Remote Access
HIPAA Policy: Security 21

Summary: Outlines requirements for protecting PHI in HIPAA covered entities with remote access

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to establish how University of Mississippi (UM) ensures the security of remote access to UM's network in order to protect 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 is applicable to all users who work outside of UM's environment, who connect to the UM's network, systems, applications, and data, including but not limited to applications that contain confidential data, from a remote location.

Policy

A. Remote Access Policy

1. UM manages and controls access to its internal and external networks. Users are only provided with access to internal and external networks that they have been specifically authorized to use. Appropriate authentication methods are used to control access by remote users.
2. All users who connect to UM's networks from a remote location only use approved and managed secure remote access technologies, as determined by the Chief Information Security Officer (CISO).
3. Where feasible, all remote access by workforce members use multi-factor authentication mechanisms. Any exceptions are documented and approved by the CISO.

4. Remote access users are responsible for adhering to all of UM's policies, not engaging in illegal activities, and not using remote access for interests other than those of UM.
5. Violation of this policy by remote access users may result in corrective disciplinary action, up to and including termination of employment and/or removal of access to UM's information assets according to the *Sanctions Policy*.
6. Violation of this policy by others, including providers, providers' offices, Business Associates, and partners may result in termination of the relationship and/or associated privileges.
7. Violation of this policy may also result in civil and criminal penalties as determined by federal and state laws and regulations.

B. Requesting Remote Access

1. Remote access is strictly controlled and only granted to workforce members with a defined business need.
2. Where required, workforce members register for a multi-factor authentication mechanism (e.g., token).
3. Business Associates and other third parties (e.g. contractors, vendors) are granted remote access provided they have a contract with UM which clearly defines the type of remote access permitted (e.g., stand-alone host, network server, etc.) as well as other conditions which may be required, such as virus protection software. Such contractual provisions must be reviewed and approved by the CISO before remote access is permitted.
4. Remote access is strictly controlled and made available only to Business Associates and other third parties with a defined business need, at the discretion of and approval by the CISO.
5. All users granted remote access privileges must sign and comply with the *Confidentiality Agreement* kept on file with Human Resources.
6. Remote access accounts that have shown no activity for 90 days are automatically disabled.

C. Remote Security

1. Connectivity from a user's remote location to UM's network is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees necessary for enabling their connectivity from the remote location.
2. All computing devices that remotely connect to UM's network must apply the most up- to-date anti-malware software and security patches. This includes personally-owned computing devices (e.g., laptops, home computers, tablets, smartphones, etc.). For computing devices using a Microsoft Operating System, all UM-endorsed Microsoft security patches must be applied and kept current.
3. Remote users ensure that remote worksites meet security and configuration standards established by UM. This includes configuration of personal routers and wireless networks.
4. Remote users that connect to UM's network must configure the equipment to comply with UM's policies.
5. Malware updates and security patching must be allowed to complete, i.e., remote users may not stop the update process on UM's computer devices or on personal computing devices.
6. A host-based firewall is used on all computing devices connecting remotely to UM's network and may not be disabled without the explicit approval of the CISO.
7. UM maintains remote access logs according to the *Audit, Logging, and Monitoring Policy*.
8. System Administrators review remote access logs to detect suspicious activity.
9. Encryption is used to protect the confidentiality and integrity of remote access sessions to the internal network and to external systems.

D. Remote Privacy

1. Only authorized users are permitted remote access to any of UM's computer systems, computer networks, and/or information, and must adhere to all of UM's policies.
2. Remote users, including Business Associates and other third parties, log-off and disconnect from UM's network when access is no longer required to perform job responsibilities.
3. Remote users lock the workstation and/or system(s) when unattended so that no other individual is able to access any Protected Health Information (PHI) or other confidential data.
4. Where possible, remote access users are automatically disconnected from the UM network when there is no recognized activity for 15 minutes.
5. Remote access users ensure that unauthorized individuals do not access UM's network. At no time does any remote access user provide their username or password to anyone, nor do they configure their remote access device to remember or automatically enter their username and password.
6. Remote access users must take necessary precautions to secure all of UM's information assets and confidential data in their possession.

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 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 Reference**: HIPAA § 164.312(e)(1)
- **HITRUST References**: 01.j User Authentication for External Connections, 01.y Teleworking, 09.s Information Exchange Policies and Procedures

Related Documents:

- Access Control Policy
- Audit, Logging, and Monitoring Policy
- Business Associate Agreement (BAA) Template
- Confidentiality Agreement Template
- Encryption Policy
- Glossary
- Sanctions Policy

Remote Access
HIPAA Policy: Security 21

Approval

Chief Information Security Officer	<date>