Remote Working
HIPAA Policy: Security 10

Summary: Outlines limitations on working remotely in HIPAA covered entities

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to support the security of University of Mississippi (UM) confidential data by limiting remote working activities to explicitly approved processes and circumstances.

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 Workforce and users that work remotely.

Policy

A. Remote Work Policy

1. UM allows workforce members to work remotely if the manager determines that remote working allows work to be performed effectively and productively.
2. Remote working is a privilege, not a benefit or a right. UM has the right to terminate a remote working arrangement at any time.
3. Participation in remote working is voluntary. Workforce members have the right to decline remote working unless the Business Continuity Plan (BCP) has been activated, in which case UM determines if remote working from an alternate site is mandatory for the duration of time that the BCP is active.

B. Working Remotely

1. UM develops and implements remote working operational plans, procedures, and guidelines.

2. Remote working activities are only authorized if appropriate security arrangements and controls are in place, and if they comply with UM's information security policies.
3. Remote workers receive training on security awareness, privacy, and their additional responsibilities while remote working.
4. UM provides information assets for remote working that are only used for UM purposes by authorized workforce members.
5. The use of UM's information assets by other persons (e.g., family, friends, etc.) is strictly prohibited.
6. Except as allowed by the *Mobile Computing Device Security Policy*, the use of personally-owned equipment that is not under the control of UM to conduct remote work involving UM confidential data is strictly prohibited.
7. Upon termination of remote working activities, access rights are reviewed and acted upon in accordance with the *Access Control Policy*.
8. Upon termination of remote working activities, all UM information assets related to the remote work are returned to UM within 14 business days and no later than 30 days.
9. Suitable protection of the remote working site is in place to protect against the theft of information assets and the unauthorized disclosure of confidential data:
    - The configuration of wireless network services is encrypted (WPA at a minimum).
    - Anti-virus protection and operating system and application patching are consistent with UM's information security policies.
10. Remote access for teleworkers complies with UM's *Remote Access Policy*.

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 may be granted by the CISO 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 §164.310(a)(2)(i), HIPAA §164.310(b)
- **HITRUST Reference**: 01.y Teleworking

Remote Working
HIPAA Policy: Security 10

Related Documents:

- Access Control Policy
- Business Continuity Management Policy
- Glossary
- Remote Access Policy

Approval

Chief Information Security Officer	<date>