MCCMH MCO Policy 3-016

Chapter: **PROVIDER NETWORK MANAGEMENT**
Title: **FOCUS ACCESS MANAGEMENT – CONTRACT NETWORK PROVIDERS**

Prior Approval Date: N/A
Current Approval Date: 10/25/2017

Approved by: BOARD ACTION

Executive Director — Date 10/25/17

I. Abstract

This policy establishes the standards and procedures of the Macomb County Community Mental Health (MCCMH) Board for compliance with the Security Rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) by ensuring that only appropriate access to EPHI via FOCUS is granted to its Contract Network Providers and their Workforce Members, limited to that which is minimally necessary in light of the relevant individual's role and responsibilities.

II. Application

This policy shall apply to all Contract Network Providers of the MCCMH Board.

III. Policy

It is the policy of the MCCMH Board to minimize the potential for unauthorized access to EPHI via FOCUS by (i) ensuring that Contract Network Providers and their Workforce Members are granted access to FOCUS only as minimally necessary for the performance of their role and responsibilities, (ii) establishing procedures for granting, modifying, and terminating access to FOCUS, (iii) establishing standard procedures for resetting FOCUS passwords, and (iv) providing for the routine review of FOCUS access, privileges, and use.

IV. Definitions

A. Appropriate Access: Access to read, write, modify, or communicate EPHI via FOCUS, in the amount minimally necessary in light of an individual's role within the organization, and consistent with the applicable job description and Security Profile.

B. Authorized Requester: Appropriate supervisory staff designated by the Contract Network Provider to request FOCUS access for subordinate Workforce Members.

C. Business Associate: Any entity which:
   a. Performs a function or activity on behalf of a Contract Network Provider 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 Contract Network Provider;
   b. Is NOT involved in the treatment of consumers; and
   c. Is NOT providing consumer-conducted financial transactions.

D. Contract Network Providers: Healthcare professionals, entities, and facilities that have contracted with the MCCMH Board to provide services to MCCMH consumers.

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

F. FOCUS Access Authorization Form: The form to be completed by the appropriate Authorized Requestor to initiate each request for new or modified access to FOCUS.

G. FOCUS Access Point of Contact: MCCMH employee from the Division of Business Management who has been designated by that Division to process all requests for access to FOCUS.

H. EPHI: 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 PHI. MCCMH EPHI is primarily stored in FOCUS.

I. Permissions: The set of rights and restrictions to access PHI within FOCUS.

J. Permissions Workgroup: An internal MCCMH committee chaired by the Corporate Compliance Officer or designee comprised the (1) the Deputy Director, (2) the FOCUS Access Point of Contact, (3) a representative from the Office of Corporate Compliance, (4) a representative from Information Systems, (5) a representative from the relevant Contract Network Provider, as necessary. The

Permissions Workgroup is tasked with developing appropriate Security Profiles for Users by relying on the User's job description to define Appropriate Access.

K. Permissions Workgroup Proxy: An individual authorized in writing by the Permissions Workgroup to make urgent and/or time-sensitive Security Profile changes, upon receiving written approval from the Compliance Officer and Information Systems Manager, in order to facilitate a similarly urgent and/or time-sensitive FOCUS Access Authorization Form request.

L. PHI: For purposes of this policy, Protected Health Information, as defined by 45 CFR § 160.103, excluding substance use disorder information.

M. Security Profile: The Permissions which are associated with the job description of a User. Security Profiles are developed by the Permissions Workgroup by relying on the User's job description to define Appropriate Access.

N. User: Contract Network Provider Workforce Member with authorized access.

O. Workforce Member: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the Contract Network Provider, is under the direct control of the Contract Network Provider, including but not limited to, network provider employees, independent contractors, and volunteers.

V. Standards

A. Access to protected health information which would identify an individual served as having a substance use disorder is governed by 42 CFR Part 2, and not addressed in this policy as access is granted by the MCCMH Office of Substance Abuse.

B. The Division of Business Management shall designate a member of its staff as the FOCUS Access Point of Contact, and shall make up-to-date contact information for such individual easily accessible to all Contract Network Providers.

C. The Permissions Workgroup shall develop and document Security Profiles for all Contract Network Provider Users.

D. Neither Security Profiles nor the Permissions associated with a Security Profile or individual User's access shall be modified without review and approval by the Permissions Workgroup. Urgent and/or time-sensitive Security Profile or Permissions modifications may be made by a Permissions Workgroup Proxy, upon receipt of written approval from the Compliance Officer and Information Systems Manager, and must be ratified and documented by the Permissions Workgroup as soon as possible thereafter.

i. Documentation confirming the approval of any Security Profile modification must be forwarded to the Compliance Officer and FOCUS Access Point of Contact for their records.

ii. Documentation confirming that changes to Permissions have been effectuated must be forwarded by the Information Systems Manager to the Compliance Officer, the FOCUS Access Point of Contact, the Authorized Requester, and the relevant User.

E. The Permissions Workgroup will meet on a monthly basis in order to carry out its business, including but not limited to: (i) developing and documenting initial job classification Security Profiles; (ii) reviewing/auditing job classification and/or individual Security Profiles to ensure that they remain appropriate; (iii) ratifying and approving urgent or time-sensitive Security Profile modification approved by the Permissions Workgroup Proxy since the last monthly meeting; (iv) analyzing any then pending requests for individual Security Profile modifications that are inconsistent with the applicable job description; and (iii) updating job classification and/or individual Security Profiles, as necessary.

F. Contract Network Providers shall ensure that an up-to-date job description is maintained by the Contract Network Provider for each and every position filled or open within such Contract Network Provider, and ensure that copies of all job descriptions are available upon request by the FOCUS Access Point of Contact.

G. Authorized Requestors shall request access to FOCUS for subordinates consistent with the relevant job description, or otherwise in compliance with this policy. Requests for FOCUS access must be made using the FOCUS Access Authorization Form, which will require the Authorized Requestor to make certain attestations as to the accuracy and completeness of the information provided.

H. The Division of Business Management shall develop and implement procedures to ensure that the FOCUS Access Point of Contact grants access to FOCUS in compliance with this policy.

I. The Division of Business Management will maintain written records of all Contract Network Provider Workforce Members granted access to FOCUS.

J. Contract Network Providers and their Workforce Members will be required to utilize a standard procedure for requesting FOCUS access password resets, which require that all requests be submitted by the owner of the account in writing to the FOCUS Access Point of Contact.

K. Business Associates and other appropriate non-provider third-party entities requested by Contract Network Providers (e.g., third party payors, external auditors) will be granted access to FOCUS only to the extent such access is HIPAA compliant (e.g., minimally necessary), only upon approval from the Compliance Officer, and only if such entity produces valid documentation proving necessity and HIPAA compliance to the satisfaction of the Compliance Officer.

i. In the case of a Business Associate, required documentation will include: (i) a valid Business Associate Agreement between the Business Associate and the Contract Network Provider; (ii) a valid contract, statement of work, or other like document that outlines the purpose for which FOCUS access is necessary for the Business Associate; and (iii) any other documentation requested by the Compliance Officer.

ii. In the case of any other third-party (non-MCCMH, non-Contract Network Provider, non-provider) entity seeking access to FOCUS, required documentation will include: (i) a valid contract, statement of work, or other like document that outlines the purpose for which FOCUS access is necessary; and (iii) any other documentation requested by the Compliance Officer.

L. FOCUS access authorizations/decisions may take up to 2-weeks to process.

M. The Office of Corporate Compliance will resolve any conflicts or discrepancies regarding Appropriate Access.

N. The Office of Corporate Compliance will systematically and regularly audit a random sampling of Contract Network Provider FOCUS access in order to ensure consistency with the standards defined herein.

O. Violation of this policy may be interpreted as a violation of MCCMH privacy and/or confidentiality standards, and/or a violation of the Contract Network Provider's contract with MCCMH, and may therefore result in an investigation by the MCCMH Office of Corporate Compliance and subsequent corrective action.

VI. Procedures

A. Authorized Requestors:

1. Contract Network Providers will designate in writing which supervisory staff members are Authorized Requesters. Written designations of Authorized Requesters (or revocation of "Authorized Requestor" status) shall be provided to the FOCUS Access Point of Contact, who shall maintain an up-to-date list of all Contract Network Provider Authorized Requestors based such written designations.

2. Requests from individuals not on the most current "Authorized Requester" list maintained by the FOCUS Access Point of Contact will not be processed.

   Timing of Access Requests: Access requests should be submitted according to the New Access or Change Request Process procedures immediately after identifying a need for FOCUS access, or after identifying any inaccurate or outdated job description or access level. In all cases the

Authorized Requester must certify that Credentialing is complete prior to submitting the request for FOCUS access.

B. New Access or Change Request Process:

1. Authorized Requesters should complete a FOCUS Access Authorization Form and forward it to FOCUS Access Point of Contact, at FOCUSAccessRequest@mccmh.net, for processing.

2. The FOCUS Access Point of Contact will review the FOCUS Access Authorization Form for completeness and consistency with MCCMH policy, consulting with the Office of Corporate Compliance as necessary.

3. Requests that are incomplete or inconsistent with MCCMH policy will not be processed, and the FOCUS Access Point of Contact will notify the Authorized Requestor of the request's deficiency via email, as soon as possible.

4. After processing an approved FOCUS Access Authorization Form, the FOCUS Access Point of Contact will notify the Authorized Requester that FOCUS Access has been authorized, and that the Authorized Requestor is required to provide login credentials and instructions to the relevant Workforce Member.

5. The FOCUS Access Point of Contact will maintain a record of all requests made under this section, as well as the disposition of such request (i.e., approved & processed, or denied and advised of deficiencies).

C. Job Description Annual Audit. Contract Network Providers must complete an annual audit of each job description within their agency in order to (i) verify that it is up-to-date, and (2) that each of its Workforce Members have Appropriate Access in light of actual circumstance.

1. Full results of the Job Description Annual Audit must be maintained by the Contract Network Provider and be made available to MCCMH upon request.

2. In all cases where the audit results indicate that a modification to the job description is required, the Contract Network Provider will ensure that the job description is so modified in accordance with its own internal policies and procedures.

3. In all cases where the audit results indicate that modifications to FOCUS access are required, the appropriate Authorized Requester should complete a FOCUS Access Authorization Form and route according to the "New Access or Change Request Process," above.

D. Internal Transfer: If a Contract Network Provider Workforce Member internally transfers to another division within the Contract Network Provider, or another practice site:

1. The Authorized Requestor for the division or site to which the Workforce Member is transferring is responsible for completing a FOCUS Access Authorization Form according to New Access or Change Request Process defined, above; and

2. The Authorized Requester for the Division from which the MCCMH Staff transferred is responsible to follow the FOCUS Access Termination Procedures in order to ensure that the Workforce Member's FOCUS access is appropriately terminated as of the date of the transfer.

3. In the event that Contract Network Provider believes that the transferred Workforce Member requires access to the FOCUS records of the division or site from which the individual transferred after the FOCUS Access Termination Procedures have already been completed (e.g., to complete information required for State reporting obligations), the Authorized Requestor for such division or site shall forward such request to the MCCMH Compliance Officer, and include a specific duration and detailed justification for the access requested.

    i. The Compliance Officer will evaluate the request to ensure compliance with MCCMH policy, as well as with applicable law.

    ii. If the request is denied, the Compliance Officer will notify the Authorized Requestor of such denial and the reasons supporting it as soon as possible, and forward a copy of the request and the documented denial to the FOCUS Access Point of Contact for their records.

    iii. If the request is approved, the Compliance Officer will (i) forward a copy of the request to the FOCUS Access Point of Contact for processing.

4. After fully processing an approved FOCUS Access Authorization Form, the FOCUS Access Point of Contact must notify the Authorized Requester that FOCUS access has been authorized, and that the Authorized Requestor is required to provide login credentials and instructions to the MCCMH Staff.

5. The FOCUS Access Point of Contact will maintain a record of all requests made under this section, as well as the disposition of such request (i.e., approved & processed, or denied and advised of deficiencies)

E. Password Reset and Account Reactivation Requests:

1. Password Reset: Any Workforce Member requiring a reset of their FOCUS password must submit their request in writing to the FOCUS Access Point of Contact.

    i. Password reset requests must be sent by the owner of the account (the Workforce Member) via email to FOCUSAccessRequest@mccmh.net, with "**PASSWORD RESET REQUEST**" in the subject line.

    ii. The body of the email should include (1) the full name of the Workforce Member requiring a password reset, (2) the name of the Contract Network Provider agency (3) the reason for the password reset, and (4) the name of the Workforce Member's direct supervisor and clinical supervisor (if applicable).

    iii. The FOCUS Access Point of Contact will notify the requester upon completion of the password reset.

    iv. The FOCUS Access Point of Contact will maintain a record of all requests made under this section, as well as the disposition of such request (i.e., approved & processed, or denied and advised of deficiencies).

2. Account Reactivation: In the event that a Workforce Member's FOCUS account is deactivated due to inactivity or any other reason:

    i. The appropriate Authorized Requester must send a request to reactivate the FOCUS account via email to FOCUSAccessRequest@mccmh.net, with "**ACCOUNT REACTIVATION REQUEST**" in the subject line.

    ii. The body of the email should include (1) the full name of the Workforce Member requiring an account reactivation, (2) the name of the Contract Network Provider agency, (3) the reason for the account deactivation, (4) the reason for the account reactivation, and (5) the name of the individual's direct supervisor and clinical supervisor (if applicable).

    iii. The FOCUS Access Point of Contact will notify the requester upon reactivation of the account.

    iv. The FOCUS Access Point of Contact will maintain a record of all requests made under this section, as well as the disposition of such request (i.e., approved & processed, or denied and advised of deficiencies)

F. FOCUS Access Termination Procedures: In any event where it is appropriate to terminate a User's FOCUS access (e.g., termination of employment, temporary leave, change in duties, transfer to another department or division, license status change, etc.) the appropriate Authorized Requester must immediately:

1. Complete a FOCUS Access Authorization Form, indicating that the request is for "Dis-enrollment;" and

2. Email the FOCUS Access Authorization form to the FOCUS Access Point of Contact at FOCUSAccessRequest@mccmh.net, with the words "**DISENROLLMENT REQUEST**" in the subject line

G. Business Associates / Non-Provider Third Parties: In the event that any Business Associate or other non-provider third-party entity requests access to FOCUS as a result of its relationship with a Contract Network Provider, such request should be routed to the Compliance Officer, with all required supporting documentation:

1. In the case of a Business Associate, required documentation will include: (i) a valid Business Associate Agreement between the Business Associate and the Contract Network Provider; (ii) a valid contract, statement of work, or other like document that outlines the purpose for which FOCUS access is necessary for the Business Associate; and (iii) any other documentation requested by the Compliance Officer.

2. In the case of any other third-party (non-MCCMH, non-Contract Network Provider, non-provider) entity seeking access to FOCUS, required documentation will include: (i) a valid contract, statement of work, or other like document that outlines the purpose for which FOCUS access is necessary; and (iii) any other documentation requested by the Compliance Officer.

The Compliance Officer will notify the requester and the FOCUS Access Point of Contact of whether the access request has been approved or denied to move forward. If the request is approved to move forward, the FOCUS Access Point of Contact will coordinate with the relevant Contract Network Provider to secure FOCUS Access Authorization Forms for each individual that has been approved by the Compliance Officer to access FOCUS.

H. Access Audits: The Office of Corporate Compliance will complete Periodic Random Access Audits in order to ensure that User access to EPHI through FOCUS is consistent MCCMH policy and applicable law.

1. The Office of Corporate Compliance shall randomly select a sample of Users on a quarterly basis, which shall be representative of fifteen percent (15%) of the total Users, and cross-check records of the sample's EPHI access via FOCUS against their job descriptions and Security Profiles.

2. Contract Network Providers and Workforce Members shall cooperate with the Office of Corporate Compliance to facilitate the audit and any investigation or remediation thereafter required.

3. The Office of Corporate Compliance shall report the cumulative annual results of the Periodic Random Access Audits to the MCCMH Board as part of its Annual Report of Compliance Activities.

VII. References / Legal Authority

A. Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104-191
B. 45 CFR § 160.103
C. 45 CFR §§164.308(a)(3)
D. MCL 330.1748
E. MCCMH MCO Policy 10-030, “Protection of Electronic Confidential Information”
F. MCCMH MCO Policy 10-325, “Minimum Necessary”
G. MCCMH MCO Policy 10-410, “Security Overview”
H. MCCMH MCO Policy 10-440, “Access Control”

VIII. Exhibits

A. FOCUS Access Authorization Form