MCCMH MCO Policy 10-442

Chapter: **DIRECTLY-OPERATED PROGRAM MANAGEMENT**
Title: **FOCUS ACCESS MANAGEMENT**

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 MCCMH Staff, limited to that which is minimally necessary in light of an individual's role within the organization.

II. Application

This policy shall apply to all MCCMH administrative and management staff and MCCMH Workforce Members (collectively, "MCCMH Staff").

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 MCCMH Staff are granted access to FOCUS only as minimally necessary for the performance of their role within the organization, (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: Division Directors or other appropriate supervisory staff that have been designated by the MCCMH Deputy Director, or authorized designee, to request FOCUS access for subordinate MCCMH Staff. Unless otherwise designated in writing by the MCCMH Deputy Director according to the standards and procedures described in this policy, the following guidelines will generally apply:

   a. When access is requested for **non-clinical staff**, the "appropriate supervisory staff" will be the staff's direct supervisor.

   b. When access is requested for **non-physician, non-nurse clinical staff**, the "appropriate supervisory staff" will be the clinical supervisor of the individual for whom access is requested.

   c. When access is requested for a **physician or nurse**, access must be requested by both (1) the clinical supervisor, and (2) the administrative supervisor; the FOCUS Access Authorization Form will not be deemed to meet the "Authorized Requestor" requirement unless both signatures are present.

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

D. Credentialing: The requirements and processes described in MCCMH MCO Policy No. 10-070, Credentialing and Re-Credentialing.

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 Division, with direct knowledge of the Security Profile privileges required, and (6) other Divisions are necessary. The Permissions Workgroup is tasked with developing appropriate Security Profiles for every job classification within MCCMH, as well as for any individual job description that requires a non-standard Security Profile.

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 an individual MCCMH Staff member's job description. Security Profiles are developed by the Permissions Workgroup, are specifically defined in each job description, and defines Appropriate Access for each MCCMH position.

N. User: MCCMH Staff with authorized access.

O. Workforce Member: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for MCCMH, is under the direct control of MCCMH, including but not limited to, administrative and directly-operated 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 MCCMH Staff.

C. The Permissions Workgroup shall develop and document Security Profiles for all MCCMH standard job classifications, as well as for any non-standard job descriptions (on an individual basis), as necessary. Documented Security Profiles must be provided to the applicable Division Director, and must include a "Last Reviewed" date, which can be verified by the Permissions Workgroup upon the request of the Deputy Director, the Office of Corporate Compliance, the Focus Access Point of Contact, or any other appropriate staff.

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 by the Authorized Requester to the MCCMH Chief of Staff to attach to the relevant job description, and 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. MCCMH Division Directors shall ensure that an up-to-date job description, including an up-to-date Security Profile, is on file within the Division for each and every position filled or open within such Division, and ensure that copies of all job descriptions are provided to the MCCMH Chief of Staff.

G. The MCCMH Chief of Staff shall maintain a repository of the job descriptions for every job title within MCCMH, including the associated Security Profiles, as well as a record of each individual MCCMH Staff who has had a Security Profile modification approved by the Permissions Workgroup, or a Non-Routine Access Request approved by the Deputy Director and Office of Corporate Compliance. The MCCMH Chief of Staff shall develop and implement procedures for ensuring that the FOCUS Access Point of Contact has access this data repository.

H. Authorized Requestors shall request access to FOCUS for subordinates strictly in compliance with the relevant job description and Security Profile. 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.

I. In each case that a FOCUS Access Authorization Form is submitted, approved and processed, the Authorized Requestor will be required to provide the applicable User with a copy of the up-to-date version of their Security Profile.

J. Division Directors and supervisory staff and shall ensure that each subordinate maintains access to EPHI strictly in compliance with their Security Profile, and that each subordinate is supervised to ensure that unauthorized access to EPHI is avoided.

K. 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.

L. FOCUS Access Authorization Forms will not be processed until the Authorized Requester informs the FOCUS Access Point of Contact that the subject-employee has received final or temporary/provisional Credentialing approval, after which point FOCUS access authorizations/decisions may take up to 2-weeks to process.

M. The Division of Business Management will maintain written records of all individuals granted access to FOCUS, and of all Security Profile modifications requested and/or completed.

N. MCCMH Staff will be required to utilize a standard procedure for requesting FOCUS access password resets, which require that all requests be submitted in writing by the owner of the account to the FOCUS Access Point of Contact.

O. Business Associates and other appropriate non-provider third-party (non-MCCMH, non-contract provider) entities (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 MCCMH;
(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-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.

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

Q. The Office of Corporate Compliance will systematically and regularly audit a random sampling of MCCMH Staff FOCUS access in order to ensure consistency with the standards defined herein.

R. Any violation of Standards V.H, J., L., O., or R., above, shall be interpreted as a violation of MCCMH privacy and confidentiality standards and policies, and may result in disciplinary action, up to and including the discharge, of the responsible MCCMH Staff.

VI. Procedures

A. Authorized Requestors: The MCCMH Deputy Director, or "authorized designee," will designate in writing which Division Directors or supervisory staff members are Authorized Requesters. No Division Director or supervisory staff member (except the MCCMH Executive Director) may request or authorize access for her/himself.

1. Notice of MCCMH Deputy Director's "authorized designee," as indicated above, shall be provided in writing by the MCCMH Deputy Director to the Chief of Staff, the Office of Corporate Compliance and the Division of Business Management.

2. Written designations of Authorized Requesters (or revocation of "Authorized Requestor" status) shall be provided to the Division of Business Management.

3. An up-to-date list of all Authorized Requestors, based on written designations received from the MCCMH Deputy Director or authorized designee, shall be maintained by the Division of Business Management and made easily accessible by the FOCUS Access Point of Contact, the Office of Corporate Compliance, and the Chief of Staff.

4. FOCUS access requests from individuals not on the most current "Authorized Requester" list maintained by the Division of Business Management will not be processed.

B. Timing of Access Requests: Access requests should be submitted according to either the "Routine Access Request" or "Non-Routine Access Request" procedures described below:

1. Upon an employee's initial Credentialing request, concurrently with submission of the request for Credentialing and supporting paperwork.

2. Upon any request for modified Credentialing or Re-Credentialing, concurrently with submission of the request for modified Credentialing or Re-Credentialing and supporting paperwork.

3. Upon final or temporary/provisional approval of the employee's Credentialing, the Authorized Requester is required to send an email to the Focus Access Point of Contact notifying of such, with "**[Requested FOCUS User's Name] – C&P Complete**" in the subject line.

4. In any case where new or revised Credentialing is not a factor motivating the need for new or revised FOCUS access, the FOCUS access request should be made immediately after identifying a need for FOCUS access, or after identifying any inaccurate or outdated job description, Security Profile, or required access.

C. Routine Access Requests: FOCUS access requests that are consistent with the applicable job description and Security Profile:

1. Authorized Requester 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 access request 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 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. After receiving notice of an approved and processed FOCUS Access Authorization Form, the Authorized Requester must also provide the relevant User with a copy of the up-to-date version of their Security Profile.

6. 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).

D. Non-Routine Access Requests: FOCUS access requests that are inconsistent with the applicable job description and Security Profile (e.g., requesting a greater level of FOCUS access than the Security Profile allows, including but not limited to any case before the Information Systems Manager adds or revises permissions), where neither final nor temporary/provisional Credentialing approval has been obtained:

1. Authorized Requester should complete a FOCUS Access Authorization Form and submit it to both the Deputy Director and the Office of Corporate Compliance, along with a detailed justification for the non-routine request.

2. The Deputy Director and the Office of Corporate Compliance shall each evaluate the Non-Routine Access Request to ensure compliance with MCCMH policy, as well as with applicable law.

3. If the request is denied, the Office of Corporate Compliance 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 files.

4. If approval is obtained, the Office of Corporate Compliance will (i) forward a copy of the request to the FOCUS Access Point of Contact for processing, and (ii) forward a copy of the request to the Permissions Workgroup or Permissions Workgroup Proxy, for non-standard Security Profile revisions, as appropriate.

5. 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.

6. After receiving notice of an approved and processed FOCUS Access Authorization Form, the Authorized Requester must also provide the relevant User with a copy of the up-to-date version of their Security Profile

7. 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. Job Description/Security Profile Annual Audit. Division Directors shall be responsible for completing an annual audit of each subordinate job description filled and/or open within their Division in order to (i) verify that it is up-to-date, and (2) that the associated Security Profile defines Appropriate Access in light of actual circumstance, referencing the Table in MCCMH MCO Policy 10-450, EPHI Security, Exhibit A and consulting the Office of Corporate Compliance, as appropriate.

1. In order to facilitate the audit, the Information Systems representative on the Permissions Workgroup, on behalf of the Permissions Workgroup, will provide Division Directors with a copy of the most up-to-date Security Profiles documented by the Permissions Workgroup for staff in their Division.

2. Full results of the Job Description/Security Profile Annual Audit must be submitted to the MCCMH Chief of Staff, by no later than September 1st of each year.

3. "Full results" shall require that each subordinate job description within the Division:

    i. Either be labelled (i) "Appropriate Job Description", or (2) "Job Description Modifications Required," with specific justification and instructions for such modifications included; **AND**

    ii. Either be labelled (i) "Appropriate Security Profile", or (2) "Security Profile Modifications Required," with specific justification and instructions for such modifications included.

4. In all cases where the audit results indicate that a modification to the job description is required, the MCCMH Chief of Staff will coordinate with the Division Director, Information Systems representative, and the Office of Corporate Compliance, as necessary, to update the job descriptions.

5. In all cases where the audit results indicate that modifications to the Security Profile are required, the MCCMH Chief of Staff will coordinate to ensure that the Division Director submits a request for modification to the Security Profile to the Permissions Workgroup or Permissions Workgroup Proxy.

6. 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 proceed according to

the "Routine Access Request" or "Non-Routine Access Request" procedures, as appropriate.

F. Internal Transfer of Employee Procedures: If MCCMH Staff transfers to another division within MCCMH

1. The Authorized Requestor for the Division to which the MCCMH Staff is transferring is responsible for completing a FOCUS Access Authorization Form according to the "Routine Access Request" or "Non-Routine Access Request" procedures 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 MCCMH Staff's FOCUS access is appropriately terminated as of the date of the transfer.

3. In the event that the transferred employee requires access to the FOCUS records of the Division from which the MCCMH Staff 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 shall request access for the MCCMH Staff and proceed according to the "Non-Routine Access Request" procedures defined above, and include a specific duration and detailed justification for the access requested.

4. 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)

G. FOCUS Password Resets & Account Reactivations:

1. Password Resets: Any MCCMH Staff 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 FOCUS account 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 individual requiring a password reset, (2) the reason for the password reset, and (3) 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 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 Reactivations: In the event that an MCCMH Staff'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 individual requiring an account reactivation, (2) the reason for the account deactivation, (3) the reason for the account reactivation, and (4) 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)

H. 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; and

   3. 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)

I. Business Associates / Non-Provider Third-Parties: In the event that any Business Associate or other non-provider third-party entity requests access to FOCUS, 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 MCCMH; (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-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 requesting entity to secure FOCUS Access Authorization Forms for each individual that has been approved by the Compliance Officer to access FOCUS.

J. 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 with applicable job descriptions, Security Profiles, and authorizations.

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. MCCMH Staff, including but not limited to Division Directors and supervisory staff, the Chief of Staff, the MCCMH Chief of Staff, the Division of Business Management, and the FOCUS Access Point of Contact, shall all 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”
G. MCCMH MCO Policy 10-440, “Access Control”
I. MCCMH MCO Policy 10-450, “EPHI Security”

VIII. Exhibits

A. FOCUS Access Authorization Form