(B), HIPAA §164.308(a)(3)(i), HIPAA §164.308(a)(3)(ii)(A), HIPAA §164.308(a)(3)(ii)(B), HIPAA §164.308(a)(3)(ii)(C), HIPAA §164.308(a)(4)(i), HIPAA §164.308(a)(4)(ii)(A), HIPAA §164.308(a)(4)(ii)(B), HIPAA §164.308(a)(4)(ii)(C), HIPAA §164.308(a)(5)(ii)(D), HIPAA §164.310(a)(2)(iii), HIPAA §164.310(b), HIPAA §164.312(a)(1), HIPAA §164.312(a)(2)(i), HIPAA §164.312(a)(2)(ii), HIPAA

§164.312(a)(2)(ii)(i), HIPAA §164.312(a)(2)(ii)(iv), HIPAA §164.312(a)(2)(iii), HIPAA §164.312(a)(2)(iv), HIPAA §164.312(d)

- **HITRUST Reference**: 01.a Access Control Policy, 01.b User Registration, 01.c Privilege Management, 01.e Review of user Access Rights, 01.i Policy on the Use of Network Services, 01.j User Authentication for External Connections, 01.l Remote Diagnostic and Configuration Port Protection, 01.m Segregation in Networks, 01.n Network Connection Control, 01.o Network Routing Control, 01.p Secure Log-on Procedures, 01.q user Identification and Authentication, 01.s Use of System Utilities, 01.t Session Time-out, 01.u Limitation of Connection Time, 01.v Information Access Restriction, 01.w Sensitive System Isolation
- **PCI Reference**: PCI DSS v1.2 8.5, PCI DSS v1.2 8.5.8, PCI DSS v3 1.1.4, PCI DSS v3 1.2, PCI DSS v3 1.2.1, PCI DSS v3 2.2.1, PCI DSS v3 2.3, PCI DSS v3 7.1, PCI DSS v3 7.1.1, PCI DSS v3 7.1.4, PCI DSS v3 7.2.1, PCI DSS v3 7.2.2, PCI DSS v3 8.1.1, PCI DSS v3 8.1.2, PCI DSS v3 8.1.3, PCI DSS v3 8.1.4, PCI DSS v3 8.1.5, PCI DSS v3 8.1.6, PCI DSS v3 8.1.7, PCI DSS v3 8.1.8, PCI DSS v3 8.2, PCI DSS v3 8.2.2, PCI DSS v3 8.3, PCI DSS v3 8.5, PCI DSS v3 8.5.1, PCI DSS v3 8.6, PCI DSS v3 8.7, PCI DSS v3 12.3.2, PCI DSS v3 12.3.8, PCI DSS v3 12.3.9, PCI DSS v3 12.3.10

Related Documents:

- Audit, Logging and Monitoring Policy
- Data Classification Policy
- Data Classification and Handling Policy
- Encryption Policy
- Glossary
- Mobile Computing Device Policy
- Network Protection Policy
- New Hire Checklist
- Remote Access Policy
- Sanctions Policy
- Termination Checklist
- Termination Policy

Access Control
HIPAA Policy: Security 07

Approval

Chief Information Security Officer	<date>
Chief Information Security Officer	<date>