MCCMH MCO Policy 10-465

(was Administrative Policy 9-10-120)

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

Prior Approval Date: 12/6/07
Current Approval Date: 9/09/10

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 limiting physical access to its electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed.

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 control and validate access to facilities where electronic information systems are housed, and document repairs and modifications to the physical components of the electronic information systems.

IV. Definitions

A. Facility
The physical premises and the interior and exterior of a building.

B. Physical Standards
physical measures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

V. Standards

A. MCCMH will maintain physical safeguards for its facilities to ensure that electronic information systems are secure from unauthorized access.

B. Non-compliance with this policy may result in immediate disciplinary action, up to and including termination of employment and potential criminal prosecution in accordance with MCCMH MCO Policy 10-435.

VI. Procedures

A. The main file server for the MCCMH information system shall be maintained in a building which has a staffed security checkpoint controlling access to the building.

B. The main file server room shall be secured with a lock or key pad.

C. MCCMH Information Technology staff (IT) shall deploy auto lockouts to all sites which will lock sessions after predetermined amounts of inactivity and which requires passwords to re-access.

D. MCCMH Network Administrator shall determine the length of time until lockout based on the assessment of risk for the various workstations.

E. Maintenance of the electronic information system can only be performed by MCCMH internal IT staff or MCCMH authorized vendors.

F. The MCCMH Security Officer, in conjunction with the MCCMH Network Administrator, shall ensure that processes exist to ensure that:

1. There is facility access for designated staff to restore lost data and/or, under the disaster recovery plan, initiate emergency mode operations, if necessary, in the event of an emergency;

2. The facility and the equipment therein are safeguarded from unauthorized physical access, tampering, and theft;

3. Access to facilities are controlled based on role or function; and

4. Repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks) are documented.

VII. References / Legal Authority

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

B. 45 CFR §§ 164.304, 164.310(a)(2)(ii)

VIII. Exhibits

A. None.