

MCCMH MCO Policy 10-440

(was Administrative Policy 9-10-070)

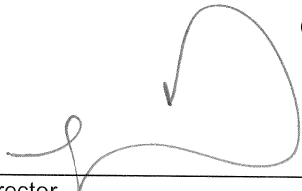
---

---

Chapter: **DIRECTLY-OPERATED PROGRAM MANAGEMENT**  
Title: **ACCESS CONTROL**

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 procedures to limit physical access to its electronic information systems and the facility or 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 physical and electronic access to protected health information through procedures which establish rules for granting access, determining initial right of access, and modifying the right to access.

**IV. Definitions**

**A. Access**

The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any electronic system resource.

- B. Access Authorization  
Granting access to electronic protected health information through access to workstations, transactions, programs, processes, or other mechanisms.
- C. Password  
A personal identifier used for access to an electronic system.
- D. User  
Person or entity with authorized access.
- E. Workstation  
An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

## **V. Standards**

- A. MCCMH shall establish procedures for access control and validation for the electronic information system and personnel security.
- B. MCCMH staff shall adhere to the procedures for security protection of the electronic information system or contained in this policy.
- C. MCCMH Administrative and Management staff shall ensure that staff members comply with the security mechanisms/procedures delineated in this policy.

## **VI. Procedures**

- A. Access Control & Other Validation Procedures
  - 1. The level of access control shall depend on user need and the level of risk and exposure to loss or compromise.
  - 2. Portable computers (eg. laptops) that have electronic protected health information shall be encrypted through the use of an encryption engine (e.g. PGP).
  - 3. Electronic access shall be controlled through authentication. Each use shall be uniquely identified and passwords shall be used to authenticate identity.
  - 4. Passwords (personal identifiers) shall not be shared.
  - 5. Users are required to change their password every six months. The MCCMH Information Technology (IT) staff shall periodically send reminders to do so.
  - 6. When leaving a server, workstation, or other computer system unattended, staff shall lock or activate the system's automatic log-off mechanism.

7. Users are responsible and accountable for access under their personal identifiers/ passwords.
8. Control configurations shall be developed for each file or database.
9. All files containing electronic protected health information shall be stored on the network, with the appropriate access controls.

**B. Personnel Security**

1. Access to specific data elements, files, functions, menus, commands and networks is based on the user's responsibilities or job functions.
2. A record shall be maintained of all access authorizations.
3. Visitor control to clinical sites is restricted.
4. The Security Officer, in conjunction with other staff from MCCMH Department(s) as assigned by the MCCMH Deputy Director, shall determine the proper access level to be granted to individuals working with protected health information.

**C. User log-in education will include, at least:**

1. Configuration of components to record log-in attempts (both successful and unsuccessful);
2. Importance of monitoring log-in success or failure;
3. Steps for checking last log-in information, and reporting suspicious information;
4. How to report discrepancies of log-in; and
5. The user's responsibility to ensure the security of health care information.

**VII. References / Legal Authority**

- A. Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104-191
- B. 45 CFR §§ 164.304, 164.308(a)(5)(ii)(B), 45 CFR § 164.310(a)(2)(iii)

**VIII. Exhibits**

- A. None.