

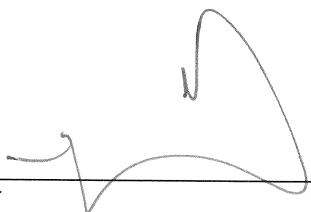
MCCMH MCO Policy 10-420

(was Administrative Policy 9-10-030)

Chapter: **DIRECTLY-OPERATED PROGRAM MANAGEMENT**
Title: **PERIODIC SECURITY EVALUATION**

Prior Approval Date: 12/6/07
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 ensuring that each security policy and security procedure developed and implemented by MCCMH is periodically evaluated for technical and non-technical viability.

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 maintain up to date security policies to effectively ensure the confidentiality, integrity and availability of electronically protected health information created, received, maintained and transmitted by MCCMH.

IV. Definitions

A. None.

V. Standards

A. Periodic Evaluation Generally

1. MCCMH security policies and directly-operated network provider security procedures initially should be evaluated to determine their compliance with the Security Administrative Standards. Once compliance with the Security Administrative Standards is established, the MCCMH security policies and directly-operated network provider security procedures shall be evaluated on a periodic basis to assure continued viability in light of technological, environmental or operational changes that could affect the security of electronically protected health information.

VI. Procedures

A. Periodic Evaluation by MCCMH HIPAA Security Officer

1. The HIPAA Security Officer will review on an on-going basis the viability of MCCMH security policies and procedures.
2. The HIPAA Security Officer will develop and recommend to the HIPAA Security Team any necessary security policy or security procedure changes.

B. Periodic Evaluation by MCCMH HIPAA Security Team

1. The HIPAA Security Team will reconvene on an annual basis to evaluate the technical and non-technical viability of MCCMH security policies. It is the responsibility of the MCCMH Security Officer to reconvene the HIPAA Security Team in accordance with this policy.
2. Any member of the HIPAA Security Team, or any other MCCMH staff person may suggest changes to the security policies or procedures by submitting such suggestion to the HIPAA Officer for consideration.
3. The HIPAA Security Team will review any suggested security policy or security procedure change and make a recommendation to the Security Officer for policy draft/changes to be approved by MCCMH Executive Staff.

C. Evaluation upon Occurrence of Certain Events

1. In the event that one or more of the following events occur, the policy evaluation process described in Standard V.B. 2 may be immediately triggered:
 - a. Changes in:

- The HIPAA Security Administrative Standards or Privacy Regulations
 - New federal, state, or local laws or regulations affecting the privacy or security of electronically protected health information
 - Changes in technology, environmental processes or business processes that may affect HIPAA security policies or security procedures
 - A serious security violation, breach, or other security incident occurs
- b. The HIPAA Security Officer may reconvene the HIPAA Security Team when deemed necessary based on information received from, but not limited to, an internal audit, routine monitoring, or otherwise reported security concern.

VII. References / Legal Authority

- A. Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104-191
- B. 45 CFR § 164.308(a)(8)

VIII. Exhibits

- A. None.