Wireless Network Security
Security Policy No. 16

Summary: UM permits wireless access to systems containing PHI

Affected Individuals: Employees in HIPPA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to ensure the protection of data in wireless networks and the protection of the University of Mississippi's (UM) network infrastructure that supports wireless access services.

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 network.

Remote work and security requirements for wireless connections outside of UM's premises (e.g., home networks, hot spots, hotel networks, etc.) are outside the scope of this policy.

Policy

A. Network Controls
   1. Business practices for the secured wireless network security include:
      - Only Pre-Defined MAC addresses are permitted to connect to the network
      - The Protected Network SSID in not Broadcast
      - Connection is via a no less than 16 character WPA2 passphrase that is changed on a periodic basis
      - Configuring access points (APs) to protect against common threats, vulnerabilities, and exposures
      - Using encryption standards such as AES, Triple Des, and Blowfish

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, 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 §164.312(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)
- **HITRUST References**: 07.a Inventory of Assets, 09.m Network Controls
- **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 1.2, PCI DSS v3 1.2.1, PCI DSS v3 1.2.2, PCI DSS v3 1.2.3, PCI DSS v3 2.1.1, PCI DSS v3 4.1.1, PCI DSS v3 11.1

Related Documents:

Wireless Network Security
Security Policy No. 16

- Data Classification and Handling Policy
- Glossary
- Incident Management Policy
- Wireless Network Diagram

Approval

Chief Information Security Officer	<date>