MCCMH MCO Policy 10-455

(was Administrative Policy 9-10-100)

Chapter: **DIRECTLY-OPERATED PROGRAM MANAGEMENT**
Title: **VIRUS PROTECTION**

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

Approved by: _____ 9/09/10
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 protecting its computers from malicious software.

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 that its electronic information system be protected against malicious software and that all appropriate measures be taken to achieve that protection.

IV. Definitions

A. Malicious Software
Software, such as a virus, designed to damage or disrupt a system.

B. User
Person or entity with authorized access.

V. Standards

A. MCCMH shall maintain protection against viruses, spyware and other malware which conforms to generally accepted information technology (IT) standards.

B. Management and Supervisory staff shall ensure that staff adhere to the above standards.

VI. Procedures

A. MCCMH electronic system software, including virus signature files, shall be promptly updated as released by the software vendors.

B. MCCMH shall employ automated methods to routinely scan all servers and workstations.

C. MCCMH staff shall be prohibited from installing any software on MCCMH network or standalone equipment prior to authorization from the MCCMH IT staff.

D. MCCMH Network Administrator shall ensure that:

1. Only software that can be verified to be free of harmful code or other destructive aspects shall be utilized throughout the MCCMH directly-operated provider network.

2. Complete information about the software deployed in the MCCMH network is maintained, such as the vendor address and telephone number, the license number and version, and update information.

3. Configuration reports of all installed software, including the operating system are maintained.

4. Software programs are re-installed from original media.

5. Software installation media are stored in a secure, tamper-proof location.

6. System and application bug fixes or patches shall be accepted only from reliable sources, such as MCCMH software vendors.

E. To protect the organization against virus and malware attacks, MCCMH Network Administrator shall:

1. Verify virus threats, to rule out possibility of hoax, before notification of the threat is transmitted;

2. Develop internal escalation procedures and virus severity levels; and

3. Develop processes to identify, contain, eradicate, and recover from virus events.

F. MCCMH staff shall report all suspected virus occurrences to the MCCMH IT staff who shall inform the MCCMH Security Officer as appropriate.

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)

VIII. Exhibits

A. None.