Security Awareness and Training
HIPAA Policy: Security 06

Summary: Outlines requirements for security training for HIPAA covered entities and the IT staff who support those units

Affected Individuals: Employees of HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to ensure security awareness and training programs are developed and implemented, including in-depth training for personnel with significant information security responsibilities.

University of Mississippi (UM) is committed to ensuring that workforce members are properly trained and made aware of security policies, procedures, potential threats, and security incidents.

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 workforce members, users and all personnel affiliated with third parties regardless of physical location.

Policy

A. Training and Awareness Policy

1. UM develops and implements training to ensure that all workforce members and third party users are aware of the security risks associated with their activities and of the applicable laws, directives, policies, standards, instructions, regulations, and procedures.
2. UM implements strategies for protecting information assets and confidential data including security awareness, education, and training.
3. UM provides specialized training for workforce members whose job functions require specialized skill or knowledge in information security.

4. UM retains records of all training activities.
5. UM conducts an annual review of the effectiveness of its training and awareness activities.

B. Information Security Training

1. Prior to being granted access to UM's confidential information, workforce members and third party users:
   - Receive security training
   - Acknowledge receipt of such training
   - Acknowledge awareness of responsibilities under UM's policies regarding confidential information.
2. All workforce members and third party users receive security training as part of initial training for new users, when required by system changes, and annually thereafter.
3. All workforce members and third party users receive training on UM's policies and procedures no later than 30 days after hire and annually thereafter.
4. Managers ensure that their workforce members receive sufficient training to remain up-to-date on issues, requirements, expectations, and procedures for protecting information assets.
5. UM maintains ongoing security awareness by publishing security bulletins and posters, conducting safety fairs, ad-hoc presentations, or monthly meetings.
6. UM reviews training materials on an annual basis or whenever there is a change in regulatory controls and updates as necessary.
7. Workforce members acknowledge that they have received security training and are aware of their responsibilities by signing an acceptance or acknowledgement of their security responsibilities.

C. Information Security Workforce Members Training

1. All information security workforce members receive specialized training regarding their roles and responsibilities as part of their initial training, when required by system changes, and annually thereafter.
2. UM provides or coordinates training for workforce members whose job functions require special knowledge of security threats, risks, vulnerabilities, techniques, and safeguards. This training focuses on expanding knowledge, skills, and abilities for workforce members who are assigned information security roles and/or responsibilities.
3. All information security workforce members receive specialized training prior to accessing information assets. A refresher training course will also need to be completed annually by all information security workforce members.
4. All information security workforce members receive regular updates regarding policies and procedures relevant to their job function.

D. Incident Response Training

1. All workforce members and third party users receive mandatory incident response training within 90 days of assuming an incident response role or responsibility, when required by system changes, and annually thereafter according to the *Incident Management Policy*.

E. Information Technology (IT) Acceptable Use Training

1. Workforce members shall receive training on the acceptable uses of information assets in accordance with the *IT Acceptable Use Policy* prior to being granted access to UM's information assets.
2. At a minimum, Workforce Members receive training and periodical reminders:

    a. To not leave confidential data on system output devices (e.g., copiers, printers, and facsimile machines).

b. That facsimile machines and photocopiers have page caches and may store pages in case of a paper or transmission fault, which may later be printed in full view once the fault is cleared.

c. Regarding using facsimile machines securely, namely to avoid:

- Sending documents and messages to the wrong number either by misdialing or using the wrong stored number.
- Unauthorized access to built-in message stores while retrieving messages.
- Deliberate or accidental programming of machines to send messages to specific numbers.

d. Not to use UM demographic data for personal use.

Policy Compliance

Enforcement

The Chief Information Security Officer (CISO) 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 §164.308 (a)(5)(i), HIPAA §164.308 (a)(5)(ii)(A), HIPAA §164.308 (a)(5)(ii)(B), HIPAA §164.308 (a)(6)(i), HIPAA §164.308 (a)(7)(ii)(D), HIPAA §164.310(b), HIPAA §164.414(a), HIPAA §164.530(b)
- **HITRUST References**: 02.e Information Security Awareness, Education and Training, 09.s Information Exchange Policies and Procedures
- **PCI References**: PCI DSS v3 4.1, PCI DSS v3 4.1.1, PCI DSS v3 6.5, PCI DSS v3 9.9, PCI DSS v3 9.9.3, PCI DSS v3 12.6, PCI DSS v3 12.6.1, PCI DSS v3 12.6.2

Related Documents:

- IT Acceptable Use Policy
- Glossary
- Incident Management Policy

Approval

Chief Information Security Officer

<date>

Security Awareness and Training
HIPAA Policy: Security 06