Network Protection
HIPAA Policy: Security 15

Summary: Ensuring PHI is protected in HIPAA covered entities by protecting networks and supporting infrastructure

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to ensure the protection of University of Mississippi (UM) data, especially confidential data in UM's networks, and protection of the supporting network infrastructure.

The secure management of UM's network requires careful consideration of the flow of information and the regulatory requirements regarding monitoring and protection of its networks.

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 users and computing devices connecting to any UM information systems network.

Policy

A. Network Controls

1. UM manages and controls its networks in order to protect UM data and other information assets that access, traverse, or reside within UM's network.
2. UM specifies the networks and network services to which users are authorized access.
3. A current network diagram exists of the covered entity areas and is updated whenever there are network changes and no less than every 6 months.
4. The network diagram is made immediately and continuously available for official operational, planning, and coordination purposes. The network diagram is classified as

internal-use-only and is handled in accordance with the *Data Classification and Handling Policy*.

5. All databases, servers and other system components storing or processing confidential data are placed behind a firewall to limit external network traffic to the internal network.
6. Routing controls are implemented through security gateways (e.g., firewalls) used between internal and external networks (e.g., the Internet and 3rd party networks).
7. Changes to the DMZ which affect the security posture are approved by the Chief Information Security Officer (CISO) and documented in the network diagram.
8. UM's confidential data is logically and/or physically partitioned by means of network architecture design and connectivity except where the risk of not doing so is accepted by the CISO.
9. Where feasible, network devices are identified and authenticated prior to establishing a connection.
10. Firewalls are configured to deny inbound traffic by default (deny all, permit by exception).
11. Servers hosting UM confidential data are not visible to the internet, nor to unprotected internal subnets.
12. The firewall rule set is reviewed periodically.
13. Firewalls restrict inbound traffic to the minimum necessary.
14. UM utilizes firewalls that employ stateful packet inspection.
15. Firewall and router baseline configuration standards are defined and implemented and reviewed annually.
16. Firewall, router, and network connection changes are approved and tested prior to implementing the changes. Changes are documented in accordance with the *Configuration Management Policy*. If testing cannot be accomplished prior to implementation, the

proposed changes and a rollback plan must be approved by the CISO prior to implementation.

17. Where feasible, UM uses at least two different DNS servers for internal name resolution.
18. Semi-annual network scans are performed to identify unauthorized components and devices.

B. Security of Outsourced Network Services

1. Security features, service levels, and management requirements for all network services are identified and included in any network services agreement.

2. Formal agreements with third party network service providers includes specific obligations for security and privacy.
3. Services provided by a third party network service provider are formally managed and regularly monitored to ensure they are in accordance with the terms of the formal agreements.

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 at any time (approval by committee), 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 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 shall 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(b)(1), HIPAA §164.308(b)(3), HIPAA §164.312(a)(2)(i), HIPAA §164.312(c)(1), HIPAA §164.312(c)(2), HIPAA §164.312(d), HIPAA §164.312(e)(1), HIPAA §164.312(e)(2)(i), HIPAA §164.312(e)(2)(ii), HIPAA §164.314(a)(1), HIPAA §164.314(a)(2)(ii)
- **HITRUST References**: 09.m Network Controls, 09.n Security of Network Services
- **PCI References**: PCI DSS v3 1.1.1, PCI DSS v3 1.1.2, PCI DSS v3 1.1.3, PCI DSS v3 1.1.4, PCI DSS v3 1.1.5, PCI DSS v3 1.1.6, PCI DSS v3 1.1.7, PCI DSS v3 1.2, PCI DSS v3 1.2.1, PCI DSS v3 1.2.2, PCI DSS v3 1.2.3, PCI DSS v3 1.3, PCI DSS v3 1.3.1, PCI DSS v3 1.3.2, PCI DSS v3 1.3.3, PCI DSS v3 1.3.4, PCI DSS v3 1.3.5, PCI DSS v3 1.3.6, PCI DSS v3 1.3.7, PCI DSS v3 1.3.8, PCI DSS v3 2.1.1, PCI DSS v3 4.1.1, PCI DSS v3 11.1, PCI DSS v3 11.4

Related Documents:

- Access Control Policy
- Configuration Management Policy
- Data Classification and Handling Policy
- Glossary

Network Protection
HIPAA Policy: Security 15

Approval

Chief Information Security Officer	<date>