Mobile Computing Device Security
HIPAA Policy: Security 20

Summary: Protecting PHI on mobile devices

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to establish security measures for the University of Mississippi (UM) that protect against the risks of using mobile computing devices.

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 mobile computing devices that connect to UM's network and access confidential data.

All workforce members and users utilizing mobile computing devices connecting to UM's network and accessing confidential data assume the responsibility for the security of information contained within.

Policy

A. Mobile Computing Device Policy

1. UM manages and controls use of mobile computing devices, and appropriate security measures are adopted to protect against the risks of using mobile computing devices.
2. Usage of mobile computing devices must comply with all international, federal and state laws, and UM policies. Unauthorized disclosure of confidential data may violate federal and/or state laws, and/or ethical standards, and may cause injury.
3. Unauthorized disclosure may result in disciplinary and/or legal actions being taken, including but not limited to termination of privileges and/or employment in accordance with the *Sanctions Policy*.

B. Bring Your Own Device (BYOD) Mobile Computing Device Policy

1. Mobile computing devices that are personally owned by workforce members are the responsibility of the owner of that device.
2. The owner of any personally-owned mobile computing device connected to UM's information assets (e.g., network, email system, website, etc.) are fully responsible for the behavior of all users on the mobile computing device, and for all data and network traffic accessed or transmitted to and from the mobile computing device, regardless of whether the owner is aware of the data and network traffic.
3. Personally-owned mobile computing devices may connect to UM's network and access confidential data in accordance with this policy and associated procedures.
4. Personally-owned mobile computing devices may be subject to additional restrictions or security measures as determined by the Chief Information Security Officer (CISO).

C. Business Mobile Computing Device Policy

1. Mobile computing devices issued by UM for business purposes remain the property of UM.
2. When the business mobile computing device is allocated, the user assumes responsibility for physical security of the device and any UM data contained within.
3. Prior to no longer being employed by UM, the user returns the mobile device in accordance with the *Termination Policy*.
4. All business mobile computing devices must be disposed of in accordance with the *Secure Disposal Policy* after they reach end of life.

D. Acceptable Use Policy

1. The *Information Technology Acceptable Use Policy* applies to all mobile computing devices regardless of ownership.

2. Users are responsible for ensuring mobile computing device applications and multimedia capabilities are not used to breach privacy and confidentiality according to the *Information Technology Acceptable Use Policy*.
3. Users must agree to take responsibility for the security of their mobile computing device and UM data contained therein.
4. Users have no expectation of privacy associated with any of UM data they store in or send through mobile computing devices.
5. Users are not permitted to bypass, or attempt to bypass, security protections on mobile computing devices connected to UM's network or communication systems.
6. Users are responsible for ensuring that confidential data is only transmitted using approved/secure communication functions including UM email.
7. Users of mobile computing devices connected to UM's email must ensure that UM data is erased when the device is no longer being used for UM business.

E. Physical Protection Policy

1. Any mobile computing device containing confidential data is not left unattended in public areas (e.g., vehicles, hotel rooms, conference rooms, airports, etc.), even for a short period of time, without being physically protected.
2. All mobile computing devices containing confidential data are carried as hand luggage when traveling and never checked as baggage nor stored anywhere prohibiting immediate access or visual contact with the device.
3. In the event that a mobile computing device containing confidential data is lost or stolen, the incident must be reported according to the *Incident Management Policy*.
4. UM implements procedures that take into account legal, insurance, and other security requirements for cases of theft or loss of mobile computing devices containing confidential data.

F. Public Places

1. Physical protection is in place when using mobile computing devices in public places, meeting rooms and other unprotected areas outside of UM premises to avoid the unauthorized access to or disclosure of confidential information.
2. Users of mobile computing devices containing confidential data take care to avoid the unintentional disclosure of confidential information to unauthorized persons in public places.

G. Access Controls

1. All mobile computing devices require authentication (e.g., password, pin number, biometric, etc.). All mobile computing devices must enter authentication credentials prior to accessing the UM guest network.
2. All mobile computing devices automatically time out after no more than five minutes of inactivity according to the *Access Control Policy*. If locked, the device require re- authentication to unlock.

H. Encryption

1. All mobile devices are encrypted according to the *Encryption Policy*.
2. If encryption is not reasonable and appropriate, UM documents the acceptance of risk.

I. Endpoint Protection Policy

1. All users are responsible for ensuring mobile computing devices are compliant with the *Endpoint Protection Policy*.
2. All users are responsible for ensuring Operating System updates and security patches for mobile computing devices are kept up-to-date.

J. Network Connections

1. UM only authorizes connections of mobile computing devices to UM's network if the devices meet the requirements of this policy.
2. Mobile computing devices that remotely access UM's network comply with the *Remote Access Policy*.
3. If UM has reason to believe that a mobile computing device connected to UM's network is using information asset resources inappropriately, or is acting in violation of federal and state laws or regulations, network traffic to and from that mobile computing device may be monitored. If justified, the mobile computing device is disconnected from UM's network, and appropriate actions are taken in accordance with the *Sanctions Policy* and federal and state law and regulations.

K. Security Awareness Training

1. Training is provided for workforce members using mobile computing devices according to the *Security Awareness and Training Policy* in order to raise awareness on the additional risks resulting from this way of working and the mobile device controls that are implemented.

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 (approval by committee) 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 Reference: HIPAA § 164.310 (b)
- HITRUST Reference: 01.x Mobile Computing and Communications
- PCI Reference: PCI DSS v3 1.4

Related Documents:

- □ Information Technology Acceptable Use Policy
- □ Access Control Policy
- □ Encryption Policy
- □ Endpoint Protection Policy
- □ Glossary
- □ Incident Management Policy
- □ Remote Access Policy
- □ Sanctions Policy
- □ Secure Disposal Policy
- □ Security Awareness and Training Policy
- □ Termination Policy

Approval

____ ____________________

Chief Information Security Officer <date>