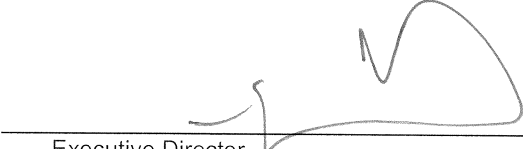


*(was Administrative Policy 9-10-040)*

Chapter: **DIRECTLY-OPERATED PROGRAM MANAGEMENT**  
Title: **SECURITY AWARENESS TRAINING**

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

Approved by:  \_\_\_\_\_  
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 conducting periodic security training.

**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 train its entire workforce (full and part time employees, independent contractors, interns, and volunteers) in the security of electronically protected health information.

**IV. Definitions**

- A. Business Associate  
Any entity which:
  1. performs a function or activity on behalf of the MCCMH Board that involves the use or disclosure of personal health information or provides any legal,

actuarial, accounting, consulting, data aggregation or management, administrative, accreditation, or financial services to or for the Board;

2. Is not involved in the treatment of consumers; and
3. Is not providing consumer-conducted financial transactions.

## **V. Standards**

- A. MCCMH, through its Security Officer, shall develop and implement a Security Education Training curriculum to meet required provisions contained in this policy.
- B. Security training shall be provided to all new and current workforce with refresher trainings annually.
- C. Revised security training shall be prepared and provided to the workforce when there are material changes to MCCMH security practices or the security rules.
- D. Security training shall be mandatory for all staff.
- E. MCCMH Administration and Management shall ensure staff compliance to this policy.

## **VI. Procedures**

- A. All current MCCMH staff members and individual contractors shall be offered training on the HIPAA Security Rules and MCCMH Security policies and practices on or before the effective date of the HIPAA Security Rules or as soon as feasible after that date with annual refresher training related to security awareness.
- B. All new staff will be trained on Macomb County Community Mental Health Board's security practices and the HIPAA Security Rules within 90 days of employment as part of their orientation to MCCMH.
- C. Security training shall be mandatory for the MCCMH workforce. Staff members who fail to attend required security training shall be referred to the Deputy Director for appropriate action.
- D. Employees/individual contractors in identified risk areas will receive more detailed security education related to their function and responsibilities.
- E. The Security Officer is responsible for ensuring the development of the security education curriculum and monitoring and ensuring that the security training and orientation meets the policy standards on this subject.

- F. Initial and refresher security awareness education seminars must include an explanation of the structure and operation of the Security program. They will introduce the Security Officer to MCCMH and provide information on how to contact the Security Officer and get additional information.
- G. Initial and refresher security awareness education seminars, at a minimum, will include information on the following aspects of the security program:
  - 1. HIPAA Security standards overview;
  - 2. Overview of MCCMH policies and procedures, including how to access and gain clarification regarding such;
  - 3. Overall discussion of threats and vulnerabilities specific to electronic protected health information;
  - 4. Information access control;
  - 5. Personnel clearance levels;
  - 6. Security Incident reporting;
  - 7. Viruses and other forms of malicious software;
  - 8. Periodic security updates;
  - 9. Log-in;
  - 10. Password management;
  - 11. The sanctions and civil and criminal penalties prescribed for wrongful actions, as well as the potential for violations to be reported to external agencies.
- H. The training methods can vary with the content and may include workshops, self-study modules, on-line training, staff meetings, and so forth. The trainings shall be completed within 30 days of the implementation date for material changes in MCCMH security practices.
- I. The MCCMH Security Officer must approve all training curriculum developed on security practices or the Security Rules. Attendees shall be provided evaluation forms to complete pertaining to initial security training. The MCCMH Security Officer shall keep copies of all attendance sheets, handouts, slides and curriculum, and evaluations will be kept in an administrative file.
- J. Annual refresher security training seminars may be available to employees/individual contractors in either electronic (e.g. computer, Internet, or video) or face-to-face formats. Employees/individual contractors will be required to attend a face-to-face refresher training minimally every three calendar years.
- K. Education materials will be developed to facilitate the security awareness sessions and ensure that a consistent message is delivered to all employees/individual contractors. Education protocols and materials must be standardized, so that everyone attending a seminar receives the same instruction.
- L. HIPAA security awareness training will be incorporated into the existing training modules MCCMH has established including:

- The Annual Training Plan
  - New Employee Orientation
  - Compliance Training
  - HIPAA Privacy Training
  - Person-Centered Planning
  - Cultural Competence
- M. The MCCMH Security Officer shall develop and implement revised security training when there are material changes to the organization's security practices or changes to the Security Rules. The training plan may focus on specific programs or may include the entire MCCMH administrative and direct service system staff depending on the scope of the changes involved.
- N. The Security Officer shall submit periodic reports to the Security Committee on all security awareness seminars.
- O. The Security Officer shall periodically send out security reminders to MCCMH staff, as well as business associates, if necessary, to make them aware of security concerns and initiatives on an ongoing basis.
- P. Urgent updates, such as new threats, hazards, vulnerabilities and/or countermeasures shall be distributed by the Security Officer and/or the MCCMH Information Technology (IT) unit.

#### **VII. References / Legal Authority**

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

#### **VIII. Exhibits**

- A. None.