Ownership Unit: Administration	Reviewed By	Effective Date	Reviewed Date	For FY	Approved By
Policy Name: HIPAA Security Policies and Procedures	Rolf Lowe, Office of General counsel	2/26/2014	05/8/2017	2017	Chief Operating Officer

Please Indicate: New Policy: ☐ Revised Policy ☐ Annual Review ☒

Statement of Policy: HIPAA Security Policies and Procedures

Detroit Wayne Mental Health Authority (DWMHA)
HIPAA Security Policies and Procedures

CONTENTS

S1000 Security Management Process	3-4
S1100 Risk Analysis	5-7
S1200 Risk Management	8-10
S1300 Workforce Sanctions	11-12
S1400 Information System Activity Review	13-14
S2000 Assigned Security Responsibility	15-16
S3000 Workforce Security	17-18
S3100 Authorization and/or Supervision	19-21
S3200 Workforce Clearance Procedure	22-23
S3300 Termination Procedures	24-26
S4000 Information Access Management	27-28
S4100 Access Authorization	29-30
S4200 Access Establishment and Modification	31-33
S5000 Security Awareness and Training	34-35
S5100 Security Reminders	36-37
S5200 Protection from Malicious Software	38-39
S5300 Log-In Monitoring	40-41
S5400 Password Management	42-43
S6000 Security Incident Procedures	44-45
S6100 Response and Reporting	46-47
S7000 Contingency Plan	48-49
S7100 Data Backup Plan	50-51
S7200 Disaster Recovery Plan	52-53
S7300 Emergency Mode Operation Plan	54-55
S7400 Testing and Revision Procedure	56-57
S7500 Applications and Data Criticality Analysis	58-59
S8000 Facility Access Controls	60-61
S8100 Contingency Operations	62-63
S8200 Facility Security Plan	64-65
S8300 Access Control and Validation Procedures	66-67
S8400 Maintenance Records	68-69
S9000 Workstation Security	70-72
S10000 Device and Media Controls	73-74
S10100 Disposal	75-76
S10200 Media Re-use	77-78
S10300 Accountability	79-80
S10400 Data Backup and Storage	81-82
S11000 Access Control	83-84
S11100 Unique User Identification	85-86
S11200 Emergency Access Procedure	87-88
S11300 Automatic Logoff	89-90
S11400 Encryption and Decryption	91-92

S12000 Audit Controls 93-94
S13000 Integrity 95-96
S13100 Mechanism to Authenticate Electronic PHI 97-98
S14000 Person or Entity Authentication 99-100
S15000 Transmission Security 101-102
S15100 Integrity Controls 103-104
S15200 Encryption 105-106

Detroit Wayne Mental Health Authority

HIPAA Security Policies

Subject: Security Management Process	**Coverage:** DWMHA
Policy #: Security-1000	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement policies and procedures to prevent, detect, contain, and correct security violations."*
Regulatory Reference:	45 CFR 164.308(a)(1)(i)

I. PURPOSE

This policy reflects Detroit Wayne Mental Health Authority's commitment to ensure the confidentiality, integrity, and availability of its information systems containing electronic protected health information (EPHI) by implementing policies and procedures to prevent, detect, mitigate, and correct security violations.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. POLICY

DWMHA must ensure the confidentiality, integrity and availability of its information systems containing EPHI by implementing appropriate and reasonable policies, procedures and controls to a) prevent, b) detect, c) mitigate, and d) correct security violations.

DWMHA's security management programs must be based on formal and regular processes for risk analysis and management, sanction policies for non-compliance, information system activity review, and training and awareness of workforce members regarding security policies, procedures, and controls.

All DWMHA workforce members are responsible for appropriately protecting EPHI maintained on DWMHA information systems from unauthorized access, modification, destruction, and disclosure.

IV. APPLICABILITY

This policy is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices within the DWMHA that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following standards and safeguards must be implemented to satisfy the requirements of this policy:

1. DWMHA must regularly identify, define and prioritize risks with respect to the confidentiality, integrity, and availability of its information systems containing EPHI, as specified in the **Risk Analysis Standard (Security - 1100)**.

2. DWMHA must implement security measures that reduce the risks to its information systems containing EPHI to reasonable and appropriate levels, as specified in the **Risk Management Standard (Security – 1200)**,

3. DWMHA must apply appropriate sanctions against workforce members who fail to comply with its security policies and procedures, as specified in the **Sanction Standard (Security – 1300)**.

4. DWMHA must regularly review records of activity on information systems containing EPHI, as specified in the **Information System Activity Review Standard (Security – 1400)**.

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Risk Analysis	**Coverage:** DWMHA
Standard #: Security-1100	**Page:** 1 of 3

HIPAA Security Rule Language:	*"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (EPHI) held by the covered entity or business associate."*
Regulatory Reference:	45 CFR 164.308(a)(1)(ii)(A) *Required specification*

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to regularly conduct accurate and thorough analysis of the potential risks to the confidentiality, integrity, and availability of its information systems containing EPHI.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must regularly identify, define and prioritize risks to the confidentiality, integrity, and availability of its information systems containing EPHI. The identification, definition and prioritization of risks to information systems containing EPHI must be based on a formal, documented risk analysis process. DWMHA must conduct a risk analysis of its information systems, and require that business associates conduct a risk analysis, on a regular basis. Such risk analysis must be used in conjunction with DWMHA's risk management process. DWMHA must also conduct a risk analysis when environmental or operational changes occur which significantly impact the confidentiality, integrity or availability of specific information systems containing EPHI.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

1. DWMHA must regularly identify, define and prioritize risks to the confidentiality, integrity, and availability of its information systems containing EPHI, and require that business associates conduct a risk analysis of information systems containing its EPHI.

2. The identification, definition and prioritization of risks to information systems containing EPHI must be based on a formal, documented risk analysis process. At a minimum, DWMHA's risk analysis process must include the following:

    a. Identification and prioritization of the threats to information systems containing EPHI.
    b. Identification and prioritization of the vulnerabilities of information systems containing EPHI.
    c. Identification and definition of security measures used to protect the confidentiality, integrity, and availability of information systems containing EPHI.
    d. Identification of the likelihood that a given threat will exploit a specific vulnerability on a DWMHA information system containing EPHI.
    e. Identification of the potential impacts to the confidentiality, integrity, and availability of information systems containing EPHI if a given threat exploits a specific vulnerability.

3. DWMHA and business associates must conduct risk analysis on a regular basis. Such risk analysis must be used in conjunction with DWMHA's risk management process to identify, select and implement security measures to protect the confidentiality, integrity, and availability of information systems containing EPHI.

4. Judgments used in DWMHA's risk analysis, such as assumptions, defaults, and uncertainties, should be explicitly stated and documented.

5. In addition to regular risk analysis, DWMHA and business associates must conduct a risk analysis when environmental or operational changes occur which significantly impact the confidentiality, integrity or availability of specific information systems containing EPHI. Such changes include but are not limited to:

    a. Significant security incidents to specific information systems containing EPHI.
    b. Significant new threats or risks to specific information systems containing EPHI.

c. Significant changes to the organizational or technical infrastructure of DWMHA which affect specific information systems containing EPHI.
d. Significant changes to DWMHA information security requirements or responsibilities which affect specific information systems containing EPHI.

6. DWMHA's risk analysis process must be based on the following steps, which shall be formally documented and securely maintained:

a. **Inventory.** DWMHA must conduct a regular inventory of its information systems containing EPHI and the security measures protecting those systems.
b. **Threat identification.** DWMHA must identify all potential threats to its information systems containing EPHI. Such threats may be natural, human or environmental.
c. **Vulnerability identification.** DWMHA must identify all vulnerabilities on its information systems containing EPHI. This should be done by regularly reviewing vulnerability sources and performing security assessments.
d. **Security control analysis.** DWMHA must analyze the security measures that have been implemented or will be implemented to protect its information systems containing EPHI; this includes both preventive and detective controls.
e. **Risk likelihood determination.** DWMHA must assign a rating to each specific risk which indicates the probability that a vulnerability will be exploited by a particular threat. Three factors should be considered: 1) threat motivation and capability, 2) type of vulnerability, and 3) existence and effectiveness of current security controls
f. **Impact analysis.** DWMHA must determine the impact to confidentiality, integrity or availability of EPHI which would result if a threat were to successfully exploit a vulnerability on an DWMHA information system containing EPHI.
g. **Risk Determination.** DWMHA must use the information obtained in the above six steps to identify the level of risk to specific information systems containing EPHI. For each vulnerability and associated possible threat, DWMHA must make a risk determination based on:
   - The likelihood a certain threat will attempt to exploit a specific vulnerability.
   - The level of impact should the threat successfully exploit the vulnerability.
   - The adequacy of planned or existing security controls.

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Risk Management	**Coverage:** DWMHA
Standard #: Security-1200	**Page:** 1 of 3

HIPAA Security Rule Language:	*"Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Sec.164.306 (a)."*
Regulatory Reference:	45 CFR 164.308(a)(1)(ii)(B) *Required specification*

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to select and implement security measures to reduce the risks to its information systems containing EPHI to a reasonable and appropriate level.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

Detroit Wayne Mental Health Authority must implement security measures that reduce the risks to its information systems containing EPHI to reasonable and appropriate levels. Selection and implementation of such security measures must be based on a formal, documented risk management process.

DWMHA must conduct risk management on a continuous basis and all selected and implemented security measures must ensure the confidentiality, integrity and availability of information systems containing EPHI and be commensurate with the risks to such systems.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is

defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

1. Security measures must be implemented to reduce the risks to information systems containing EPHI to reasonable and appropriate levels. Selection and implementation of such security measures must be based on a formal, documented risk management process. At a minimum, the risk management process must include the following:

    a. Assessment and prioritization of risks to information systems containing EPHI.
    b. Selection and implementation of reasonable, appropriate and cost-effective security measures to manage, mitigate, or accept identified risks.
    c. Workforce member training and awareness on implemented security measures.
    d. Regular evaluation and revision, as necessary, of existing security measures.

2. DWMHA must manage risk on a continuous basis and all selected and implemented security measures must ensure the confidentiality, integrity and availability of information systems containing EPHI. Strategies for managing risk should be commensurate with the risk prioritization as described below to such systems, using one or more of the following methods to manage risk: risk acceptance, risk avoidance, risk limitation, or risk transference.

3. DWMHA's risk management process must be based on the following steps, which shall be formally documented and securely maintained:

    a. **Inventory.** DWMHA must conduct a regular inventory of its information systems containing EPHI and the security measures protecting those systems. DWMHA must be able to identify its information systems and the relative value and importance of those systems.
    b. **Risk prioritization.** Based on the risks defined by DWMHA's risk analysis, risks must be prioritized on a scale from high to low based on the potential impact to information systems containing EPHI and the probability of occurrence. When deciding what DWMHA resources should be allocated to identified risks, highest priority must be given to those risks with unacceptably high risk rankings.
    c. **Method selection.** DWMHA must select the most appropriate security methods to minimize or eliminate identified risks to information systems containing EPHI. Such selections must be based on the nature of a specific risk and the feasibility and effectiveness of a specific method.
    d. **Security method selection.** DWMHA must determine the most appropriate, reasonable and cost-effective security method(s) for reducing identified risks to information systems containing EPHI.
    e. **Assignment of responsibility.** DWMHA workforce members who have the appropriate expertise must be identified and assigned responsibility for implementing selected security method(s).

f. **Security method implementation**. Selected security method(s) must be correctly implemented.

g. **Security method evaluation.** Selected security method(s) must be regularly evaluated and revised as necessary.

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Workforce Sanctions	**Coverage:** DWMHA
Standard #: Security-1300	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate."*
Regulatory Reference:	45 CFR 164.308(a)(1)(ii)(C)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to apply appropriate sanctions against workforce members who fail to comply with its security policies and procedures.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

Detroit Wayne Mental Health Authority's workforce members and DWMHA business associates must comply with all applicable security policies and procedures. DWMHA and its business associates must have a formal, documented process for applying appropriate sanctions to workforce members who do not comply with its security policies and procedures. Sanctions must be commensurate with the severity of the non-compliance with DWMHA security policies and procedures.

IV. APPLICABILITY

This standard is applicable to all workforce members, departments, and health care components that use or disclose electronic protected health information for any purposes. This standard's scope includes all protected health information in electronic form.

V. PROCEDURE

1. DWMHA and its business associates must have a formal, documented process for applying appropriate sanctions against workforce members who do not comply with its security policies and procedures.

2. The identification and definition of such sanctions are defined in the applicable DWMHA's policies.

3. Sanctions can include but are not limited to:

a. Suspension
b. Required retraining
c. Letter of reprimand
d. Termination

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Information System Activity Review	**Coverage:** DWMHA
Standard #: Security-1400	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."*
Regulatory Reference:	45 CFR 164.308(a)(1)(ii)(D)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to regularly review records of activity on information systems containing EPHI.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must regularly review records of activity on information systems containing EPHI. Appropriate hardware, software, or procedural auditing mechanisms must be implemented on information systems that contain or use EPHI. Records of activity created by audit mechanisms implemented on information systems must be reviewed regularly.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

1. DWMHA must regularly review records of activity on information systems containing EPHI. Records of activity may include but are not limited to:

    a. Audit logs
    b. Access reports
    c. Security incident tracking reports

2. Appropriate hardware, software, or procedural auditing mechanisms must be implemented on DWMHA information systems that contain or use EPHI. At a minimum, such mechanisms must provide the following information if feasible:

    a. Date and time of activity
    b. Origin of activity
    c. Identification of user performing activity
    d. Description of attempted or completed activity

3. Such review must be via a formal documented process. At a minimum, the process must include:

    a. Definition of which workforce members will review records of activity
    b. Definition of what activity is significant
    c. Procedures defining how significant activity will be identified and reported
    d. Procedures for preserving records of significant activity

4. DWMHA must maintain the documentation of the review of such systems for a minimum of six years.

5. Whenever possible, DWMHA workforce members should not monitor or review activity related to their own user account.

Detroit Wayne Mental Health Authority

HIPAA Security Policies

Subject: Assigned Security Responsibility	**Coverage:** DWMHA
Policy #: Security-2000	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate."*
Regulatory Reference:	45 CFR 164.308(a)(2)

I. PURPOSE

This policy reflects Detroit Wayne Mental Health Authority's commitment to assign a single employee overall final responsibility for the confidentiality, integrity, and availability of its EPHI.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. POLICY

DWMHA's Information Security Officer is responsible for the development and implementation of all policies and procedures necessary to appropriately protect the confidentiality, integrity, and availability of DWMHA information systems and EPHI.

IV. APPLICABILITY

This policy is applicable for DWMHA Administration. This policy's scope includes all protected health information in electronic form.

V. PROCEDURE

The DWMHA Information Security Officer's responsibilities include, but are not limited to:

1. Ensure that DWMHA information systems comply with all applicable federal, state, and local laws and regulations.
2. Ensure that no DWMHA information system compromises the confidentiality, integrity, or availability of any other DWMHA information system.
3. Develop, document, and ensure dissemination of appropriate security policies, procedures, and standards for the users and administrators of DWMHA information systems and the data contained within them.
4. Ensure that newly acquired DWMHA information systems have features that support required and/or addressable security Implementation Specifications.
5. Coordinate the selection, implementation, and administration of significant DWMHA security controls.
6. Ensure DWMHA workforce members receive regular security awareness and training.
7. Conduct periodic risk analysis of DWMHA information systems and security processes.
8. Develop and implement an effective risk management program.
9. Regularly monitor and evaluate threats and risks to DWMHA information systems.
10. Develop and monitor/audit records of DWMHA information systems' activity to identify inappropriate activity.
11. Maintain an inventory of all DWMHA information systems that contain EPHI.
12. Create an effective security incident response policy and related procedures.
13. Ensure adequate physical security controls exist to protect DWMHA's EPHI.
14. Coordinate with DWMHA's Privacy Officer to ensure that security policies, procedures and controls support compliance with the HIPAA Privacy Rule.
15. Evaluate new security technologies that may be appropriate for protecting DWMHA's information systems.
16. Ensure that all of D-DCCMHA's business associates are compliant with the applicable HIPAA security rules.

Detroit Wayne Mental Health Authority

HIPAA Security Policies

Subject: Workforce Security	**Coverage:** DWMHA
Policy #: Security-3000	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a) (4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information."*
Regulatory Reference:	45 CFR 164.308(a)(3)(i)

I. PURPOSE

This policy reflects Detroit Wayne Mental Health Authority's commitment to allow access to information systems containing EPHI only to workforce members who have been appropriately authorized. The type and extent of access authorized to DWMHA information systems containing EPHI must be based on review by the system owners/stewards or their designated delegates.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. POLICY

Only properly authorized workforce members are provided access to information systems containing EPHI. The type and extent of access authorized to DWMHA information systems containing EPHI must be based on review by the system owners/stewards or their designated delegates.

Access to DWMHA information systems containing EPHI must be granted only to properly trained DWMHA workforce members who have a need for EPHI in order to accomplish a legitimate task.

IV. APPLICABILITY

This policy is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following standards and safeguards must be implemented to satisfy the requirements of this policy:

1. As defined in DWMHA's **Authorization and/or Supervision Standard (Security – 3100)**, DWMHA must ensure that all workforce members who have the ability to access DWMHA information systems containing EPHI are appropriately authorized or supervised.

2. As defined in DWMHA's **Workforce Clearance Standard (Security – 3200)**, DWMHA workforce members must be adequately screened during the hiring process, including background checks.

3. As defined in DWMHA's **Termination Procedures Standard (Security – 3300)**, DWMHA must create and implement a formal, documented process for terminating access to EPHI when the employment of a workforce member ends.

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Authorization and/or Supervision	**Coverage:** DWMHA
Standard #: Security-3100	**Page:** 1 of 3

HIPAA Security Rule Language:	*"Implement procedures for the authorization and/or supervision of workforce members who work with EPHI or in locations where it might be accessed."*
Regulatory Reference:	45 CFR 164.308(a)(3)(ii)(A)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to ensure that all workforce members who can access DWMHA information systems containing EPHI are appropriately authorized or supervised.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must ensure that all workforce members who can access DWMHA information systems containing EPHI are appropriately authorized and/or supervised.

DWMHA must have a formal documented process for granting authorization to access to DWMHA information systems containing EPHI. The type and extent of access granted to DWMHA information systems containing EPHI must be based on review by the system owners/stewards or their designated delegates. Access to DWMHA information systems containing EPHI must be authorized only for DWMHA workforce members having a need for specific information in order to accomplish their respective job responsibilities.

Before third-party persons are granted access to DWMHA information systems containing EPHI or DWMHA locations where EPHI can be accessed, a review by the system owners/stewards or their designated delegates must be conducted. Access by third-party persons to DWMHA information systems containing EPHI or DWMHA

locations where EPHI can be accessed, must be allowed only after appropriate security controls have been implemented and an agreement has been signed defining the terms for access. Whenever appropriate, third-party persons should be supervised by an appropriate DWMHA employee.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following standards and safeguards must be implemented to satisfy the requirements of this standard:

1. Appropriate DWMHA information system stewards/owners or their chosen delegates must define and authorize all access to DWMHA information systems containing EPHI. Such information system owners and delegates must be formally designated and documented as specified in the **Access Authorization Standard (Security - 4100)**.

2. The type and extent of access granted to DWMHA information systems containing EPHI must be based on specifications in the **Access Establishment and Modification Standard (Security - 4200).**

3. Before third party persons are granted access to DWMHA information systems containing EPHI or DWMHA locations where EPHI can be accessed; review by the system owners/stewards or their designated delegates must be performed. At a minimum, the review must consider the following factors:

- Type of access required
- Sensitivity of the EPHI on the information system
- Security controls on the information system
- Security controls used by the third party

4. Access by third party persons to DWMHA information systems containing EPHI or DWMHA locations where EPHI can be accessed must be allowed only after appropriate security controls have been implemented and an agreement has been signed defining the terms for access. The agreement must define the following:

- The security processes and controls necessary to ensure compliance with DWMHA's security policies.
- Restrictions regarding the use and disclosure of DWMHA data.
- DWMHA's right to monitor and revoke third party persons' access and activity.

5. Where appropriate, third party persons should be supervised by an appropriate DWMHA employee when they are accessing DWMHA information systems containing EPHI or in a DWMHA location where EPHI might be accessed.

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Workforce Clearance Procedure	**Coverage:** DWMHA
Standard #: Security-3200	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement procedures to determine that the access of a workforce member to EPHI is appropriate."*
Regulatory Reference:	45 CFR 164.308(a)(3)(ii)(B)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to ensure that all workforce members have appropriate authorization to access DWMHA information systems containing EPHI.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

The background of all DWMHA workforce members must be adequately reviewed during the hiring process.

DWMHA must identify the level of access required by all DWMHA workforce members who access DWMHA information systems containing EPHI.

When defining an organizational position, the DWMHA must identify and define both the security responsibilities of and level of supervision required for the position.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following standards and safeguards must be implemented to satisfy the requirements of this standard:

1. DWMHA must identify the appropriate level of access required by all DWMHA workforce members who access DWMHA information systems containing EPHI. Such access must be formally documented and securely maintained.

2. The background of all DWMHA workforce members must be adequately reviewed during the hiring process. Verification checks include, but are not limited to character references and criminal background checks.

3. When defining a position, the DWMHA and the hiring manager must identify the security responsibilities and supervision required for the position. Security responsibilities include general responsibilities for implementing or maintaining security, as well as any specific responsibilities for the protection of the confidentiality, integrity, or availability of DWMHA information systems or processes.

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Termination Procedures	**Coverage:** DWMHA
Standard #: Security-3300	**Page:** 1 of 3

HIPAA Security Rule Language:	*"Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section."*
Regulatory Reference:	45 CFR 164.308(a)(3)(ii)(C)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to create and implement a formal, documented process for terminating access to EPHI when the employment of a workforce member ends.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

When the employment of, or other arrangement with, DWMHA workforce members ends, their information systems privileges, both internal and remote, must be disabled or removed by the time of departure. When workforce members depart from DWMHA, they must return all DWMHA supplied equipment by the time of departure. A workforce member who departs from DWMHA must not retain, give away, or remove from DWMHA premises any DWMHA information. Special attention must be paid to situations where a workforce member has been terminated and poses a risk to information or systems at DWMHA.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is

defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following standards and safeguards must be implemented to satisfy the requirements of this standard:

1. DWMHA must create and implement a formal, documented process for terminating access to EPHI when the employment of a workforce member ends.

2. When the employment of DWMHA workforce members ends, their information systems privileges, both internal and remote, must be disabled or removed by the time of departure. Consideration should also be given to physical access to areas where EPHI is located.

3. All DWMHA workforce members must have their information system privileges automatically disabled after their user ID or access method has had 60 days of inactivity. All such privileges that are disabled in this manner must be reviewed to ensure that the inactivity is not due to termination of employment. If termination is the reason for inactivity, there must be review of situation to ensure that all access to EPHI (or ability to physically access information) has been eliminated.

4. When workforce members depart from DWMHA, they must return all DWMHA supplied equipment (PCs, PDAs, Mobile phones, Keys, etc.) by the time of departure. The return of all such equipment must be tracked and logged.

5. If a departing workforce member has used cryptography on DWMHA data, they must make the cryptographic keys available to appropriate management by the time of departure.

6. As appropriate, all physical security access codes used to protect DWMHA information systems that are known by a departing workforce member must be deactivated or changed. For example, the PIN to a keypad lock that restricts entry to a DWMHA facility containing information systems with EPHI must be changed if a workforce member who knows the PIN departs.

7. A workforce member who departs from DWMHA must not retain, give away, or remove from DWMHA premises any DWMHA information (this does not apply to copies of information provided to the public or copies of correspondence directly related to the terms and conditions of employment). All other DWMHA information in the possession of the departing workforce member must be provided to the person's immediate supervisor at the time of departure.

8. Prior to the departure of a terminating DWMHA workforce member, their computers' resident files must be promptly reviewed by their immediate supervisors to determine the appropriate transfer or disposal of any confidential information.

9. Special attention must be paid to situations where a departing employee poses a risk to information or systems at DWMHA. If a workforce member is to be terminated immediately, their information system privileges must be removed or disabled just before they are notified of the termination.

10. DWMHA or their designees must periodically review information system access privileges to ensure that this policy is being adhered to and that existing procedures are effective.

Detroit Wayne Mental Health Authority

HIPAA Security Policies

Subject: Information Access Management	**Coverage:** DWMHA
Policy #: Security-4000	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part."*
Regulatory Reference:	45 CFR 164.308(a)(4)(i)

I. PURPOSE

This policy reflects Detroit Wayne Mental Health Authority's commitment to have a formal documented process for authorizing appropriate access to DWMHA information systems containing EPHI.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. POLICY

DWMHA must have a formal documented process for authorizing appropriate access to DWMHA information systems containing EPHI.

DWMHA workforce members must not be allowed access to information systems containing EPHI until properly authorized.

Appropriate DWMHA information system owners/stewards or their chosen delegates must define and authorize all access to DWMHA information systems containing EPHI. Such information system owners/stewards and delegates must be formally designated and documented.

Access to DWMHA information systems containing EPHI must be authorized only for DWMHA workforce members who have a need for specific information in order to accomplish the work responsibilities of their specific jobs. Such access must also be regularly reviewed and revised as necessary.

IV. APPLICABILITY

This policy is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following standards and safeguards must be implemented to satisfy the requirements of this policy:

1. DWMHA must have a formal documented process for authorizing appropriate access to its information systems containing EPHI, as specified in the **Access Authorization Standard (Security – 4100)**.

2. DWMHA must have a formal, documented process for establishing, documenting, reviewing, and modifying access to its information systems containing EPHI, as specified in the **Access Establishment and Modification Standard (Security - 4200)**.

Detroit- Wayne County Community Mental Health Authority

HIPAA Security Standards

Subject: Access Authorization	**Coverage:** DWMHA
Standard #: Security-4100	**Page:** 1 of 2

HIPAA Security Rule Language:	"*Implement policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, process, or other mechanism.*"
Regulatory Reference:	45 CFR 164.308(a)(4)(ii)(B)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to have a formal documented process for authorizing appropriate access to DWMHA information systems containing EPHI.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must have a formal documented process for granting and authorizing appropriate access to DWMHA information systems containing EPHI. This process must be conducted by appropriate information system stewards/owners.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following safeguards must be implemented to satisfy the requirements of this standard:

1. DWMHA must have a formal documented process for granting access to DWMHA information systems that contain EPHI. At a minimum, the process must include:

- Procedure for granting access to DWMHA information systems containing EPHI.
- Procedure for tracking and logging authorization of access to DWMHA information systems containing EPHI.
- Procedure for regularly reviewing and revising, as necessary, authorization of access to DWMHA information systems containing EPHI.

2. DWMHA information system stewards/owners or their chosen delegates must define and authorize all access to DWMHA information systems containing EPHI that is entrusted to them. Such information system stewards/owners and delegates must be formally designated and documented.

3. Access to DWMHA information systems containing EPHI must be authorized only for DWMHA workforce members having a need for specific information in order to accomplish a legitimate task. Access must not be allowed until properly authorized. All such access must be defined and documented as specified in the **Access Establishment and Modification Standard (Security – 4200)**. Such access must also be regularly reviewed and revised as necessary.

4. DWMHA workforce members must not willfully attempt to gain access to DWMHA information systems containing EPHI for which they have not been given proper authorization.

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Access Establishment and Modification	**Coverage:** DWMHA
Standard #: Security-4200	**Page:** 1 of 3

HIPAA Security Rule Language:	*"Implement policies and procedures that, based upon the covered entity's or business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process."*
Regulatory Reference:	45 CFR 164.308(a)(4)(ii)(C)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to have a formal documented process for establishing, documenting, reviewing, and modifying access to DWMHA information systems containing EPHI.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must have a formal, documented process for establishing, documenting, reviewing, and modifying access to DWMHA information systems containing EPHI.

Authorized DWMHA information system owners/stewards or their designated delegates must regularly review workforce member access rights to DWMHA information systems containing EPHI to ensure that they are provided only to those having a need for specific information in order to accomplish a legitimate task. All revisions to DWMHA workforce member access rights must be tracked and logged.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is

defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following safeguards must be implemented to satisfy the requirements of this standard:

1. DWMHA and their business associates must have a formal, documented process for establishing, documenting, reviewing, and modifying access to DWMHA information systems containing EPHI. At a minimum, the process must include:

- Procedure for establishing different levels of access to DWMHA information systems containing EPHI.
- Procedure for documenting levels of access established to DWMHA information systems containing EPHI.
- Procedure for regularly reviewing DWMHA workforce member access privileges to DWMHA information systems containing EPHI.
- Procedure for modifying DWMHA workforce member access privileges to DWMHA information systems containing EPHI.

2. Only properly authorized and trained DWMHA workforce members may access DWMHA information systems containing EPHI. Such access must be established via a formal, documented process. At a minimum, this process must include:

- Identification and definition of permitted access methods
- Identification and definition of length of time that access will be granted
- Procedure for both granting a workforce member an access method (e.g. password or token) and changing an existing access method
- Procedure for managing access rights in a distributed and networked environment
- Appropriate tracking and logging of activities by authorized workforce members on DWMHA information systems containing EPHI

3. Where appropriate, security controls or methods that allow access to be established to DWMHA information systems containing EPHI must include, at a minimum:

- Unique user identifiers (user IDs) that enable individual users to be uniquely identified. User IDs must not give any indication of the user's privilege level. Common or shared identifiers must not be used to gain access to DWMHA information systems containing EPHI. When unique user identifiers are insufficient or inappropriate, shared identifiers may be used to gain access to DWMHA information systems not containing EPHI. However, this should be a last resort when there are no other feasible alternatives. Further, anytime shared identifiers are used, the system and/or applicable administrators and data owners must have a mechanism of tracking the individuals that are aware of the shared identifiers/credentials. The shared identifiers/credentials must be changed promptly anytime an individual with knowledge of the credentials and passphrase

transfers or is terminated from employment by DWMHA, or no longer needs access to the EPHI for any reason.
- The prompt removal or disabling of access methods for persons and entities that no longer need access to DWMHA EPHI.
- Verification that redundant user identifiers are not issued.

4. Access to DWMHA information systems containing EPHI must be limited to DWMHA workforce members who have a need for specific EPHI in order to perform their job responsibilities.

5. Appropriate DWMHA information system owners/stewards or their designated delegates must regularly review workforce member access rights to DWMHA information systems containing EPHI to ensure that they are provided only to those who have a need for specific EPHI in order to accomplish a legitimate task. Such rights must be revised as necessary.

6. All revisions to DWMHA workforce member access rights must be tracked and logged. At a minimum, such tracking and logging must provide the following information:

- Date and time of revision
- Identification of workforce member whose access is being revised
- Brief description of revised access right(s)
- Reason for revision

This information must be securely maintained.

Detroit Wayne Mental Health Authority

HIPAA Security Policies

Subject: Security Awareness and Training	**Coverage:** DWMHA
Policy #: Security-5000	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement a security awareness and training program for all members of a covered entity's workforce (including management)."* 1. Security reminders (ii)(A) 2. Protection from malicious software (ii)(B) 3. Log-in monitoring (ii)(C) 4. Password management (ii)(D)
Regulatory Reference:	45 CFR 164.308(a)(5)(i)-(ii)

I. PURPOSE

This policy reflects Detroit Wayne Mental Health Authority's commitment to provide regular security awareness and training to its workforce members.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. POLICY

DWMHA must develop, implement, and regularly review a formal, documented program for providing appropriate security training and awareness to its workforce members. All DWMHA's workforce members must be provided with sufficient training and supporting reference materials to enable them to appropriately protect EPHI on DWMHA information systems.

All new DWMHA workforce members must receive appropriate security training before being provided with access or accounts on DWMHA information systems within thirty (30) days of hire. Existing workforce members must receive security training updates at a minimum of once a year.

Business associates must be made regularly aware of DWMHA security policies, standards, and procedures. Third party persons who access DWMHA healthcare computing systems or EPHI must be made aware of DWMHA security policies, standards, and procedures.

IV. APPLICABILITY

This policy is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following standards and safeguards must be implemented to satisfy the requirements of this policy:

1. As defined in DWMHA's **Security Reminders Standard (Security – 5100)**, DWMHA must provide regular security information and awareness to its workforce members.

2. As defined in DWMHA's **Protection from Malicious Software Standard (Security 5200)**, DWMHA must regularly train its workforce members about its process for guarding against, detecting, and reporting malicious software that poses a risk to its information systems and data.

3. As defined in DWMHA's **Log-in Monitoring Standard (Security - 5300)**, DWMHA must regularly train its workforce members about its process for monitoring log-in attempts and reporting discrepancies.

4. As defined in DWMHA's **Password Management Standard (Security – 5400)**, DWMHA must regularly train its workforce members about its process for creating, changing and safeguarding passwords.

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Security Reminders	**Coverage:** DWMHA
Standard #: Security-5100	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Periodic security updates"*
Regulatory Reference:	45 CFR 164.308(a)(5)(ii)(A)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to provide regular security information and awareness to its workforce members.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must distribute security reminders on a regular basis to its workforce members.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following standards and safeguards must be implemented to satisfy the requirements of this standard:

1. DWMHA must periodically distribute security reminders to all of its workforce members.

2. Security reminders will address security topics that include, but are not limited to:

- Information security policies
- Information security controls and processes
- Risks to healthcare information systems and EPHI
- Security best practices (e.g. how to choose a good password, how to report a security incident)
- DWMHA's information security legal and business responsibilities (e.g. HIPAA, business associate contracts)

3. In addition to providing regular security reminders, DWMHA must provide security information and awareness to all of its workforce members when any of the following events occur:

- Revisions to DWMHA's information security policies or procedures
- New information security controls are implemented at DWMHA
- Changes to information security controls
- Changes in legal or business responsibilities
- New threats or risks to EPHI

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Protection From Malicious Software	**Coverage:** DWMHA
Standard #: Security-5200	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement…..Procedures for guarding against, detecting, and reporting malicious software…..."*
Regulatory Reference:	45 CFR 164.308(a)(5)(ii)(B)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to provide regular training and awareness to its employees about its process for guarding against, detecting, and reporting malicious software that poses a risk to its information systems.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must train workforce members on guarding against, detecting, and reporting malicious software that poses a risk to its information systems.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following safeguards must be implemented to satisfy the requirements of this standard:

1. DWMHA must train workforce members on following procedures for guarding against, detecting, and reporting on malicious software.

2. Training and awareness must cover the following topics at minimum:

- How to identify and handle potential scams and hoaxes
- Explanation of how DWMHA anti-virus and malware protection software operate
- How to configure and use anti-virus and mal-ware protection software
- Good security practices for web browsing, sharing files, and opening email attachments
- Risks of installing unsupported software
- Security updates for workstations and software applications
- What to do when anti-virus and mal-ware protection software detects a virus or worm

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Log-In Monitoring	**Coverage:** DWMHA
Standard #: Security-5300	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement….Procedures for monitoring log-in attempts and reporting discrepancies….."*
Regulatory Reference:	45 CFR 164.308(a)(5)(ii)(C)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to regularly train and remind its workforce members about its process for monitoring log-in attempts and reporting discrepancies.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must train workforce members on monitoring log-in attempts and reporting discrepancies.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following safeguards must be implemented to satisfy the requirements of this standard:

1. DWMHA must train workforce members on following procedures for monitoring log-in attempts and reporting discrepancies.

2. Training and awareness must cover the following topics at minimum:

- How to effectively use DWMHA's secure log-in processes
- How to detect log-in discrepancies
- How to report log-in discrepancies

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Password Management	**Coverage:** DWMHA
Standard #: Security-5400	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement....Procedures for creating, changing, and safeguarding passwords…"*
Regulatory Reference:	45 CFR 164.308(a)(5)(ii)(D)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to provide regular training and awareness to its workforce members about creating, changing, and safeguarding passwords.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must train workforce members on appropriately creating, changing, and safeguarding passwords.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following safeguards must be implemented to satisfy the requirements of this standard:

1. DWMHA must train workforce members on following procedures for creating, changing and safeguarding passwords.

2. Training and awareness must cover the following topics at minimum:

- DWMHA's Minimum Passphrase (password) requirements
- Good password practices
- Ensuring that DWMHA workforce members understand that all activities involving their user identification and password will be attributed to them

Detroit Wayne Mental Health Authority

HIPAA Security Policies

Subject: Security Incident Procedures	**Coverage:** DWMHA
Policy #: Security-6000	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement policies and procedures to address security incidents."*
Regulatory Reference:	45 CFR 164.308(a)(6)(i)

I. PURPOSE

This policy reflects Detroit Wayne Mental Health Authority's commitment to implement policies and procedures for detecting and responding to security incidents.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. POLICY

DWMHA must have a formal, documented process for quickly and effectively detecting and responding to security incidents that may impact the confidentiality, integrity, or availability of DWMHA's information systems.

All DWMHA's actions to respond to and recover from security incidents must be carefully and formally controlled. At a minimum, formal procedures must ensure that all actions taken are intended to minimize the damage of a security incident and prevent further damage, all actions taken are carefully documented, and all actions taken are reported to appropriate management and reviewed in a timely manner.

All DWMHA workforce members must report any observed or suspected security incidents as quickly as possible via the DWMHA's security incident reporting procedure.

IV. APPLICABILITY

This policy is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following safeguards must be implemented to satisfy the requirements of this policy:

1. DWMHA must have a formal, documented process for quickly and effectively detecting and responding to security incidents, as specified in the **Response and Reporting Standard (Security – 6100)**.

VI. DEFINITION

A security incident is defined as any event that creates a risk to the confidentiality, integrity, or availability of EPHI.

Detroit Wayne Mental Health Authority

HIPAA Security Standard

Subject: Response and Reporting	**Coverage:** DWMHA
Standard #: Security-6100	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes."*
Regulatory Reference:	45 CFR 164.308(a)(6)(ii)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to effectively detect and respond to security incidents in order to protect the confidentiality, integrity, and availability of its information systems.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA and/or their business associates must be able to effectively detect, respond to, and mitigate the effects of security incidents in order to protect the confidentiality, integrity, and availability of its EPHI stored on healthcare computing systems.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following standards and safeguards must be implemented to satisfy the requirements of this policy:

1. DWMHA and their business associates must have a process for detecting security incidents. This may include, but is not limited to: regular review of data access logs, system alert messages, and other application anomalies.

2. DWMHA and business associates must report suspected security incidents to the DWMHA IT Help Desk.

3. DWMHA and business associates must document the security incident, which includes at a minimum the following:
   - Name of person(s) conducting the incident response investigation
   - Description of the data and the computing system affected by the incident
   - Time and date of incident
   - Damage to data and the computing system(s)
   - Suspected cause of the incident
   - Actions taken to mitigate damage and restore the data and/or computing system
   - Recommendations for further actions to enhance security of EPHI

4. DWMHA and business associates must submit incident documentation to the IT Security Officer.

Detroit Wayne Mental Health Authority

HIPAA Security Policies

Subject: Contingency Plan	**Coverage:** DWMHA
Policy #: Security-7000	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information (EPHI)."*
Regulatory Reference:	45 CFR 164.308(a)(7)(i)

I. PURPOSE

This policy reflects Detroit Wayne Mental Health Authority's commitment to effectively prepare for and respond to emergencies or disasters in order to protect the confidentiality, integrity and availability of its information systems.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. POLICY

DWMHA must have a formal process for both preparing for and effectively responding to emergencies and disasters that damage the confidentiality, integrity, or availability of its information systems.

DWMHA's disaster and emergency response process must reduce the disruption to DWMHA information systems to an acceptable level through a combination of preventative and recovery controls and processes. Such controls and processes must identify and reduce risks to DWMHA information systems, limit damage caused by disasters and emergencies, and ensure the timely resumption of significant information systems and processes. Such controls and processes must be commensurate with the value of the information systems being protected or recovered.

DWMHA workforce members must receive regular training and awareness on the DWMHA's disaster preparation and disaster and emergency response processes.

IV. APPLICABILITY

This policy is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following standards and safeguards must be implemented to satisfy the requirements of this policy:

1. DWMHA must have a formal process for assuring all EPHI on the DWMHA's information systems and electronic media must be regularly backed up and securely stored as specified in the **Data Backup Standard (Security – 7100).**

2. DWMHA must create and document a Disaster Recovery Plan to recover its information systems if they are impacted by a disaster as specified in the **Disaster Recovery Plan Standard (Security - 7200).**

3. DWMHA must have a formal, documented Emergency Mode Operations plan to enable the continuance of crucial business processes that protect the security of its information systems containing EPHI during and immediately after a crisis situation as specified in the **Emergency Mode Operations Plan Standard (Security – 7300).**

4. DWMHA must conduct regular testing of its Disaster Recovery Plan to ensure that it is up to date and effective as specified in the **Testing and Revision Procedures Standard (Security - 7400).**

5. DWMHA must have a formal process for defining and identifying the criticality of its information systems as specified in the **Application and Data Criticality Analysis Standard (Security - 7500).**

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Data Backup Plan	**Coverage:** DWMHA
Standard #: Security-7100	**Page:** 1of 2

HIPAA Security Rule Language:	*"Establish and implement procedures to create and maintain retrievable exact copies of EPHI."*
Regulatory Reference:	45 CFR 164.308(a)(7)(ii)(A)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to backup and securely store all EPHI on its information systems and electronic media.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

All EPHI on DWMHA information systems and electronic media must be regularly backed up and securely stored. Backup and restoration procedures must be regularly tested.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

1. DWMHA must have formal, documented procedures for creating and maintaining retrievable exact copies of EPHI. At a minimum these procedures must identify the healthcare computing systems to be backed up, provide a backup schedule, identify where backup media are stored and who may access them, outline restoration process, and identify who is responsible for ensuring the backup of the EPHI.

2. The criticality of the data will determine the frequency of data backups, retention of data backups, as well as where data backups and restoration procedures will be stored.

3. Backup copies of EPHI will be stored at a secure location and must be accessible to authorized DWMHA workforce members for prompt retrieval of the information. The secure location must be as geographically distant from the location of the healthcare computing system as is feasible.

4. Restoration procedures for EPHI must be regularly tested as specified in the **Testing and Revision Procedures Standard (Security – 7400)** to ensure that they are effective and that they can be completed within the time allotted in the DWMHA disaster recovery plan.

Detroit Wayne Mental Health Authority

HIPAA Security Standard

Subject: Disaster Recovery Plan	**Coverage:** DWMHA
Standard #: Security-7200	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Establish (and implement as needed) procedures to restore any loss of data."*
Regulatory Reference:	45 CFR 164.308(a)(7)(ii)(B)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to implement a Disaster Recovery Plan to recover its healthcare computing systems if they are impacted by a disaster.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must create, document, and maintain a Disaster Recovery Plan to recover its information systems if they are impacted by a disaster. DWMHA workforce members with disaster recovery responsibilities must receive annual training on the Disaster Recovery Plan. All appropriate DWMHA workforce members must have access to a current copy of the plan.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

1. DWMHA must create and document a Disaster Recovery Plan to recover its information systems if they are impacted by a disaster. The plan must be reviewed and revised on an annual basis or more frequently as needed.

2. The Disaster Recovery Plan must include at a minimum:

- Identification and definition of workforce member responsibilities
- Conditions for activating the plan
- Location of data backups
- Restoration procedures

3. Workforce members with disaster recovery responsibilities must receive annual training on the disaster recovery plan.

4. All appropriate DWMHA workforce members must have access to a current copy of the Disaster Recovery Plan.

Detroit Wayne Mental Health Authority

HIPAA Security Standard

Subject: Emergency Mode Operation Plan	**Coverage:** DWMHA
Standard #: Security-7300	**Page:** 1of 2

HIPAA Security Rule Language:	*"Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode."*
Regulatory Reference:	45 CFR 164.308(a)(7)(ii)(C)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to have an Emergency Mode Operations Plan for protecting its information systems containing EPHI during and immediately after a crisis situation.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must have a formal, documented Emergency Mode Operation Plan to enable the continuation of crucial business processes that protect the security of its information systems containing EPHI during and immediately after a crisis situation. DWMHA workforce members must receive annual training and awareness on the Emergency Mode Operations Plan. All appropriate DWMHA workforce members must have access to a current copy of the plan and an appropriate number of current copies of the plan must be kept off-site.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

1. DWMHA must have a formal, documented Emergency Mode Operations Plan for protecting its information systems containing EPHI during and immediately after a crisis situation. At a minimum, the plan must:

- Identify and prioritize emergencies that may impact DWMHA information systems containing EPHI.
- Define procedures for how DWMHA will respond to specific emergencies that impact information systems containing EPHI.
- Define procedures for how DWMHA, during and immediately after a crisis situation, will maintain the processes and controls that ensure the availability, integrity and confidentiality of EPHI on DWMHA information systems.
- Define a procedure that ensures that authorized employees can enter DWMHA facilities to enable continuation of processes and controls that protect EPHI while DWMHA is operating in emergency mode.

2. DWMHA workforce members must receive annual training and awareness on the emergency mode operations plan.

3. All appropriate DWMHA workforce members must have access to current copy of the plan and an appropriate number of current copies of the plan must be kept off-site.

Detroit Wayne Mental Health Authority

HIPAA Security Standard

Subject: Testing and Revision Procedure	**Coverage:** DWMHA
Standard #: Security-7400	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement procedures for periodic testing and revision of contingency plans."*
Regulatory Reference:	45 CFR 164.308(a)(7)(ii)(D)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to regularly test its information technology Disaster Recovery and Emergency Mode Operation Plans.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must conduct regular testing of its IT Disaster Recovery and Emergency Mode Operation Plans to ensure that they are up to date and effective. The testing should be conducted on an annual basis or as frequently as is feasible. The results of testing must be formally documented.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

1. DWMHA must conduct regular testing of its Disaster Recovery and Emergency Mode Operation Plans to ensure they are current, operative. Criticality of the data and resource availability will determine the frequency of testing. However, the testing should be conducted on an annual basis or as frequently as is feasible.

2. The results of such tests must be formally documented. The Disaster Recovery and Emergency Mode Operation Plans must be revised as necessary to address issues or gaps identified in the testing process.

Detroit Wayne Mental Health Authority

HIPAA Security Standard

Subject: Applications and Data Criticality Analysis	**Coverage:** DWMHA
Standard #: Security-7500	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Assess the relative criticality of specific applications and data in support of other contingency plan components."*
Regulatory Reference:	45 CFR 164.308(a)(7)(ii)(E)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to conduct an annual analysis of the criticality of its healthcare computing systems.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must have a formal process for defining and identifying the criticality of its healthcare computing systems and the data contained within them. The prioritization of DWMHA information systems must be based on an analysis of the impact to DWMHA services, processes, and business objectives if disasters or emergencies cause specific information systems to be unavailable for particular periods of time. The criticality analysis must be conducted with significant involvement from the administrators, users, and owners of DWMHA information systems and business processes. The criticality analysis must be conducted at least annually.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

1. DWMHA must have a formal, documented process for defining and identifying the criticality of its information systems and the data contained within them. At a minimum, the process must include:

- Creating an inventory of interdependent systems and their dependencies.
- Documenting the criticality of DWMHA's information systems (e.g. impact on patient care).
- Identifying and documenting the impact to DWMHA services, if specific DWMHA information systems are unavailable for different periods of time (e.g. 1 hour, 1 day).
- Identifying the maximum time periods that healthcare computing systems can be unavailable.
- Prioritizing healthcare computing system components according to their criticality to the DWMHA's ability to function at normal levels.

2. The criticality analysis must be conducted at least annually. The criticality analysis report must be securely maintained.

Detroit Community Mental Health Authority

HIPAA Security Policies

Subject: Facility Access Controls	**Coverage:** DWMHA
Policy #: Security-8000	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement policies and procedures to limit physical access to a covered entity's electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."*
Regulatory Reference:	45 CFR 164.310(a)(1)

I. PURPOSE

This policy reflects Detroit Wayne Mental Health Authority's commitment to prevent unauthorized physical access to its facilities while ensuring that properly authorized access is allowed.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. POLICY

DWMHA must appropriately limit physical access to the health care computing systems contained within its facilities while ensuring that properly authorized workforce members can physically access such systems. DWMHA health care computing systems containing EPHI must be physically located in such a manner as to minimize the risk that unauthorized persons can gain access to them. The level of protection must be commensurate with that of identified risks.

IV. APPLICABILITY

This policy is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following standards and safeguards must be implemented to satisfy the requirements of this policy:

1. As defined in DWMHA's **Contingency Operations Standard (Security – 8100)**, DWMHA must have formal, documented procedures for allowing authorized workforce members to enter its facilities to take necessary actions as defined in its disaster recovery and emergency mode operations plans.

2. As defined in DWMHA's **Facility Security Plan Standard (Security - 8200)**, DWMHA must have a facility security plan that details how it will protect its facilities and equipment.

3. As defined in DWMHA's **Access Control and Validation Procedures Standard (Security – 8300)**, DWMHA must implement procedures to control and validate individuals' access to DWMHA's facilities based on their roles or functions.

4. As defined in DWMHA's **Maintenance Records Standard (Security – 8400)**, DWMHA must document all repairs and modifications to the physical components of its facilities that are related to security.

Detroit Community Mental Health Authority

HIPAA Security Standards

Subject: Contingency Operations	**Coverage:** DWMHA
Standard #: Security-8100	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency."*
Regulatory Reference:	45 CFR 164.310(a)(2)(i)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to ensure that, in the event of a disaster or emergency, appropriate individuals can enter its facilities to take necessary actions defined in its Disaster Recovery and Business Continuity Plans.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must have formal, documented procedures for allowing designated individuals to enter its facilities to take necessary actions as defined in its Disaster Recovery and Business Continuity Plans.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following safeguards must be implemented to satisfy the requirements of this standard:

1. DWMHA must ensure that, in the event of a disaster or emergency, appropriate persons can enter its facility to take necessary actions defined in its Disaster Recovery and Business Continuity Plans.

2. Based on its Disaster Recovery and Business Continuity Plans, DWMHA must develop, implement, and regularly review a formal, documented procedure that ensures that authorized employees can enter the facility to enable continuation of processes, and controls that protect EPHI while the DWMHA is operating in emergency mode.

3. In the event of an emergency, only authorized DWMHA employees may administer or modify processes and controls which protect EPHI contained on information systems. Such employees or roles must be defined in DWMHA's Disaster Recovery and/or Business Continuity Plans.

Detroit Community Mental Health Authority

HIPAA Security Standards

Subject: Facility Security Plan	**Coverage:** DWMHA
Standard #: Security-8200	**Page:** 1 of 2

HIPAA Security Rule Language:	"*Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.*"
Regulatory Reference:	45 CFR 164.310(a)(2)(ii)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to maintain a facility security plan for protecting its facilities and all healthcare computing systems contained within them.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must have a facility security plan that details how it will protect its facilities and the equipment therein, from unauthorized access, tampering, or theft of its healthcare computing systems.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following safeguards must be implemented to satisfy the requirements of this standard:

1. DWMHA must maintain and regularly review a formal, documented facility security plan that describes how its facilities and equipment within them will be appropriately protected. The plan must be revised as necessary.

2. At a minimum, DWMHA's facility security plan must address the following:

- Identification of DWMHA healthcare computing systems to be protected from unauthorized physical access, tampering, and theft.
- Identification of processes and controls used to protect DWMHA healthcare computing systems from unauthorized physical access, tampering, and theft.
- Actions to be taken if unauthorized physical access, tampering, or theft attempts are made against DWMHA healthcare computing systems.
- A maintenance schedule that specifies how and when the plan will be tested, as well as the process for maintaining the plan.

Detroit Community Mental Health Authority

HIPAA Security Standards

Subject: Access Control and Validation Procedures	**Coverage:** DWMHA
Standard #: Security-8300	**Page:** 1of 2

HIPAA Security Rule Language:	*"Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision."*
Regulatory Reference:	45 CFR 164.310(a)(2)(iii)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to control and validate physical access to its facilities containing healthcare computing systems or software programs that can access healthcare computing systems.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must control and validate physical access to its facilities that have healthcare computing systems or software programs that can access healthcare computing systems. All physical access rights to such facilities must be clearly defined and documented, with access provided only to DWMHA workforce members who have a need for specific access of the healthcare computing system in order to accomplish a legitimate task. Additionally, such access rights must define specific roles or functions and the physical access rights associated with each.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is

defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following safeguards must be implemented to satisfy the requirements of this standard:

1. DWMHA will identify and document all organizational or functional areas considered sensitive due to the nature of the EPHI that is stored or available within them.

2. After documenting sensitive areas, access rights to such areas should be given only to workforce members who have a need for specific physical access in order to accomplish a legitimate task.

3. All visitors to sensitive facilities where healthcare computing systems are located must show proper identification, state reason for need to access, and sign in prior to gaining access.

4. DWMHA workforce members must immediately report to appropriate management the loss or theft of any device (e.g. card or token) that enables them to gain physical access to such sensitive facilities.

5. DWMHA workforce members must wear an identification badge when at DWMHA facilities where healthcare computing systems are located and should be encouraged to report unknown persons not wearing such identification.

6. All access rights to DWMHA facilities where healthcare computing systems are located or software programs that can access healthcare computing systems must be regularly reviewed and revised as necessary.

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Maintenance Records	**Coverage:** DWMHA
Standard #: Security-8400	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks)."*
Regulatory Reference:	45 CFR 164.310(a)(2)(iv)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to document all repairs and modifications to the physical components of its facilities that are related to the protection of EPHI.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must document all repairs and modifications to the physical components of its facilities that contain healthcare computing systems.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following safeguards must be implemented to satisfy the requirements of this standard:

1. DWMHA must document all repairs and modifications to the physical components of its facilities where healthcare computing systems are located. Physical components include, but are not limited to: electronic card access systems, locks, doors, and walls.

2. DWMHA must conduct an inventory of all the physical components of its facilities that are related to the protection of healthcare computing systems on an annual basis at a minimum. Inventory results must be documented and stored in a secure manner.

3. Repairs or modifications to any DWMHA physical component listed in the above inventory must be documented. At a minimum, the documentation must include:

- Date and time of repair or modification
- Reason for repair or modification
- Person(s) performing the repair or modification
- Outcome of repair or modification

Detroit Wayne Mental Health Authority

HIPAA Security Policies

Subject: Workstation Security	**Coverage:** DWMHA
Policy #: Security-9000	**Page:** 1 of 3

HIPAA Security Rule Language:	*"Implement physical safeguards for all workstations that access EPHI, to restrict access to authorized users."* *"Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access EPHI."*
Regulatory Reference:	45 CFR 164.310(b)-(c)

I. PURPOSE

This policy reflects Detroit Wayne Mental Health Authority's commitment to the protection of workstations that store or access EPHI while ensuring that authorized workforce members have appropriate access.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. POLICY

DWMHA will prevent unauthorized access to workstations that store or access EPHI while maintaining the access of authorized employees. Workforce members must not use DWMHA workstations to engage in any activity that is either illegal under local, state, federal, or international law, or is in violation of DWMHA policy. Access to DWMHA workstations with EPHI must be controlled and authenticated.

IV. APPLICABILITY

This policy is applicable to all workforce members who use, are responsible for, or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following standards and safeguards must be implemented to satisfy the requirements of this policy:

1. DWMHA must prevent unauthorized physical access to workstations that can access EPHI and ensure that authorized workforce members have appropriate access.

2. All workforce members who use DWMHA workstations must take all reasonable precautions to protect the confidentiality, integrity, and availability of EPHI contained on or accessed by the workstations. For example, positioning monitors or shielding workstations so that data shown on the screen is not visible to unauthorized persons.

3. Unauthorized DWMHA workforce members must not willfully attempt to gain physical access to workstations that store or access EPHI.

4. DWMHA workforce members must report loss or theft of any access device (such as a card or token) that allows them physical access to areas having workstations that can access EPHI.

5. Access to all DWMHA workstations must be authenticated via a process that includes, at a minimum:

- Unique user IDs that enable users to be identified and tracked.
- Passwords must be masked, suppressed, or otherwise obscured so that unauthorized persons are not able to observe them.
- The initial password(s) issued to a new DWMHA workforce member must be valid only for the new user's first logon to a workstation. At initial logon, the user must be required to choose another password
- Upon termination of workforce member employment or contracted services, workstation access privileges will be removed.

6. DWMHA workforce members must not share their user accounts or passwords with others. If a workforce member believes that someone else is inappropriately using a user account or password, they must immediately notify their manager.

7. Anti-virus software must be installed on workstations to prevent transmission of malicious software. Such software must be regularly updated.

8. DWMHA workforce members must activate their workstation locking software whenever they leave their workstation unattended. DWMHA workforce members must log off from or lock their workstation(s) when their shifts are complete.

9. Connections from a workstation to a healthcare computing system must be logged off after the session is completed.

10. Special precautions must be taken with portable workstations such as laptops, smart phones, electronic tablets and personal digital assistants (PDA). At a minimum the following guidelines must be followed with such systems:

- EPHI must not be stored on portable workstations unless such information is appropriately protected. If EPHI is stored on the portable device, it must be encrypted.
- Locking software for unattended laptops must be activated.
- Portable workstations containing EPHI must be carried as carry-on (hand) baggage when workforce members use public transport. They must be concealed and/or locked when in private transport (e.g., locked in the trunk of an automobile).

11. For workstations with EPHI stored locally on hard drives or other memory devices, additional security measures are required. At a minimum these requirements include:

- Approval must be acquired prior to storing EPHI on workstations or devices external to the DWMHA's existing computer system. If approval is granted, DWMHA's HIPAA Security Officer will review the security controls against the HIPAA Security requirements.
- DWMHA must inventory and document EPHI stored on workstations when first installed and at least on an annual basis thereafter.
- DWMHA must review and document the security safeguards related to the protection of EPHI stored on their workforce member workstations.
- Data files containing EPHI will be encrypted wherever possible and password protected.

12. Report theft of all devices to DWMHA and the police immediately.

If the database or application will reside on a portable device, adherence to DWMHA Workstation Security Policy, #9000 is required.

Detroit Wayne Mental Health Authority

HIPAA Security Policies

Subject: Device and Media Controls	**Coverage:** DWMHA
Policy #: Security-10000	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility."*
Regulatory Reference:	45 CFR 164.310(d)(1)

I. PURPOSE

This policy reflects Detroit Wayne Mental Health Authority's commitment to appropriately control healthcare computing systems and their associated electronic media containing EPHI moving into, out of and within its facilities.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. POLICY

DWMHA must ensure EPHI located on DWMHA's healthcare computing systems and their associated electronic media must be protected against damage, theft, and unauthorized access. EPHI must be consistently protected and managed through its entire life cycle, from origination to destruction.

DWMHA must regularly conduct a formal, documented process that ensures consistent control of all healthcare computing systems and their associated electronic media containing EPHI that is created, sent, received or destroyed. The destruction of any EPHI should be governed by the DWMHA's Data Retention Policy. Questions concerning the destruction of EPHI should be directed to the DWMHA Privacy Officer.

IV. APPLICABILITY

This policy is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

1. All DWMHA healthcare computing systems and their associated electronic media containing EPHI must be located and stored in secure environments that are protected by appropriate security barriers and entry controls.

2. As defined in DWMHA's **Disposal Standard (Security - 10100)**, all healthcare computing systems and their associated electronic media containing EPHI must be disposed of securely and safely when no longer required. The destruction of any EPHI should be governed by the DWMHA's Data Retention Policy. Questions concerning the destruction of EPHI should be directed to the DWMHA Privacy Officer.

3. As defined in DWMHA's **Media Re-use Standard (Security – 10200)**, all EPHI on DWMHA healthcare computing systems and their associated electronic media must be carefully removed before the media or healthcare computing systems are made available for re-use.

4. As defined in DWMHA's **Accountability Standard (Security - 10300)**, all healthcare computing systems and their associated electronic media containing EPHI that is received by or removed from a sensitive area must be appropriately tracked and logged.

5. As defined in DWMHA's **Data Backup and Storage Standard (Security – 10400)**, backup copies of all EPHI located on DWMHA healthcare computing systems or their associated electronic media must be regularly made and stored securely.

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Disposal	**Coverage:** DWMHA
Standard #: Security-10100	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement policies and procedures to address the final disposition of EPHI, and/or the hardware or electronic media on which it is stored."*
Regulatory Reference:	45 CFR 64.310(d)(2)(i)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to appropriately dispose of healthcare computing systems and their associated electronic media containing EPHI when it is no longer needed.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

All DWMHA healthcare computing systems and their associated electronic media containing EPHI that are no longer required must be disposed of in a secure manner. Careless disposal of such information systems and media could result in EPHI being revealed to unauthorized persons. The destruction of any EPHI should be governed by the DWMHA's Data Retention Policy. Questions concerning the destruction of EPHI should be directed to the DWMHA Privacy Officer.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

1. All DWMHA healthcare computing systems and their associated electronic media containing EPHI must be disposed of properly when no longer needed for legitimate use. The destruction of any EPHI should be governed by the DWMHA's Data Retention Policy. Questions concerning the destruction of EPHI should be directed to the DWMHA Privacy Officer. Healthcare computing systems and electronic media to which this policy applies include, but are not limited to: computers (desktops, laptops, PDAs, tablets, etc.), floppy disks, backup tapes, CD\DVD-ROMs, zip drives, portable hard drives, flash memory devices and smart phones.

2. To dispose of a healthcare computing system or electronic medium containing EPHI, the data must be completely removed with data sanitization tool(s) that erase or overwrite media in a manner that prevents the data from being recovered. "Deleting" typically does not destroy data and may enable unauthorized persons to recover EPHI from the media.

3. An alternative to data sanitization of electronic media is physical destruction. The physical destruction of electronic media may be feasible where the media is inexpensive and the destruction methods are easy and safe. For example, floppy disks and CD-ROMs are relatively inexpensive and can be easily destroyed with a pair of scissors, if handled carefully.

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Media Re-use	**Coverage:** DWMHA
Standard #: Security-10200	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement procedures for removal of EPHI from electronic media before the media are made available for re-use."*
Regulatory Reference:	45 CFR 164.310(d)(2)(ii)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to erase all EPHI from electronic media associated with a healthcare computing system before its re-use.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

All EPHI on DWMHA's electronic media associated with a healthcare computing system must be removed before the media are re-used. Failure to remove EPHI could result in it being revealed to unauthorized persons.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

1. All EPHI on healthcare computing systems and their associated electronic media must be removed before the systems and media can be re-used. Healthcare computing systems and electronic media to which this policy applies include, but are not limited to: computers (desktops, laptops, PDAs, tablets, etc.), floppy disks, backup tapes, CD\DVD-ROMs, zip drives, portable hard drives, flash memory devices and smart phones.

2. EPHI on healthcare computing systems and their associated electronic media must be removed with data sanitization tool(s), which erase or overwrite media in a manner that prevents the data from being recovered. “Deleting” typically does not destroy data and may enable unauthorized persons to recover EPHI from the media.

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Accountability	**Coverage:** DWMHA
Standard #: Security-10300	**Page:** 1 of 2

HIPAA Security Rule Language:	*" Maintain a record of the movements of hardware and electronic media and any person responsible therefore."*
Regulatory Reference:	45 CFR 164.310(d)(2)(iii)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to appropriately track and log the movements of EPHI on healthcare computing systems and their associated electronic media and to hold DWMHA workforce members accountable for such movement.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

All movement of DWMHA healthcare computing systems and their associated electronic media containing EPHI into, out of, and within its facilities must be appropriately tracked and logged.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

1. DWMHA must maintain an inventory of all healthcare computing systems and their associated devices that store EPHI. The inventory must also identify the persons responsible for the devices containing EPHI.

2. DWMHA must maintain a record of the movement of healthcare computing systems and their associated media containing EPHI as it moves into and out of the facility.

3. Before healthcare computing systems and their associated media containing EPHI are moved to a location outside of DWMHA's premises, the move must be approved by the DWMHA and the move must be tracked and documented.

4. DWMHA workforce members, who move healthcare computing systems or their associated electronic media containing EPHI, are responsible for the subsequent use of such items and must take all appropriate and reasonable actions to protect them against damage, theft, and unauthorized access.

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Data Backup and Storage	**Coverage:** DWMHA
Standard #: Security-10400	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Create a retrievable, exact copy of EPHI, when needed, before movement of equipment."*
Regulatory Reference:	45 CFR 164.310(d)(2)(iv)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to backup and securely store all EPHI on its healthcare computing systems and their associated electronic media.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

All EPHI on DWMHA healthcare computing systems and their associated electronic media must be regularly backed up and securely stored. Backup and restoration procedures must be regularly tested.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

1. Backup copies of all EPHI on healthcare computing systems and their associated electronic media must be made regularly and stored in a secure location.

2. Backup and restoration procedures for healthcare computing systems and their associated electronic media must be regularly tested to ensure that they are effective and can be completed within a reasonable amount of time.

3. The healthcare computing system's backup media containing EPHI at a remote backup storage site must be given an appropriate level of physical and environmental protection consistent with the standards applied to the protection of EPHI at DWMHA.

4. The retention period for backup of EPHI on healthcare computing systems must be defined and documented.

Detroit Wayne Mental Health Authority

HIPAA Security Policies

Subject: Access Control	**Coverage:** DWMHA
Policy #: Security-11000	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights as specified in the Information Access Management Standard."*
Regulatory Reference:	45 CFR 164.312(a)(1)

I. PURPOSE

This policy reflects Detroit Wayne Mental Health Authority's commitment to implement policies and procedures for information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. POLICY

DWMHA must implement access control mechanisms for information systems that contain EPHI only to those persons and software programs that have been granted access rights.

IV. APPLICABILITY

This policy is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following standards and safeguards must be implemented to satisfy the requirements of this policy:

1. As defined in DWMHA's **Unique User Identification Standard (Security – 11100)**, access to DWMHA information systems must be via user identifiers that uniquely identify workforce members and enable activities with each identifier to be traced to a specific person or entity.

2. As defined in DWMHA's **Emergency Access Procedure Standard (Security – 11200),** DWMHA must have a formal, documented emergency access procedure enabling authorized workforce members to obtain required EPHI during an emergency.

3. As defined in DWMHA's **Automatic Logoff Standard (Security - 11300)**, DWMHA healthcare computing systems must automatically terminate electronic sessions when such sessions are not in use. If sessions cannot be terminated automatically, the workstations must be automatically locked after a period of inactivity.

4. As defined in DWMHA's **Encryption and Decryption Standard (Security – 11400)**, where necessary, appropriate encryption must be used to protect the confidentiality, integrity and availability of EPHI contained on DWMHA information systems.

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Unique User Identification	**Coverage:** DWMHA
Standard #: Security-11100	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Assign a unique name and/or number for identifying and tracking user identity."*
Regulatory Reference:	45 CFR 164.312(a)(2)(i)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to assign a unique name or number to identify and track the identity of workforce members who access DWMHA information systems containing EPHI.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

Access to DWMHA information systems containing EPHI must be via user identifiers that uniquely identify workforce members and enable activities of each identifier to be traced to a specific person or entity.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following safeguards must be implemented to satisfy the requirements of this standard:

1. DWMHA information systems must grant users access via unique identifiers that:

   - identify workforce members or users
   - allow activities performed on information systems to be traced back to a particular individual through tracking of unique identifiers.

2. Unique identifiers must not give any indication of the user's privilege level.

3. All DWMHA users must authenticate their identity by providing something they know or have, such as a password, personal identification number (PIN), token, or biometric feature.

4. Where DWMHA cannot implement unique user IDs for specific health care applications, they must implement appropriate compensating controls, such as maintaining a list of personnel with access to and knowledge of the credentials used to access the health care application, and changing of the "generic" credentials used to access the specific health care application whenever a person with knowledge of the credentials transfers or is no longer employed.

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Emergency Access Procedure	**Coverage:** DWMHA
Standard #: Security-11200	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Establish (and implement as needed) procedures for obtaining necessary EPHI during an emergency."*
Regulatory Reference:	45 CFR 164.312(a)(2)(ii)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to have an emergency access procedure enabling authorized workforce members to obtain required EPHI during an emergency.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must have a formal, documented emergency access procedure enabling authorized workforce members to obtain required EPHI during an emergency.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following safeguards must be implemented to satisfy the requirements of this standard:

1. DWMHA must have a formal, documented emergency access procedure enabling authorized workforce members to obtain required EPHI during an emergency. At a minimum, the procedure must:

- Identify and define manual and automated methods to be used by authorized DWMHA workforce members to access EPHI during an emergency.
- Identify and define appropriate logging and auditing that must occur when authorized DWMHA workforce members access EPHI during an emergency.

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Automatic Logoff	**Coverage:** DWMHA
Standard #: Security-11300	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."*
Regulatory Reference:	45 CFR 164.312(a)(2)(iii)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to develop and implement procedures for terminating electronic sessions on information systems that contain or access EPHI.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must terminate or lock inactive electronic sessions for information systems that contain or access EPHI.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following safeguards must be implemented to satisfy the requirements of this standard:

1. Where possible DWMHA must implement automatic logoffs for inactive health care applications sessions.

2. Where DWMHA cannot implement automatic logoffs for inactive health care applications, they must implement automatic locking on all workstations used to access those applications.

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Encryption and Decryption	**Coverage:** DWMHA
Standard #: Security-11400	**Page:** 1 of 2

HIPAA Security Rule Language:	"*Implement a mechanism to encrypt and decrypt EPHI.*"
Regulatory Reference:	45 CFR 164.312(a)(2)(iv)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to appropriately use encryption to protect the confidentiality, integrity and availability of EPHI contained on DWMHA healthcare computing systems.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

Where appropriate, encryption should be used to protect the confidentiality, integrity, and availability of EPHI contained on DWMHA healthcare computing systems. It is understood that the use of encryption implies that a reliable decryption method is employed.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following safeguards must be implemented to satisfy the requirements of this standard:

1. DWMHA must consider the following factors at a minimum in determining whether or not specific EPHI must be encrypted on a healthcare computing system:

- The sensitivity of the EPHI
- The risks to the EPHI
- The expected impact to DWMHA functionality and work flow if the EPHI is encrypted
- Alternative methods available to protect the confidentiality, integrity, and availability of the EPHI

Detroit Wayne Mental Health Authority

HIPAA Security Policies

Subject: Audit Controls	**Coverage:** DWMHA
Policy #: Security-12000	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI."*
Regulatory Reference:	45 CFR 164.312(b)

I. PURPOSE

This policy reflects Detroit Wayne Mental Health Authority's commitment to use appropriate audit controls on its information systems that contain or use EPHI.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. POLICY

DWMHA must record and examine significant activity on its information systems that contain or use EPHI. Appropriate hardware, software, or procedural auditing mechanisms must be implemented on DWMHA information systems that contain or use EPHI.

IV. APPLICABILITY

This policy is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following standards and safeguards must be implemented to satisfy the requirements of this policy:

1. DWMHA must record and examine significant activity on its information systems that contain or use EPHI. DWMHA must identify, define, and document what constitutes "significant activity" on a specific information system. Such activity might include:

- User access to EPHI and user account activity
- Use of certain software programs or utilities
- Use of a privileged account
- Healthcare computing system anomalies, such as unplanned system shutdown or application errors
- Failed and successful authentication attempts

2. Appropriate hardware, software, or procedural auditing mechanisms must be implemented on DWMHA healthcare systems that contain or use EPHI. At a minimum, such mechanisms must provide the following information:

- Date and time of activity
- Origin of activity
- Identification of user performing activity
- Description of attempted or completed activity

3. DWMHA must develop and implement a formal process for audit log review. At a minimum, the process must include:

- Definition of which workforce members will review records of activity
- Definition of what activity is significant
- Procedures defining how significant activity will be identified and reported
- Procedures for preserving records of significant activity

4. When possible, DWMHA workforce members should not review audit logs that pertain to their own system activity. In addition, workforce members should not have the ability to alter or delete log entries that pertain to their own system activity. If it is not possible to limit this access, management should ensure that appropriate compensating controls are documented and implemented.

Detroit Wayne Mental Health Authority

HIPAA Security Policies

Subject: Integrity	**Coverage:** DWMHA
Policy #: Security-13000	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement policies and procedures to protect EPHI from improper alteration or destruction."*
Regulatory Reference:	45 CFR 164.312(c)(1)

I. PURPOSE

This policy reflects Detroit Wayne Mental Health Authority's commitment to ensure the confidentiality, integrity, and availability of its healthcare computing systems containing EPHI by implementing policies and procedures to prevent, detect, contain, and correct security violations.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. POLICY

DWMHA must appropriately protect the integrity of all EPHI contained on its healthcare computing systems. Such EPHI must be protected from improper alteration or destruction.

IV. APPLICABILITY

This policy is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI that is accessed remotely by healthcare workers.

V. PROCEDURE

1. As defined in DWMHA's **Mechanism to Authenticate Electronic Protected Health Information Standard (Security - 13100)**, DWMHA must implement a formal, documented process for appropriately protecting the integrity of all EPHI contained on its healthcare computing systems.

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Mechanism to Authenticate Electronic Protected Health Information	**Coverage:** DWMHA
Standard #: Security-13100	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner."*
Regulatory Reference:	45 CFR 164.312(c)(2)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to implement appropriate electronic mechanisms to confirm that electronic EPHI contained on DWMHA healthcare computing systems has not been altered or destroyed in an unauthorized manner.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

DWMHA must implement appropriate electronic mechanisms to confirm that EPHI contained on DWMHA healthcare computing systems has not been altered or destroyed in an unauthorized way.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

1. Electronic mechanisms used to protect the integrity of EPHI contained on DWMHA healthcare computing systems must ensure that the value and state of the EPHI is maintained, and it is protected from unauthorized modification and destruction. Such mechanisms must also be capable of detecting unauthorized alteration or destruction of EPHI. Such mechanisms might include:

- System memory, hard drives, and other data storage devices with error-detection capabilities
- File and data checksums
- Encryption

Detroit Wayne Mental Health Authority

HIPAA Security Policies

Subject: Person or Entity Authentication	**Coverage:** DWMHA
Policy #: Security-14000	**Page:** 1 of 2

HIPAA Security Rule Language:	*"Implement procedures to verify that a person or entity seeking access to EPHI is the one claimed."*
Regulatory Reference:	45 CFR 164.312(d)

I. PURPOSE

This policy reflects Detroit Wayne Mental Health Authority's commitment to ensure that all persons or entities seeking access to the DWMHA's EPHI are appropriately authenticated before access is granted.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. POLICY

DWMHA must authenticate all persons or entities seeking access to the DWMHA's EPHI before access is granted. DWMHA must use an appropriate and reasonable system(s) to ensure that only properly authenticated persons and entities access its EPHI.

IV. APPLICABILITY

This policy is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI that is accessed remotely by healthcare workers.

V. PROCEDURE

1. DWMHA must authenticate all persons or entities seeking access to the DWMHA's EPHI before access is granted. Authentication may include, but is not limited to the following:

    - User name and password
    - Biometrics
    - Challenge and response mechanisms
    - Secure identification cards

Detroit Wayne Mental Health Authority

HIPAA Security Policies

Subject: Transmission Security	**Coverage:** DWMHA
Policy #: Security-15000	**Page:** 1 of 2

HIPAA Security Rule Language:	"*Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.*"
Regulatory Reference:	45 CFR 164.312(e)(1)

I. PURPOSE

This policy reflects Detroit Wayne Mental Health Authority's commitment to appropriately protect the confidentiality, integrity, and availability of all EPHI that it transmits over electronic communications networks.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. POLICY

DWMHA must appropriately protect the confidentiality, integrity, and availability of all EPHI it transmits over electronic communications networks.

IV. APPLICABILITY

This policy is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI that is accessed remotely by healthcare workers.

V. PROCEDURE

1. As defined in DWMHA's **Integrity Controls Standard Security - 15100)**, DWMHA must use integrity controls where appropriate to protect the confidentiality, integrity, and availability of EPHI transmitted over electronic communications networks.

2. As defined in DWMHA's **Encryption Standard (Security – 15200)**, DWMHA must use encryption where appropriate to protect the confidentiality, integrity, and availability of EPHI transmitted over electronic communications networks.

Detroit- Wayne Mental Health Authority

HIPAA Security Standards

Subject: Integrity Controls	**Coverage:** DWMHA
Standard #: Security-15100	**Page:** 1 of 2

HIPAA Security Rule Language:	"*Implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of.*"
Regulatory Reference:	45 CFR 164.312(e)(2)(i)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to use appropriate integrity controls to protect the confidentiality, integrity, and availability of EPHI transmitted over electronic communications networks.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

Appropriate integrity controls must be used to protect the confidentiality, integrity, and availability of DWMHA EPHI transmitted over electronic communications networks. DWMHA's integrity controls must ensure that the value and state of all transmitted EPHI is maintained, and the data is protected from unauthorized modification.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

1. DWMHA must use integrity controls that are appropriate for protecting the confidentiality, integrity, and availability of EPHI transmitted over electronic communications networks. The appropriateness of controls must be based upon sensitivity of and risks to EPHI. For example, EPHI transmitted over public networks represent a much higher risk than EPHI transmitted over DWMHA's healthcare network. Integrity controls may include, but are not limited to:

- Encryption
- Checksums
- Point-to-point communications, such as Virtual Private Networks (VPN)
- Switched networks

Detroit Wayne Mental Health Authority

HIPAA Security Standards

Subject: Encryption	**Coverage:** DWMHA
Standard #: Security-15200	**Page:** 1 of 2

HIPAA Security Rule Language:	"*Implement a mechanism to encrypt EPHI whenever deemed appropriate.*"
Regulatory Reference:	45 CFR 164.312(e)(2)(ii)

I. PURPOSE

This standard reflects Detroit Wayne Mental Health Authority's commitment to appropriately use encryption to protect the confidentiality, integrity and availability of EPHI transmitted over electronic communications networks.

II. AUTHORIZATION AND ENFORCEMENT

DWMHA management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWMHA IT Security Officer, DWMHA HIPAA Security Officer, and DWMHA HIPAA Privacy Officer.

III. STANDARD

Appropriate encryption must be used to protect the confidentiality, integrity, and availability of DWMHA EPHI transmitted over electronic communications networks.

IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

1. DWMHA must consider the following factors at a minimum in determining whether or not encryption must be used when sending specific EPHI over an electronic communications network:

- The sensitivity of the EPHI
- The risks to the EPHI
- The expected impact to DWMHA functionality and work flow if the EPHI is encrypted
- Alternative methods available to protect the confidentiality, integrity and availability of the EPHI