MCCMH MCO Policy 10-430

(was Administrative Policy 9-10-050)

Chapter: **DIRECTLY-OPERATED PROGRAM MANAGEMENT**
Title: **SECURITY INCIDENT REPORTING PROCESS**

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

Approved by: _____ 09/04/10
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 establishing the process for regularly identifying, reporting, mitigating, and documenting the effects of Security Incidents and their outcomes.

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 the confidentiality, integrity, and availability of electronically protected health information (EPHI) be protected by ensuring that all security incidents are appropriately identified, reported, mitigated, and documented.

IV. Definitions

A. Security Incident
The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

V. Standards

A. MCCMH shall establish a system to identify, monitor, correct and document security incidents which affect or may threaten the MCCMH Information System network and/or EPHI.

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

C. The entire MCCMH workforce is responsible for complying with MCCMH security measures for its electronic information system.

VI. Procedures

A. MCCMH shall maintain internal reporting processes to ensure that employees, contractors, or other interested parties can easily report security incidents or suspected security incidents which affect MCCMH.

B. Security incidents that should be reported include, but are not limited to:

1. Virus, worm, or other malicious code attacks which result in intrusion and/or damage to the MCCMH network;

2. Network or system intrusions;

3. Persistent intrusion attempts from a particular entity;

4. Unauthorized access to EPHI, EPHI-based system, or EPHI-based network; and

5. Unrecoverable EPHI data loss due to disaster, failure, or error.

C. Response to a security incident shall prioritize the actions to be taken during an incident to:

1. Protect human life and safety;

2. Protect classified and/or sensitive data;

3. Protect other data;

4. Prevent damage to electronic systems; and

5. Minimize disruption of computing resources (including processes).

D. No retaliatory action will be taken against any employee/individual contractor or other party who reports a security violation in good faith, regardless of the

seriousness of the security incident or the level of employee/individual contractor or agent responsible for the violation. Identification of a reporting party who requests anonymity shall be protected to the degree feasible. Whenever reporting parties disclose their identities, they will be held in confidence to the fullest extent practical or allowed by law. If disclosure of the reporting party's identity occurs, MCCMH will ensure that he or she is not disciplined or penalized for reporting the security violation.

E. Workforce Reporting:

1. Any MCCMH staff member who believes that a security incident has occurred shall report those concerns to his/her supervisor and to the MCCMH Information Technology (IT) staff.

2. The administrative/program supervisor shall notify MCCMH IT staff if a security incident involving penetration of a virus or unauthorized access to EPHI occurs or is suspected.

3. The MCCMH IT Network Administrator shall keep the MCCMH Security Officer informed of any security incident.

4. The MCCMH Security Officer shall publish the e-mail addresses and telephone numbers of the MCCMH IT unit, as well as his/her own.

5. The MCCMH IT Network Administrator and/or the MCCMH Security Officer shall be available to meet with employees/individual contractors or other persons who choose to make security incident inquiries and reports in person.

F. Monitoring and Reporting:

1. MCCMH IT staff is responsible for monitoring the security of the MCCMH network through generally accepted standard software and hardware tools available for this purpose.

2. Serious incidents which result or could have resulted in an occurrence described in VI.B. shall be reported to the MCCMH Security Officer by the MCCMH IT Network Administrator.

G. Reporting and Correction:

1. Serious incidents shall be reported orally to the Security Officer by the MCCMH IT staff when the incident is first identified.

2. Written reports of the incident prepared by MCCMH IT Network Administrator shall include:

   a. Description of the incident;

b. Whether EPHI was compromised;
c. Scope of incident (e.g., number of computers and sites involved, extent of system compromise or damage);
d. Entry point of the incident;
e. Actions taken to control/correct the incident;
f. Further actions which may need to occur to protect the system from future similar attacks.

H. Follow-Up

The MCCMH Security Officer shall:

1. Review all security incidents which result in a formal report from the MCCMH IT Network Administrator.

2. Determine what, if any, additional follow-up activity is necessary, including:

   a. Taking an inventory of the systems' assets;
   b. Including the lessons learned as a result of the security incident in a revised security plan;
   c. Developing a new risk analysis, if necessary;
   d. Commencing an investigation and possible prosecution of the individuals who caused the security incident;
   e. Communicating any matter deemed potentially unlawful to County Corporation Counsel, as necessary; and
   f. Preparing reports, documenting which reports are to be logged, sequentially numbered, and maintained.

3. Prepare reports periodically, but not less frequently than annually, for the Security Committee, Executive Staff and/or Quality Council.

4. Assign responsibility for monitoring corrective actions taken.

5. Ensure that reports to County Corporation Counsel or federal office(s) are made as necessary.

VII. References / Legal Authority

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

B. 45 CFR §164.308(a)(6)

C. 45 CFR §164.400 et seq.

VIII. Exhibits

A. None.