MCCMH MCO Policy 10-470

(was Administrative Policy 9-10-140)

Chapter: **DIRECTLY-OPERATED PROGRAM MANAGEMENT**
Title: **CONTINGENCY PLANS FOR EPHI 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) to ensure that its response to an emergency or other occurrence that damages systems that contain electronic protected health information (EPHI) complies with the Security Rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

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 protect the availability, integrity, and security of electronic data during unexpected negative events by ensuring that MCCMH can appropriately respond to an emergency, natural disaster or other occurrence, including but not limited to fire, vandalism, terrorism, system failure, procedural failure, or natural disaster, that affects any system or network used to access, store, transmit, or receive EPHI.

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 shall develop and implement a disaster recovery plan to protect electronic data from destruction or loss due to an emergency, natural disaster, or other occurrence.

B. MCCMH shall develop and implement a back-up plan for EPHI data storage in a physically secure environment.

C. MCCMH shall develop and implement an emergency mode operations plan to ensure continuation of critical business operations in an emergency.

VI. Procedures

A. Applications and Data Criticality Analysis

1. The MCCMH Information Technology (IT) staff unit shall conduct a critical assessment of data and application criticality periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

2. The MCCMH Security Officer, in conjunction with the MCCMH IT staff, shall assess the relative criticality of specific applications and data within MCCMH for purposes of developing the data backup plan, the disaster recovery plan and the emergency mode operation plan.

B. Data Backup Plan

1. The MCCMH IT staff unit shall maintain a data backup plan which requires that all media used for backing up EPHI be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.

2. Pursuant to the data backup plan, the MCCMH IT staff unit would create and maintain retrievable exact copies of all EPHI determined to be medium and high risk.

3. The data backup plan shall apply to all medium and high risk files, records, images, voice or video files that may contain EPHI.

4. If an off-site storage facility or backup service is used, a written contract or Business Associate Agreement shall be executed to ensure that the Business Associate will safeguard the EPHI in an appropriate manner.

5. The MCCMH IT staff unit shall test the data backup procedures outlined in the data backup plan on a periodic basis to ensure that exact copies of EPHI can be retrieved and made available.

C. Disaster Recovery Plan

1. The MCCMH IT staff unit shall maintain a disaster recovery plan pursuant to which it can restore or recover any loss of EPHI and the systems needed to make that EPHI available in a timely manner.

2. The MCCMH disaster recovery plan shall include procedures to restore EPHI from data backups in the case of a disaster causing data loss.

3. The MCCMH disaster recovery plan shall include a system for logging system outages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan.

4. The MCCMH disaster recovery plan shall be documented and easily available to the necessary personnel at all times, who are trained to implement the disaster recovery plan.

5. The disaster recovery procedures outlined in the MCCMH disaster recovery plan shall be tested on a periodic basis to ensure that EPHI and the systems needed to make EPHI available can be restored or recovered.

D. Emergency Mode Operation Plan

1. The MCCMH IT staff shall develop and maintain an Emergency Mode Operations Plan.

2. The Emergency Mode Operations Plan shall be easily available to necessary personnel at all times, who are trained in the processes for emergency mode operations.

3. The MCCMH IT staff shall test the emergency mode operation procedures on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.

VII. References / Legal Authority

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

B. 45 CFR §§ 164.308(a)(7)(i), 164.310(a)(2)(i)

VIII. Exhibits

A. None.