MCCMH MCO Policy 10-370

Chapter: **DIRECTLY-OPERATED PROGRAM MANAGEMENT**
Title: **HIPAA PRIVACY BREACH ASSESSMENT AND NOTIFICATION**

Prior Approval Date: N/A
Current Approval Date: 3/27/19

Approved by: BOARD ACTION

Executive Director — Date: 3-27-19

I. Abstract

This policy defines the standards of the Macomb County Community Mental Health (MCCMH) Board (the "Board") for compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Final Rule requirements with respect to the investigation of breaches of Protected Health Information (PHI) and subsequent breach notification.

II. Application

This policy shall apply to the MCCMH Board, as well as all MCCMH Workforce Members (including but not limited to all directly-operated providers) and Business Associates.

III. Policy

It is the policy of the MCCMH Board to comply with 45 CFR 164.404 – 164.414, including but not limited to all requirements regarding breach notification.

IV. Definitions

A. Breach: The acquisition, access, use, or disclosure of PHI in a manner that compromises the security or privacy of the PHI.

B. Business Associate: A person or entity that performs certain services, functions, or activities that involve the use or disclosure of PHI on behalf of MCCMH as a HIPAA "covered entity". MCCMH Workforce Members are not "business associates".

Business associate functions and activities may include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business associate services may include: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

C. Covered Entity: (1) a health plan; (2) a health care clearinghouse; or (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA/HITECH regulations.

D. Protected Health Information (PHI): Clinical records and other information, including demographic information or the fact that an individual is a MCCMH patient, collected from a patient in any form, and held or disclosed by MCCMH, whether communicated electronically, on paper, orally or any other means that: (i) relates to the past, present, or future physical or mental health or condition of a patient, the provision of health care to a patient, or the past, present, or future payment for the provision of health care to a patient; and (ii) identifies or provides a reasonable basis for the belief that the information can be used to identify a patient.

E. Unsecured PHI: Unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(2) of Public Law 111-5.

F. 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. Breach Risk Assessment: Any unauthorized acquisition, access, use or disclosure of PHI will be presumed to be a Breach unless MCCMH can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the protected health information or to whom the disclosure was made;

3. Whether the protected health information was actually acquired or viewed; and

4. The extent to which the risk to the protected health information has been mitigated.

5. Exclusions: The following will not be deemed a Breach of PHI (See 45 CFR 164.402):

i. Any unintentional acquisition, access, or use of PHI, if done in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by HIPAA/HITECH.

ii. Any inadvertent disclosure by a person who is authorized to access PHI to another person authorized to access PHI, where the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA/HITECH.

iii. A disclosure of PHI where MCCMH has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

NOTE: The Compliance Officer and Corporate Counsel are the only individuals who may determine if one of these exceptions applies to any disclosure of PHI. Any such determination must be thoroughly documented.

B. A Breach will be treated as discovered as of the first day on which the Breach is known, or by exercising reasonable diligence, would have been known. MCCMH is deemed to have knowledge of a Breach if it is known, or by exercising reasonable diligence would have been known, by any person other than the person committing the Breach, who is a Workforce Member or agent of MCCMH. (See 45 CFR 164.404(a)(2))

C. Notification to Individuals: Following the discovery of a Breach of Unsecured PHI, notification shall be sent to each individual whose Unsecured PHI has been or is reasonably believed to have been accessed, acquired, used, or disclosed as a result of such Breach.

1. Timing: Generally, Breach Notification must be provided to affected individuals without unreasonable delay and in no case later than 60 calendar days after discovery of a Breach.

2. Content: Breach notification shall be written in plain, understandable language, and shall include, to the extent possible:

i. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

ii. A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

iii. Any steps individuals should take to protect themselves from potential harm resulting from the Breach;

iv. A brief description of the investigation of the Breach, what is being done to mitigate harm to individuals, and to protect against any further Breaches; and

v. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

3. Acceptable Methods:

i. Written Notice:

a) Written notification by first class mail to the individual at their last known address or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by email. The notification may be provided in one or more mailings as information becomes available.

b) If MCCMH knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification may be by first class mail to either the next of kin or personal representative. The notification may be provided in one or more mailings as information becomes available.

ii. Substitute Notice: Where there is insufficient or out of date contact information that precludes written notification directly to the individual, a substitute form of notice that is reasonably calculated to reach the individual shall be provided. Substitute notice is not required where there is insufficient or out of date contact information that precludes written notice to the next of kin or personal representative of a deceased individual.

a) For fewer than 10-individuals, substitute notice may be provided by an alternative form of written notice, telephone, or other means.

b) For 10 or more individuals, substitute notice shall (i) be in the form of either a conspicuous posting for a period of 90 days on the home page of the MCCMH Web site, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the Breach likely reside; and (ii) Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's Unsecured PHI may be included in the Breach.

iii. Urgent Situations. Where the MCCMH Compliance Officer determines that urgency is required because of possible imminent misuse of Unsecured PHI, MCCMH may provide information to individuals by telephone or other means, as appropriate, in addition to providing Written Notice.

D. Notification to the Media: Where a Breach of Unsecured PHI involves more than 500 residents of a State or jurisdiction, MCCMH shall notify prominent media outlets serving the State or jurisdiction

1. Timing: Where appropriate, MCCMH shall provide notification to the media without unreasonable delay, and in no case later than 60-calendar days after discovery of the Breach.

2. Content: Breach notification shall be written in plain, understandable language, and shall include, to the extent possible, the same elements as are required for general notification to individuals (See Section V.C.2., above).

E. Notification to the Government:

1. Following the discovery of a Breach of Unsecured PHI, notification shall be provided to the government in the manner specified on the Department of Health and Human Services website.

2. For Breaches involving 500 or more individuals, notification to the government must be contemporaneous with notice to the individuals.

3. For Breaches involving less than 500 individuals, MCCMH shall maintain a log of such Breaches and, not later than 60-days after the end of each calendar year, provide notification to the government of all Breaches discovered during the preceding calendar year.

F. Notification by a Business Associate:

1. Following the discovery of a Breach of Unsecured PHI, a Business Associate shall notify MCCMH of such Breach.

2. A Breach will be considered "discovered" by a Business Associate as of the first day on which such Breach is known to the Business Associate or, by exercising reasonable diligence, would have been known to the Business Associate. A Business Associate shall be deemed to have knowledge of a Breach if the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).

3. Timing. A Business Associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a Breach.

4. Content. The Business Associate's notice to MCCMH must include, to the extent possible (i) the identification of each individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used, or disclosed during the Breach; (ii) any other available information that MCCMH is required to include in notification to the individual.

5. Additional Business Associate obligations are defined in the MCCMH Business Associate Agreement, as well as in MCCMH MCO Policy No. 10-315, "Business Associates".

G. Law Enforcement Delay. If a law enforcement official states to MCCMH or one of its Business Associates that a notification, notice, or posting providing notice of Breach

would impede a criminal investigation or cause damage to national security, MCCMH or the relevant Business Associate shall:

1. If the statement from the law enforcement official is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30-days from the date of the oral statement, unless a written statement is submitted during that time, in which case MCCMH and/or the Business Associate shall comply with the directive in the written statement.

H. Training. MCCMH will train Workforce Members on this policy within a reasonable period of time after becoming a Workforce Member, and otherwise as such is consistent with 45 CFR 164.530(b). The Board will document all training regarding this policy and retain such documents for a minimum of 6-years from the date of its creation.

I. Complaints from Individuals Served:

1. Individual subjects of PHI may make complaints regarding the Board's policies and procedures respecting confidentiality and/or the Board's compliance with such policies, procedures, or the requirements of HIPAA/HITECH.

2. Privacy complaints from Individuals Served should be made to the MCCMH Office of Recipient Rights (ORR) according to the process described in MCCMH MCO Policy No. 10-350, "Privacy Complaint Process".

3. The ORR will investigate all privacy complaints according to the standards and procedures set forth in MCCMH MCO Policy No. 9-510, "Recipient Rights Investigations", and promptly forward appropriate details to Corporate Compliance for processing according to the standards and procedures set forth herein.

4. The Board will document all such complaints and their disposition, if any, and retain such documentation for a minimum of 6-years from the date of its creation.

5. The Board shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any Individual Served for the exercise of any right established under HIPAA/HITECH, for making a privacy complaint, or for participating in any process or investigation regarding any potential or reported violation of HIPAA/HITECH.

J. Sanctions: The Board will apply appropriate sanctions against any Workforce Member(s) who fail to comply with the Board's privacy policies and procedures or with requirements of HIPAA/HITECH. The Board will document any sanctions that

are applied, if any, and retain such documentation for a minimum of 6-years from the date of its creation.

K. MCCMH shall not require any Individual Served to waive their right under 45 CFR 160.603 to make a complaint to the Secretary of Health and Human Services, as a condition for the provision of treatment, payment, enrollment, or eligibility for benefits.

VI. Procedures

A. Reporting a Known or Suspected Breach:

1. If any Workforce Member becomes aware of any known or suspected instances where PHI may have been accessed or disclosed inconsistent with HIPAA or with MCCMH policy, the Workforce Member must immediately report such issue to both Corporate Compliance and Recipient Rights, as follows:

   i. To Corporate Compliance using any of the following methods:

      a) Telephone (Anonymously, if desired) - 586-469-6481

      b) Email - ComplianceReporting@mccmh.net

   ii. To Recipient Rights using any of the following methods:

      a) Telephone - (586) 469-6528

      b) Fax - (586) 466-4131

      c) Hand delivery of a Recipient Rights Complaint form (Exhibit F to MCO 9-321) detailing the occurrence

2. Examples of issues that should be reported for further investigation include, but are not limited to:

   i. Access of PHI by unauthorized individuals;

   ii. Access of PHI by authorized individuals for non-job-function related purposes;

   iii. Disclosure of PHI to unauthorized individuals

   iv. Disclosure of PHI without an authorization when an authorization is required; and

   v. Disposing PHI without following appropriate protocols.

3. Workforce Members must not attempt to investigate the matter or determine whether an actual (reportable) Breach has occurred before reporting, or whether or not Breach notification obligations have been triggered.

4. Failure to report a known or suspected Breach is a violation of this policy and may result in disciplinary action in accordance with the Board's policies and procedures.

5. Business Associates, subcontractors and/or vendors are required to report any Breach of confidentiality consistent with the terms of their Business Associate Agreement, MCO 10-315, and HIPAA/HITECH.

B. Breach Investigation: Upon receiving a report or learning of an issue that may trigger Breach notification obligations, Corporate Compliance shall gather and document relevant facts and circumstances to determine (i) whether the matter involved Unsecured PHI; if so, (ii) if there has been an impermissible use or disclosure under the privacy regulations that triggers the Board's Breach notification obligations; and (iii) whether the Board's Breach notification obligations have been triggered.

C. Risk Analysis: After gathering all relevant facts (and after consulting the Compliance Officer and/or Corporate Counsel to determine if a Breach exception exists), Corporate Compliance will perform a risk analysis to determine if a Breach has occurred. Under the Privacy Rule, any acquisition, access, use or disclosure is presumed to be a Breach and must be reported unless the Board can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of PHI;
2. Whether the PHI is individually identifiable;
3. The types of identifiers and the likelihood of re-identification;
4. The unauthorized person who accessed/obtained PHI or to whom the disclosure was made (for example, if the person to whom the PHI was improperly disclosed is another HIPAA-covered entity who is also obligated to protect PHI there would likely be a determination that there is a low probability that the PHI was compromised);
5. Whether the PHI was actually acquired or only viewed (e.g. where a laptop with unencrypted PHI is lost, does the forensic analysis reveal that the PHI was actually accessed);
6. The extent to which any risk of PHI has been mitigated.

Depending on the circumstances, some factors may outweigh others. In all cases, the risk assessment must be and thoroughly documented.

D. Breach Notification:

1. In any case where Corporate Compliance cannot establish that there is a low probability that the relevant PHI has been compromised, and/or where there is a high probability that the compromised PHI poses a significant risk of financial, reputational, or other harm to the Individual, the Compliance Officer and Corporate Counsel should be consulted.

2. Where the Compliance Officer and/or Corporate Counsel determine that a reportable Breach has occurred, the Compliance Officer shall direct appropriate staff to make appropriate notification without unreasonable delay but no later than 60-calendar days after discovery of the Breach.

3. Corporate Compliance with maintain documentation of the investigation and documentation which demonstrates that all required notifications were made, or alternatively, documentation that notification was not required.

E. Documentation: Corporate Compliance will ensure that all documentation required by this policy are created and maintained as required.

VII. References / Legal Authority

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

B. 45 CFR §164.404-414

C. 45 CFR §164.530

D. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Department of Health and Human Resources Final Rule, 78 Fed. Reg. 5566 (January 25, 2013) (to be codified at 45 CFR Parts 160 and 164)

E. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html

VIII. Exhibits

None