**Purpose**

The purpose of this policy is to establish guidelines for maintaining the privacy, security, and integrity of electronic protected health information (ePHI) in compliance with the Health Insurance Portability and Accountability Act (HIPAA).

**Scope**

This policy applies to all employees, contractors, business associates, and outsourced providers of [Your Organization’s Name] who handle ePHI.

**Approval**

This policy has been approved by the Organization’s security requirements and the HIPAA security requirements. Policy is effective as of the date indicated below.

**Effective Date**: Date  
**Approved By**: Name/Title

**Review, Update, and Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description of Change | Approved By |
| 1.0 | 6/2/2024 | Initial Draft. | MC3 Technologies |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Administrative Safeguards 2](#_Toc173763191)

[1.1 Security Management Process 3](#_Toc173763192)

[1.1 Assigned Security Responsibility 3](#_Toc173763193)

[1.2 Workforce Security 3](#_Toc173763194)

[1.3 Information Access Management 3](#_Toc173763195)

[1.4 Security Awareness and Training 3](#_Toc173763196)

[1.5 Security Incident Procedures 3](#_Toc173763197)

[1.6 Contingency Plan 4](#_Toc173763198)

[1.7 Evaluation 4](#_Toc173763199)

[2. Business Associate Contracts and Other Arrangements 4](#_Toc173763200)

[2.1. Outsourced Provider Agreements 4](#_Toc173763201)

[3. Physical Safeguards 5](#_Toc173763202)

[3.1 Facility Access Controls 5](#_Toc173763203)

[3.2 Workstation Use 5](#_Toc173763204)

[3.3 Workstation Security 5](#_Toc173763205)

[3.4 Device and Media Controls 5](#_Toc173763206)

[4. Technical Safeguards 6](#_Toc173763207)

[4.1 Access Control 6](#_Toc173763208)

[4.2 Audit Controls 6](#_Toc173763209)

[4.3 Integrity 6](#_Toc173763210)

[4.4 Person or Entity Authentication 6](#_Toc173763211)

[4.5 Transmission Security 6](#_Toc173763212)

[5. Organizational Requirements 7](#_Toc173763213)

[5.1 Business Associate Contracts or Other Arrangements 7](#_Toc173763214)

[5.2 Outsourced Provider Agreements 7](#_Toc173763215)

[6. Policies and Procedures and Documentation Requirements 8](#_Toc173763216)

[6.1 Policies and Procedures 8](#_Toc173763217)

[6.2 Documentation 8](#_Toc173763218)

[Policy Enforcement 9](#_Toc173763219)

[Review and Revision 9](#_Toc173763220)

[Definitions 9](#_Toc173763221)

1. Administrative Safeguards

*Organization shall:*

1.1 Security Management Process

* Conduct a risk analysis to identify potential risks and vulnerabilities to ePHI.Implement risk management measures to reduce identified risks.Apply sanctions to workforce members who fail to comply with security policies.Regularly review information system activity, including audit logs and security incident tracking reports.

1.1 Assigned Security Responsibility

* Designate a security official responsible for developing and implementing security policies and procedures.

1.2 Workforce Security

* Implement procedures to ensure appropriate access for workforce members and prevent unauthorized access.
* Supervise workforce members to ensure compliance with security policies.
* Establish procedures for determining and managing access rights for workforce members.
* Implement termination procedures to revoke access to ePHI when employment ends.

1.3 Information Access Management

* Implement policies for authorizing access to ePHI based on the user’s role or function.
* Ensure ePHI is isolated from unauthorized personnel.
* Document, review, and modify user access rights as needed.

1.4 Security Awareness and Training

* Implement a security awareness and training program for all workforce members.
* Provide regular security reminders and training on protecting against malicious software, monitoring log-in attempts, and password management.

1.5 Security Incident Procedures

* Implement procedures to identify, respond to, and mitigate security incidents.
* Document and report security incidents and their outcomes.

1.6 Contingency Plan

* Develop and implement a contingency plan to respond to emergencies affecting systems containing ePHI.
* Establish data backup, disaster recovery, and emergency mode operation plans.
* Periodically test and revise contingency plans.
* Conduct applications and data criticality analysis.

1.7 Evaluation

* Perform periodic technical and non-technical evaluations to ensure compliance with the security policies and procedures.

2. Business Associate Contracts and Other Arrangements

*Organization shall:*

2.1. Outsourced Provider Agreements

Ensure that outsourced providers comply with HIPAA security requirements through written agreements.

Verify that outsourced providers implement appropriate safeguards to protect ePHI.

Require outsourced providers to promptly report any security incidents involving ePHI to [Your Organizations Name].

3. Physical Safeguards

*Organization shall:*

3.1 Facility Access Controls

* Implement procedures to limit physical access to facilities housing ePHI to authorized personnel.
* Develop a facility security plan to protect against unauthorized access, tampering, and theft.
* Document maintenance and repair activities for facility components related to ePHI security.

3.2 Workstation Use

* Define and implement policies specifying the proper use of workstations that access ePHI.

3.3 Workstation Security

* Implement physical safeguards to restrict access to workstations containing ePHI to authorized users.

3.4 Device and Media Controls

* Implement policies for the receipt, removal, disposal, and reuse of hardware and electronic media containing ePHI.
* Maintain accountability records for hardware and electronic media movements.
* Ensure proper data backup and storage procedures.

4. Technical Safeguards

*Organization shall:*

4.1 Access Control

* Implement technical policies and procedures to control access to ePHI.
* Assign unique user IDs and establish emergency access procedures.
* Implement automatic logoff and encryption/decryption mechanisms.

4.2 Audit Controls

* Implement mechanisms to record and examine activity in information systems containing ePHI.

4.3 Integrity

* Implement policies to protect ePHI from improper alteration or destruction.
* Implement electronic mechanisms to ensure ePHI integrity.

4.4 Person or Entity Authentication

* Implement procedures to verify the identity of persons or entities seeking access to ePHI.

4.5 Transmission Security

* Implement technical security measures to protect ePHI during electronic transmission.
* Ensure integrity controls and encryption are in place.

5. Organizational Requirements

*Organization shall:*

5.1 Business Associate Contracts or Other Arrangements

* Ensure that business associates safeguard ePHI through written contracts or other arrangements, outlining permissible uses and required safeguards.

5.2 Outsourced Provider Agreements

* Establish written agreements with outsourced providers to ensure they comply with HIPAA security requirements.
* Require outsourced providers to implement appropriate safeguards to protect ePHI.
* Mandate that outsourced providers promptly report any security incidents involving ePHI to [Your Organizations Name].

6. Policies and Procedures and Documentation Requirements

*Organization shall:*

6.1 Policies and Procedures

* Develop and implement reasonable and appropriate policies and procedures to comply with HIPAA standards.

6.2 Documentation

* Maintain written documentation of policies and procedures.
* Retain documentation for at least six years.
* Make documentation available to those responsible for implementing procedures.
* Periodically review and update documentation in response to changes affecting ePHI security.

Policy Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment or contract, as well as potential legal action.

Review and Revision

This policy will be reviewed annually and revised as needed to ensure continued compliance with HIPAA regulations.

Definitions

* **ePHI**: Electronic Protected Health Information.
* **Business Associate**: A person or entity that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involves the use or disclosure of ePHI.
* **Workforce**: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for [Your Organizations Name], is under the direct control of [Your Organizations Name].
* **Covered Entity**: Health plans, healthcare clearinghouses, and healthcare providers who transmit any health information in electronic form.
* **Outsourced Provider**: A third-party service provider engaged by [Your Organizations Name] to perform functions or activities involving the use or disclosure of ePHI.

Bottom of Form