

Chapter: **DIRECTLY-OPERATED PROGRAM MANAGEMENT**
Title: **PROTECTION OF ELECTRONIC CONFIDENTIAL INFORMATION**
Also see MCCMH MCO Policies 10-031, "Expectation of Privacy, Monitoring, Prohibited Content and Use of Electronic and Telephonic Communications;" 10-032, "Acceptable Internet Use;" and 10-033, "Use of All Staff Email Messaging."

Prior Approval Date: 9/9/10
Current Approval Date: 5/22/19

Approved by: BOARD ACTION


Executive Director


Date

I. Abstract

This policy establishes the standards and procedures of the Macomb County Community Mental Health Board (MCCMH) to protect electronic confidential information from unauthorized use / disclosure.

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 electronic confidential information obtained or maintained by MCCMH from unauthorized use or disclosure.

IV. Definitions

A. Confidential Information

1. All information in MCCMH clinical records;
2. Other information concerning MCCMH consumers, providers, quality improvement and peer review records;

3. Personnel records, including records kept by the MCCMH Administrative Office that identify employees, independent contractors, volunteers, and interns to the extent that the records are used or have been used, or may affect or be used relative to the individuals' qualifications for employment, contracting, promotion, transfer, additional compensation or disciplinary action;
 4. Administrative information concerning the MCCMH infrastructure, business relationships, methods, operations, financials, or services of MCCMH not available through the Freedom of Information Act.
- B. Electronic Protected Health Information (EPHI)
Individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. EPHI is defined within HIPAA legislation within paragraphs (1)(i) or (1)(ii) of the definition of protected health information.
- C. Integrity of Database
A process by which information validated within the system must exist for each database.
- D. Workforce Member
Employees, volunteers, trainees, certain independent contractors who work at MCCMH facilities, and other persons whose conduct, in the performance of work for MCCMH, is under the direct control of such MCCMH, whether or not they are paid by MCCMH.

V. Standards

- A. MCCMH employees, independent contractors, volunteers, and interns ("all individuals") shall be accountable for maintaining the protection and integrity of electronic confidential information, which begins with accessing the data and continues with the use of the information.
- B. All electronic and telephonic communications systems and all communication and information transmitted by, received from, or stored in MCCMH systems, including confidential information, are the property of MCCMH and may be audited pursuant to Executive Director or Deputy Director authorization.
- C. MCCMH computer files shall not be disclosed or used for the benefit of any person, corporation, or other entity.
- D. Supervisors shall be responsible for the timeliness, security and integrity of the electronic confidential information maintained within the course and scope of their position through the use of appropriate control measures and the support of MCCMH policies.

- E. Integrity of electronic confidential information copied and transferred from MCCMH to another system shall be the responsibility of the receiving system. Responsibility for the correct transfer and validation of data lies with both systems and the responsible Supervisors.
- F. Unauthorized use or disclosure of electronic confidential information regarding consumers, employees, independent contractors, volunteers, interns, contract providers, quality improvement, peer review records, or the MCCMH infrastructure shall be prohibited. Improper conduct includes, but is not limited to:
 - 1. Unauthorized access to disclosure, dissemination or copying of any information concerning MCCMH consumers, employees, independent contractors, volunteers, interns, providers, quality improvement, peer review records, or the MCCMH infrastructure.
 - 2. Using or attempting to use or obtain another person's user identification (ID) and password or security code, or allowing the use of one's user ID and password or security code by another (other than by MCCMH Information Technology (IT) staff during the normal course of business).
 - 3. Unauthorized modification of confidential information or database structure.
 - 4. Unauthorized access whether internally or from or to a remote location.
 - 5. Unauthorized use or release of MCCMH proprietary information.
- G. Inappropriate access to, modification, destruction or disclosure of electronic confidential information in any format is prohibited. These formats include but are not limited to the following:
 - 1. Personal computers
 - 2. Electronic or voice mail
 - 3. Fax machines
 - 4. Internet / Intranet
 - 5. Other electronic or printed media
- H. Electronic mail used for authorized disclosures of protected health information originating from MCCMH directly-operated providers to other agencies (i.e. to MCCMH contracted network providers) shall be encrypted through the use of an encryption engine (e.g. Zix) as of November 1, 2010, that shall automatically scan for information that may qualify as electronic protected health information. Email content that triggers a match to the rules of the encryption engine will be encrypted prior to delivery.

1. The subject line of an email, which cannot be encrypted, shall not contain any individually identifiable health information. Examples of prohibited items in the subject line are names, client identification numbers, and social security numbers.
 2. The secure encryption engine (Zix) may be manually triggered by inclusion of the word “secure” in the subject line.
 3. The secure encryption engine may be manually disabled where the email content may trigger the encryption engine, but does not contain protected health information, by inclusion of the word “noencrypt” in the subject line.
 4. The MCCMH IT Department shall support and modify the rules of the Zix encryption engine and make reasonable attempts to avoid encryption of “false positives” (information which met a rule, but upon examination, did not require encryption).
 5. The MCCMH IT Department shall provide usage materials and user support relating to the encryption of email.
- I. Access to and the release of specific sensitive information (including but not limited to clinical records, drug or alcohol abuse, quality improvement, peer review records, AIDS/ARC/HIV) shall be governed by MCCMH MCO Policy 6-001, “Release of Confidential Information - General,” MCCMH MCO Policy 6-002, “Release of Confidential Information - Alcohol and Drug Abuse,” MCCMH MCO Policy 10-325, “Minimum Necessary HIPAA Privacy,” MCCMH MCO 3-016, “FOCUS Access Management – Contract Network Providers,” MCCMH MCO 10-442, “FOCUS Access Management,” MCCMH MCO 10-440, “Access Control,” and MCCMH MCO 10-410, “Security Overview.”
 - J. Internal or external dissemination of consumer identifiers, consumer data and data concerning the MCCMH infrastructure shall be evaluated against the consumer’s business requirements and the need to know that information and be approved by the owner of the data.
 - K. Access or use of confidential information for other than job requirements is a serious offense that may result in disciplinary action up to and including termination of employment or contract.
 - L. Every MCCMH employee, independent contractor, volunteer, intern, and other Workforce Member will be required to read, sign and adhere to the MCCMH Workforce Confidentiality Agreement as a condition of their continued employment/affiliation with MCCMH.

VI. Procedures

A. ID/Password

1. MCCMH IT staff shall assign security levels and authorize unique identification and password assignments to staff members and other authorized individuals for access to clinical and/or other confidential information on a “need to know” basis only. “Need to know” is determined by the individual’s Supervisor and will be consistent with this policy.
2. Users of electronic media containing confidential information shall possess individual IDs/passwords.
3. An individual’s multiple attempts to sign-on with an improper access code may result in a “lock out” status of the individual until his/her accessibility to the system is restored by IT staff.
4. Supervisors shall notify the IT staff when access assignments need to be changed due to an individual’s change in status (i.e., terminations, change of job positions).
5. Intentional release of a password or willful failure to change a compromised password may result in disciplinary action up to and including termination of employment or contract.

B. Other Methods of Accessing Computer Systems

1. If another method of accessing a computer system is used, such as an ID badge or swipe card, use of the ID badge or swipe card shall be restricted to the identified individual.

C. Administration and Maintenance

1. MCCMH IT may monitor and log access to the various centrally located electronic based systems within MCCMH.
2. If misuse is suspected or detected, the Supervisor, Program Manager, Division Director shall be notified. Misuse shall be reported to the MCCMH Executive Director and Deputy Director who shall determine the need for proper investigation.
3. Program Supervisors shall establish inclusions in their Program Manuals pertaining to security and maintenance of electronic confidential information at their service sites.
4. Confidentiality Agreements:
 - i. Program Supervisors & Division Directors shall ensure that each new Workforce Member after June 1, 2019, signs a MCCMH Workforce

Confidentiality Agreement (Exhibit A) prior to commencing work for or on behalf of MCCMH.

- ii. Existing Workforce Members as of June 1, 2019, will be required to sign a MCCMH Workforce Confidentiality Agreement (Exhibit A) coincident with their next annual HIPAA refresher training. Program Supervisors & Division Directors shall be responsible to ensure that every Workforce Member reporting to them signs a Confidentiality Agreement prior to June 1, 2020.
- iii. The original signed agreement should remain in the Workforce Member's personnel file, and a copy should be provided to the Workforce Member for their records.

VII. References / Legal Authority

- A. Macomb County Personnel Manual (October 15, 2009), "Computer Usage, E-Mail and Internet Policy," 4.4, and "Confidential Information," 4.9
- B. Commission on Accreditation of Rehabilitation Facilities (CARF) 2010 Standards Manual, § 1.F., "Legal Requirements," 1, 3, 4, pp 53-54; 1.K., "Rights of the Persons Served," 2, p 84
- C. MCCMH MCO Policy 6-001, "Release of Confidential Information - General"
- D. MCCMH MCO Policy 6-002, "Release of Confidential Information - Alcohol and Drug Abuse"
- E. MCCMH MCO Policy 6-004, "Facsimile Document Transmission"

VIII. Exhibits

- A. MCCMH Workforce Confidentiality Agreement.