MCCMH MCO Policy 10-460

(was Administrative Policy 9-10-110)

Chapter: **DIRECTLY-OPERATED PROGRAM MANAGEMENT**
Title: **PASSWORD MANAGEMENT**

Prior Approval Date: 9/09/10
Current Approval Date: 5/22/19

Approved by: BOARD ACTION

Executive Director — Date 5/22/19

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) to ensure that passwords are created and used by the MCCMH workforce to access any network, system, or application used to view, transmit, receive, or store electronic protected health information (EPHI).

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 password management be strictly implemented to prevent the significant security threat of unauthorized access to its computer systems and exploitation of potential security vulnerabilities elsewhere in the systems.

IV. Definitions

A. FOCUS: The electronic medical record system and billing platform utilized by MCCMH.

B. MCCMH Systems: The MCCMH computer network and all systems and programs in which PHI is created, modified, stored, transmitted or maintained by or on behalf of MCCMH.

C. Password: Confidential authentication information composed of a string of characters / a personal identifier

V. Standards

A. MCCMH shall have a password management system for its workforce.

B. MCCMH shall provide training to its workforce in password management security.

C. MCCMH Administration and Management Staff shall ensure that all staff accessing MCCMH EPHI comply with the procedures contained in this policy.

VI. Procedures

A. The MCCMH password management system shall include the following emphases:

1. Rules to be followed in creating and changing passwords, including password adequacy (e.g., length, complexity) and frequency considerations, including:

    a. For MCCMH Systems other than FOCUS:

        i. Passwords shall be at least ten (10) characters long.

        ii. Passwords must contain a minimum of three (3) of the following four (4) options: (i) upper case letter, (ii) lower case letter, (iii) number, and/or (iv) symbol.

        iii. Users are required to change their password every ninety (90) days. The MCCMH Information Technology (IT) staff shall periodically send reminders to do so.

    b. For FOCUS, those rules for creating and changing passwords that are built into the application by the developer. At minimum, Users will be required to create passwords containing at least eight (8) non-blank characters including letters and numbers, and change their FOCUS password every ninety (90) days.

2. The importance of keeping passwords confidential and include storage considerations to ensure protection.

3. Authorization and/or supervision of the MCCMH workforce who work with EPHI or in locations where it might be accessed.

B. The MCCMH password management security training shall include the following:

1. Emphasis on adhering first to all published policies and procedures; and

2. Emphasis on the practice of verifying an official's identity, position and/or authority prior to taking direction from that person with respect to security measures.

C. All MCCMH workforce shall use the same set of software applications as defined by the MCCMH IT unit.

D. Upon notification of hire or termination of staff from the Office of the MCCMH Deputy Director, the MCCMH IT unit shall create passwords for new workforce members and nullify the passwords of terminated workforce members.

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)(ii)(D)

VIII. Exhibits

A. None.