

MCCMH MCO Policy 10-410

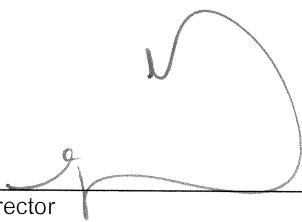
(was Administrative Policy 9-10-010)

Chapter: **DIRECTLY-OPERATED PROGRAM MANAGEMENT**
Title: **SECURITY OVERVIEW**

Prior Approval Date: 12/06/07
Current Approval Date: 9/9/10

Approved by: _____

Executive Director



Date

09/09/10

I. ABSTRACT

This policy establishes the standards and procedures of the Macomb County Community Mental Health Board (MCCMH) for compliance with the Security Rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) by implementing security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Administrative Standards.

II. APPLICATION

This policy shall apply to the MCCMH administrative offices and to all directly-operated network providers of the MCCMH Board.

III. POLICY

It is the policy of the MCCMH Board to ensure the privacy and security of the creation, receipt, maintenance, and transmission of electronic protected health information.

IV. DEFINITIONS

- A. Electronic Protected Health Information (EPHI)
Protected Health Information means individually identifiable health information: transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium. EPHI is defined within HIPAA legislation within paragraphs (1)(i) or (1)(ii) of the definition of protected health information.

- B. **Security Officer**
The MCCMH employee who has been assigned security responsibility by MCCMH.
- C. **Risk Analysis**
Conducting an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
- D. **Security Incident**
The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- E. **Security Implementation**
Mechanism to authenticate electronic protected health information by verifying that electronic protected health information has not been altered or destroyed in an unauthorized manner.
- F. **Authenticate**
Verifying that a person or entity seeking access to electronic protected health information is the person/entity claimed.

V. STANDARDS

- A. In accordance with HIPAA Security Rules, MCCMH Security standards are based on the following principles:
 - 1. Access to data systems is granted on a need to know basis;
 - 2. Level of access is determined by position role and function within the organization;
 - 3. Role and function are determined by Administrative / Management / Supervisory staff and access is implemented by the MCCMH Department(s) as assigned by the MCCMH Deputy Director.
 - 4. MCCMH shall implement security using all reasonable, available, effective and commonly-accepted methods of security.
- B. Following these principles, MCCMH shall:
 - 1. Ensure the confidentiality, integrity, and availability of all electronic protected health information it creates, receives, maintains, or transmits;
 - 2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the HIPAA Standards; and
4. Ensure compliance by its workforce.

C. MCCMH has:

1. Created the position of HIPAA Security Officer who is responsible for the ongoing management of MCCMH information security policies and technical systems in order to maintain the confidentiality, integrity, and availability of all organizational healthcare information systems.
2. Created an organizational infrastructure to measure the security of its electronically protected health information. This consists of a Security Team, consisting of the Security Officer and representatives from across the organization that can define policies and procedures that will secure the data. Subteams may be appointed as appropriate to further define or address specific issues.
3. Established a mechanism for upper management to regularly review the Security Team's work, thus providing instruction, feedback, and approval as appropriate. Upper management involvement is critical to counter resistance within an organization.
4. Performed a risk analysis which reviewed MCCMH's cost of risk today (i.e., what security losses would occur if no additional security action were taken). With this data, MCCMH evaluated various security implementations (safeguards) to determine reasonable and appropriate safeguards in the environment. Safeguards were analyzed with reference to the likely contribution to protecting MCCMH's electronic protected health information.
5. MCCMH has implemented the security implementations which were determined to be reasonable and appropriate.

VI. PROCEDURES

A. The HIPAA Security Officer is responsible for:

1. Implementing, managing, and enforcing information security directives as mandated by HIPAA;
2. Ensuring the ongoing integration of information security with business strategies and requirements;
3. Ensuring that the access control, disaster recovery, business continuity, security incident response, and risk management needs of the organization are properly addressed;

4. Leading information security awareness and training initiatives to educate workforce about information risks;
5. Performing ongoing information risk assessments and audits to ensure that MCCMH's information systems are adequately protected and meet HIPAA certification requirements;
6. Working with vendors, outside consultants, and other third parties to improve information security within the organization; and
7. Leading a security incident response effort to contain, investigate, and prevent further computer security breaches.

VII. REFERENCES / LEGAL AUTHORITY

- A. Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104-191
- B. 45 CFR §§160.103, 164.105, 304, 306(d)(3), 308(a), and 316

VIII. EXHIBITS

- A. None.