MCCMH MCO Policy 10-415

(was Administrative Policy 9-10-020)

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

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

Approved by: ______________________ 09/09/10
Executive Director Date

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 establishing the process for security audits.

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 confidentiality, integrity, and availability of electronic protected health information (EPHI) and resources by implementing hardware, software, and/or procedural mechanisms that record and examine activity in the MCCMH information systems that contain or use EPHI.

IV. DEFINITIONS

A. Security Audit
A comprehensive means of determining if security violations are taking place and the scope of the damage that would be experienced if they were. A comprehensive security assessment includes penetration testing of internal and external systems and a review of security strategies, policies, and procedure.

B. User
A person or entity with authorized access.

V. STANDARDS

A. Audits and Other Evaluation Techniques

1. The MCCMH Board recognizes extensive auditing and monitoring of its directly-operated programs, records, and activities is necessary to detect violations of the HIPAA Security Administrative Standards. The HIPAA Security Office is delegated the duty to ensure that there is a management process to audit and monitor, at regular intervals, the performance of the Board, its employees/individual contractors, and its providers regarding the security program. The HIPAA Security Office will use County Corporation Counsel when necessary to maintain attorney-client confidentiality.

2. The HIPAA Security Officer will ensure that the audits include, at a minimum, any attempt to achieve an unauthorized security level by any person, process, or other entity in the network. This includes login and logout, super user access and any "anonymous" or "guest" access to public servers.

3. Security audit data shall be carefully secured at the site and in backups.

B. At least once a year, the HIPAA Security Officer shall be responsible for generating an Annual Report of MCCMH HIPAA Security Audits. The report should inform the Board Executives and the Board of Directors of the strengths and weaknesses of the HIPAA Security Audits, how they should be altered to prevent violations in the future, and whether they should be changed in scope or frequency to better detect violations. The report will contain, at a minimum, a summary of the year’s security audits for the previous 12-month period.

VI. PROCEDURES

A. MCCMH shall:

1. Subscribe to advisories that are issued by various security incident response entities (e.g., operating systems security announcements, virus protection vendor security announcements);

2. Ensure that security patches that are produced by MCCMH equipment vendors are installed;

3. Actively watch the configurations of MCCMH electronic systems to identify any changes that may have occurred;

4. Review all security policies and procedures regularly;

5. Read relevant materials and/or receive appropriate training(s) to keep up to date; and

6. Regularly check for compliance with policies and procedures.

B. The Security Officer shall treat each security incident seriously, but shall determine the role the user played (e.g., was the user naive?) and whether there could be a mistake in attributing the security breach to the user.

VII. REFERENCES / LEGAL AUTHORITY

A. Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104-191

B. 45 CFR §§ 164.304, 164.312(b)

VIII. EXHIBITS

A. None.