COMMUNITY MENTAL HEALTH PARTNERSHIP OF SOUTHEASTERN MICHIGAN/PIHP	*Policy and Procedure* *Confidentiality & Access to Consumer Records*
Department: Corporate Compliance Committee **Author:**	**Local Policy Number (if used)**
Regional Operations Committee Approval Date **7/27/2020**	**Implementation Date** **8/24/2020**

I. PURPOSE

This policy establishes guidelines for maintaining confidentiality of consumer information and consumer records, and to identify circumstances under which information may be disclosed.

II. REVISION HISTORY

DATE	REV. NO.	MODIFICATION
10/24/04	1.0	Regional/CMHPSM policy created
8/21/07	1.1	Social Security Number protections added
1/28/11	1.2	Revisions made for compliance with HITECH laws and outcomes of reviews (MDCH ORR); language changes made
4/13/12	1.3	Revisions made per recommendations of MDCH ORR
8/18/14	1.4	Revisions made per recommendations of MDCH ORR and to incorporate new regional entity
4/28/2017	1.5	Revisions made per Public Act 129 of 2014.
9/20/2017	1.6	Revisions made per Public Act 129 of 2014.
5/17/18	1.7	Revisions made per changes to MDHHS ORR Attachment B
6/2020	1.8	Addition of Exhibit C, Template Letter for Notification of Breaches, per EQR CAP

III. APPLICATION

This policy applies to all officials, board members staff, students, volunteers and contractual organizations within the provider network of the Community Mental Health Partnership of Southeast Michigan (CMHPSM).

Effective February 17, 2009, all Business Associates (BAs) are required to abide by all HIPPA and HITECH regulations described in this policy in the same manner as covered entities, including security and privacy rules, penalties, and accountability for Business Associate Agreements, and Health Information Exchanges.

IV. POLICY

It is the policy of the CMHPSM that information in the record of a consumer and other information obtained while providing services to a consumer, shall be kept confidential and is considered Protected Health Information (PHI), including the fact that a person is or is not receiving services. Confidential information may be disclosed outside the CMHSP and its contractual agencies only in the circumstances allowed by law and referenced in this policy.

V. DEFINITIONS

Breach - the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. The term ‘‘breach’’ does not include:

A. Any unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity or business associate IF —
   1. such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate; AND
   2. such information is not further acquired, accessed, used, or disclosed by any person; OR

B. Any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at same facility; AND

C. Any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

Business Associate - An individual or corporate "person" that performs on behalf of the covered entity any function or activity involving the use or disclosure of protected health information (PHI); and is not a member of the covered entity's workforce. Per the HITECH Act of 2009 business associates are now accountable to HIPAA and HITECH regulations in the same way as covered entities.

Clinical Record - The medical and billing records, including protected health information that is maintained for enrollment, treatment and decision making, payment and claims adjudication. This record shall include both the electronic health record and any historical paper records.

Community Mental Health Partnership of Southeast Michigan (CMHPSM) - The Regional Entity that serves as the CMHPSM for Lenawee, Livingston, Monroe and Washtenaw for mental health, developmental disabilities, and substance use disorder services.

Community Mental Health Services Program (CMHSP) - A program operated under Chapter 2 of the Mental Health Code as a county community mental health agency, a community mental health authority, or a community mental health organization.

Confidential Information - All identifiable personal information and material about a consumer, including information contained in automated data banks, health records, and the information that an individual is or is not receiving services.

Confidentiality – To keep all identifiable personal information about a consumer private and not allow such information to be seen or used by anyone who does not have specific authorization or legal permission to do so.

Covered Entity – per 160.103 of title 45, Code of Federal Regulations, Section 160.103, any entity that is:

1. A health plan.
2. A health care clearinghouse.
3. A health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA/HITECH

For the purposes of this policy, the CMHPSM, the CMHSPs, and contractual providers/bodies that meet the above definition, are considered covered entities and will be held to this policy as such.

Data Use Agreement – An agreement that assures that the recipient of a limited data set will only use or disclose the protected health information for limited purposes. The agreement must establish permitted uses and disclosures of the limited data set, establish who is permitted to use or receive the limited data set, and provide for the confidentiality of the limited data set.

Documentable Request - A written request, or a verbal request which shall be documented by staff in the clinical record.

Electronic Health Record – An electronic record of health-related information created, gathered, managed, and consulted by clinicians and staff.

Health Information Exchange (HIE) - An HIE is a community-wide information system used by participating healthcare providers to share health information about consumers for treatment coordination purposes.

Holder of the Record - The agency charged with responsibility for maintaining and safeguarding each consumer's primary record. The CMHSP is the holder of the record for all consumers receiving services from the CMHSP or from an organization providing services under contract with the CMHSP. The CMHSP may delegate to organizations under contract the responsibility of maintaining portions of the record.

Individually identifiable health information - information, including demographic data that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.[13] Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain

other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

Legal Representative - A legal representative is defined as any of the following:
1. A court-appointed guardian,
2. A parent with legal custody of a minor recipient,
3. In the case of a deceased recipient, the executor of the estate or court appointed personal representative,
4. A patient advocate under a durable power of attorney or other advanced directive.

Limited Data Set – Protected health information that excludes direct identifiers of the consumer or of relatives, employers, or household members of the consumer. Direct identifiers are: name, postal address information, phone and fax numbers, e-mail address, social security numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers, device identifiers or serial numbers, URL's, internet protocol address numbers, biometric identifiers, and photographic or any comparable images.

Personal Health Record (PHR) - an electronic record of personal identifiable health information (as defined in section 13407(f)(2)) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

Privileged Information - Information obtained by a psychiatrist, psychologist or other staff member in connection with examination, diagnosis or treatment of a consumer.

Protected Health Information (PHI) - Protected health information means individually identifiable health information that is:
1. Transmitted by electronic media;
2. Maintained in electronic media; or
3. Transmitted or maintained in any other form or medium.

Psychotherapy Notes - Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Regional Entity - The entity established under section 204b of the Michigan Mental Health Code to provide specialty services and supports for people with mental health, developmental disabilities, and substance use disorder needs.

Standard Consent Form – A form created by MDHHS under Public Act 129 of 2014 that requires the CMHPSM and its provider network to use, accept and honor the standard release form.

VI. STANDARDS

A. CMHPSM, CMHSP, and contract agency staff are responsible to ensure individuals served, their legal representatives, and families are educated on their rights and responsibilities related to the elements of confidentiality.

B. The Privacy Officer will follow up regarding all suspected confidentiality breaches. The CMHSP Compliance Liaison will review those investigations/interventions to determine if a HITECH-related breach occurred and consult with the CMHPSM Compliance Officer as needed. The CMHSP Compliance Liaison will ensure compliance with all notification requirements are made to individuals, media, HHS and legal entities where applicable.

C. The CMHSP Compliance Liaison will collaborate with the CMHPSM Compliance Officer to ensure all notification requirements are provided to the media, HHS, and legal entities where applicable.

D. All other confidentiality matters discussed in this policy will be managed by the local Privacy Officer/ local Office of Recipient Rights.

E. All business associates of the CMHPSM shall notify the applicable Covered Entity (CE) of all breaches.

F. The CMHPSM Compliance Officer will maintain data on all breaches and report this data annually to HHS as required.

G. Confidential information entered into the clinical record on or after March 28, 1996, shall be disclosed to a legally competent adult consumer upon his/her request without regard to detriment. Disclosure shall be made as expeditiously as possible, but in no event later than the earlier of 30 days from the date of the request or prior to release from treatment.

H. The CMHPSM and its provider network will use, accept and honor the MDHHS standard release form.

I. Other than exceptions noted in this policy, confidential information may be released with consent from one of the following:
    1. Consumer
    2. Consumer's guardian with authority to consent
    3. Parent with legal custody of a minor consumer
    4. Court approved personal representative or executor of the estate of a deceased consumer to:
        a. Providers of mental health services to the consumer.
        b. An attorney for the consumer.
        c. The consumer or any other person or agency in accordance with this policy.

<u>Information That Must Be Disclosed With or Without Consent</u>

Confidential information must be disclosed, with consent if possible or without consent, under one or more of the following circumstances:

1. Order or Subpoena of a court or legislature for non-privileged information.

2. To a prosecutor as necessary for the prosecutor to participate in a proceeding governed by the Mental Health Code.
3. To the Auditor General (Office of Inspector General).
4. When necessary to comply with another provision of law, e.g., Children's Protective Services Act, Adult Protective Services Act. (Within 14 days after receipt of a written request from DHS Child Protective Services, pertinent records and information shall be released.) Specific procedures are set forth in the policy on Abuse and Neglect.
5. To the Michigan Department of Health and Human Services (MDHHS) when necessary in order for the Department to discharge a responsibility placed upon it by law.
6. To a surviving spouse of the recipient or, if there is no surviving spouse, to the individual or individuals most closely related to the deceased recipient within the third degree of consanguinity (relation by blood) as defined in civil law, for the purpose of applying for and receiving benefits.
7. Under order or subpoena from a Court, to an attorney or other regarding a Child Protective Services civil action per MCLA 722.631.

<u>Information That May Be Disclosed at Discretion of Holder of Record With or Without Consent</u>

Confidential information may be disclosed, with consent if possible or without consent, at the discretion of the holder of the record:

a. To enable a consumer to apply for or receive benefits which shall accrue to the CMHSP Board or shall be subject to collection for liability for mental health services.
b. As necessary for treatment, coordination of care, or payment for the delivery of mental health services, in accordance with the Health Insurance Portability and Accountability Act (HIPAA).

c. For mental health research, evaluation, accreditation, or statistical compilation. The individual who is the subject of the information shall not be identified in the disclosed information unless the identification is essential in order to achieve the purpose for which the information is sought or if preventing the identification would clearly be impractical, but not if the subject of the information is likely to be harmed by the identification. In the case of research, disclosure will not be allowed without an authorization, or an authorization waiver from an Institutional Review Board, unless disclosure is limited to a limited data set and a data use agreement is in place.
d. To providers of mental or other health services or to a local police agency or other public agency when there is a compelling need for disclosure based upon a substantial probability of harm to the consumer or others.

The holder of the record, when authorized to release information to an external mental health provider for clinical purposes by the consumer, guardian, or parent of a minor, as applicable, shall release a copy of the entire medical and clinical record.

Consumer information and records may be exchanged among CMHSP staff and with contractual agencies which provide mental health services without obtaining a Release of Information authorization to the extent that such exchange of information is necessary for the provision of services as allowable by HIPAA/HITECH laws and set forth in the Notice of Privacy Practices.

Consumer information and records exchanged among SUD providers shall comply with re-disclosure protections in accordance with 42 CFR Part 2.

Privileged information shall not be disclosed in civil, legislative, or administrative cases or proceedings, unless the consumer or legal representative has waived the privilege, except under circumstances required by law.

Information shall be provided to external physicians or psychologists appointed or retained by the CMHSP to testify in civil, criminal, or administrative proceedings. The holder of the record shall:

1. Notify physician or psychologists, before the review of records, when the records contain privileged communication which cannot be disclosed in court.
2. Inform the court or other entity that issues a subpoena or order and the Attorney General's office, if involved, if subpoenaed or ordered information is privileged under a provision of law. Privileged information shall not be disclosed unless disclosure is permitted because of an express waiver of privilege or because of other conditions which, by law, permit or require disclosure.
3. Any substance use information that may be provided must follow the requirements of 42 CFR Part 2.

Redisclosure: Specific information in the record obtained from other agencies through a Release of Information authorization will be released with a signed Release of Information authorization unless precluded by 42 CFR Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records. Persons requesting information that cannot be re-disclosed shall be referred directly to the source agency. If the request is made by the consumer, or someone legally authorized to act on behalf of the consumer, for the purpose of obtaining access to the consumer's own record, the entire medical and clinical record will be made available, including information obtained from other agencies.

Information regarding persons other than the consumer identified on the Release of Information authorization shall not be disclosed without similar consent from those persons. With regard to family members, a Release of Information authorization signed by the parent of a minor, guardian, or consumer does not permit disclosure of information regarding any other member of the family unless:

1. The release form specifically includes the other family members and all adult family members have signed a release of information form, or
2. The information released is general and does not include specificity on any family member who has not signed a release of information.

The holder of the record shall not decline to disclose information if a consumer, guardian, or parent of a minor has consented, except for a documented reason. When information is disclosed, the identity of the person to whom it pertains shall be protected and shall not be disclosed unless it is germane to the authorized purpose for which disclosure was sought; and, when practicable, no other information shall be disclosed unless it is germane to the authorized purpose for which disclosure was sought and based on the requestor's "need to know.:

Clinical record information released to any agency or individual shall be accompanied by a Notice of Federal and State Laws Against Further Disclosure.

Accounting of Disclosures

A record shall be kept on the Confidential Information Release/Accounting of Disclosures Log of all disclosures of confidential information and shall include the following information:

1. Information released
2. To whom it is released
3. The date it was released
4. The purpose claimed by the person requesting the information and how the disclosed information relates to the purpose.
5. The legal basis under which a disclosure was made.
6. Statement that the persons receiving the disclosed information can only further disclose consistent with the authorized purpose for which it was released, e.g. Notice of Federal and State Laws Against Further Disclosure.

All accounting of disclosure lists must include the date of the disclosure the name of the person, entity, or business associate to whom the disclosure was made a brief description of the confidential information that was disclosed A summary of Sec, 748, Confidentiality, of P.A. 258 as amended, Michigan Mental Health Code, shall be made a part of each consumer's record and a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure

As of 2/17/2009 business associates must also maintain an accounting of disclosures for each individual they serve, in compliance with the requirements set forth in this policy.

The accounting list can include all covered entity (CE) and business associate (BA) disclosures, or just list CE disclosures and identify the BAs from which individuals could ask for a separate accounting list.
Business associates can be directly asked for an accounting of disclosures they make about an individual, and are therefore required to maintain their own accounting of disclosures

A consumer has the right to request an accounting of disclosures of their confidential information made in the six years prior to the date on which the accounting is requested, but no sooner than April 14, 2003. This accounting does *not* have to include:

- disclosures that were for treatment, payment, and healthcare operations as outlined in the Notice of Privacy Practices and were prior to 1/1/2014 for information that was disclosed as part of the individual's Electronic Health Record (EHR);
- disclosures made without an authorization that were required by law;
- disclosures for national security or intelligence purposes;
- disclosures made as part of a limited data set; or
- disclosures made pursuant to a signed Release of Information authorization.

The accounting of disclosures from a paper/non-EHR record must be provided to the consumer within sixty days of receipt of their Request, must include disclosures that occurred during the preceding six (6) years (or a shorter time period at the request of the individual), but not prior to April 14, 2003, and must include disclosures made to or by the CMHSP and its business associates.

A consumer also has the right to request an electronic copy of their electronic health record.

Peer Review

The records, data, and knowledge collected for or by individuals or committees assigned a peer review function, including the review function under Sec. 143a(1) of the Mental Health Code, are confidential, are not considered part of the consumer's clinical record, shall be used only for the purposes of peer review, are not public records, and are not subject to court subpoena.

Requests for Information from Attorneys, Prosecutors and from Attorneys or Others through Subpoena

If a staff member receives a request for information from an attorney or receives a subpoena requesting confidential information, that Program's Administrator/Department Head or his/her designee shall be informed. That Program's Administrator shall inform the CMH Director/Designee and shall make available to the CMH Director/Designee a copy of the subpoena or request for information along with a description of the actions contemplated by the program.

Information shall be provided by the holder of the record to attorneys, other than prosecuting attorneys, as follows:

1. Attorneys representing recipients may review records on the provider's premises only upon presentation of identification and a consent for release of confidential information completed by the consumer, guardian, or parent of a minor.
2. An attorney who has been retained or appointed to represent a minor pursuant to an objection to hospitalization of a minor shall be allowed to review the records.
3. An attorney who does not represent a consumer may review records only if the attorney presents a certified copy of an order from a court directing disclosure of information to that attorney.
4. An attorney shall be refused written or telephoned requests for information, unless the request is accompanied or preceded by a certified copy of an order from a court ordering disclosure of information to that attorney or unless a consent or release has been appropriately executed. The attorney shall be advised of the procedures for reviewing and obtaining copies of recipient records

A prosecutor may be given non-privileged information pursuant to a subpoena if it relates to proceedings under the Mental Health Code, and a good faith effort has been made to notify the consumer and provide the consumer an opportunity to file an objection with the court. Privileged information may be disclosed pursuant to a court order, if it relates to proceedings under the Mental Health Code, including all of the following:

1. Names of witnesses to acts which support the criteria for involuntary admission.
2. Information relevant to alternatives to admission to a hospital or facility.
3. Other information designated in policies of the governing body.

Any substance use information requested by or provided to an attorney/prosecutor must be in compliance with 42 CFR Part 2. If staff are unsure how to proceed with responding

to requests related to substance use information, staff shall consult with their local Compliance Officer, Recipient Rights Officer, or the PIHP Compliance Officer

Court Services Confidentiality

Information obtained in interviews that take place as part of the court commitment procedure, including commitment interviews and alternative report interviews, may be disclosed without a Release of Information authorization only with respect to the particular purpose for which the examination occurred. A staff member conducting such an interview must explain to the consumer that any information obtained in the interview is not confidential, in relation to a court proceeding. If the consumer was not informed that communications could be used in court proceedings, then those communications are privileged and shall not be disclosed, unless the person has waived the privilege.

Any substance use information requested by or provided to a court must be in compliance with 42 CFR Part 2. If staff are unsure how to proceed with responding to requests related to substance use information, staff shall consult with their local Compliance Officer, Recipient Rights Officer, or the PIHP Compliance Officer

Disclosure of Information Regarding HIV/AIDS Status

A Release of Information authorization that specifies that consent is given for disclosure of information regarding HIV/AIDS status must be obtained before releasing such information. A general consent to release medical or health information is not sufficient.

State law allows information regarding a consumer's HIV/AIDS status to be released without a Release of Information authorization to those staff, students, or volunteers of the CMHSP or organizations under contract to the CMHSP who are diagnosing or caring for the consumer. These are the only staff, students, or volunteers who have a "need to know" this information and includes only those who are providing direct treatment or managing the treatment of the consumer's physical and mental health care. Disclosure to anyone else will require a signed Release of Information authorization.

Disclosure may be made to the local Department of Public Health regarding HIV/AIDS status without a Release of Information authorization if necessary to:

1. Protect the health of an individual.
2. To diagnose and care for a consumer.
3. To prevent further transmission of the virus.

Disclosure to the local Department of Public Health shall not contain information that identifies the individual to whom the information pertains, unless the identifying information is determined by the person making the disclosure to be reasonably necessary to prevent a foreseeable risk of transmission of the virus.

Disclosure of Information Regarding Substance Use Disorder Treatment Program Services

A Release of Information authorization indicating the specific information to be disclosed must be obtained before releasing information regarding consumers who are receiving any alcohol or drug abuse related services, including assessment, diagnosis, counseling, or referral for treatment.

A substance use disorder treatment program may not inform a person outside the program that a consumer attends the program, or disclose any information identifying a consumer as an alcohol or drug abuser unless:

1. The consumer consents to disclose about substance abuse treatment in writing, or
2. The disclosure is required by court order, or
3. The disclosure is made to medical personnel in a medical emergency, or
4. The disclosure is made to qualified personnel for research, audit, or program evaluation, or
5. The consumer commits or threatens to commit a crime either at the program or against any person who works for the program, or
6. There is suspected child abuse and/or neglect which must be reported to DHS Child Protective Services, or
7. Information is needed by a qualified service organization in order to provide services to the program.

Disclosure of Information to Protection and Advocacy Staff

If a staff member receives a request for information from Protection and Advocacy staff, that CMH Director/Designee and Program's Administrator/Department Head shall be informed prior to the disclosure of any confidential information.

If required by state or federal law, the CMHSP grants a representative of Michigan Protection and Advocacy Services access to the records of:

1. A consumer, if the consumer, or other empowered representative has consented to the access.
2. A consumer, including a consumer who has died or whose whereabouts are unknown, if all of the following apply:
    a. Because of mental or physical condition, the consumer is unable to consent to the access.
    b. The consumer does not have a guardian or other legal representative, or the consumer's guardian is the state.
    c. Michigan P&A Services has received a complaint on behalf of the consumer or has probable cause to believe, based on monitoring or other evidence that the consumer has been subject to abuse of neglect.
3. A consumer who has a guardian or other legal representative if all of the following apply:
    a. A complaint has been received by the P&A system or there is probable cause to believe the health or safety of the consumer is in serious and immediate jeopardy.
    b. Upon receipt of the name and address of the consumer's legal representative, Michigan P&A Services has contacted the representative and offered assistance in resolving the situation.
    c. The representative has failed or refused to act on behalf of the consumer.

Use and Protection of Consumer Social Security Numbers

Social Security numbers shall be protected as confidential information when obtained in the course of business by CMHPSM staff and contracted providers. No person shall knowingly obtain, store, transfer, use, disclose or dispose of a Social Security number

that the CMHPSM obtains or possesses except in accordance with the Social Security Privacy Act and this policy.

Obtaining Social Security Numbers

Social Security numbers should be collected only where required by federal and state law or as otherwise permitted by federal and state law for legitimate reasons consistent with this policy. Legitimate reasons for collecting a Social Security number include, but are not limited to:

- Where required for billing purposes.
- When state or federal law, rule, regulation, or court order authorizes, permits, or requires that a social security number appear in the document.
- When a document is sent as part of an application or enrollment process initiated by the consumer.
- When a document is sent to establish, confirm the status of, service, amend, or terminate an account, contract, policy, or health insurance benefit or to confirm the accuracy of a social security number of an individual who has an account, contract, policy, health insurance benefit.
- When a document or information is received by a public body under any of the following circumstances:
    i. The document or information is a public record and is received in compliance with the freedom of information act, 1976 PA 442, MCL 15.231 to 15.246.
    ii. The document or information is a copy of a public record filed or recorded with a county clerk or register of deeds office and is received by that office to a person entitled to receive that record.

Use of Social Security Numbers

Wherever possible, identifying information other than a consumer's Social Security Number shall be used in the course of providing services and supports. Such other identifying information includes the electronically assigned consumer identification number.

All or more than 4 sequential digits of a social security number contained in a public record are exempt from disclosure under the Freedom of Information Act, 1976 PA 442, MCL 15.231 to 15.246. Therefore, a consumer's SSN shall not be disclosed/shall be protected from disclosure with any documents that are sent out in response to a request under the Freedom of Information Act.

Public Display and Account Numbers

No more than four sequential digits of a Social Security number shall be used as a primary account number for an individual.

No more than four sequential digits of a Social Security number shall be placed on, or any materials or documents designed for public display (i.e. identification cards, badges, time cards).

Documents, materials or computer screens that display all or more than four sequential digits of a Social Security number shall be kept out of public view at all times.

Forms used in the provision of services to consumers shall use the Consumer ID number assigned to each consumer. Where use of a consumer's Social Security number is necessary in the course of assuring provision of services/supports, no more than the last four numbers of a consumer's social security number shall be used.

Computer Transmission
No more than four sequential digits of a Social Security number shall be used or transmitted on the Internet or on a computer system or network unless the connection is secure, or the transmission is encrypted.

Mailed Documents
All documents containing more than four sequential digits of a Social Security number shall only be sent in cases where state and federal law, rule, regulation, or court order or rule authorizes, permits or requires that a Social Security number appear in the document.
Documents containing more than four sequential digits of a Social Security number that are sent through the mail shall not reveal the number through the envelope window or otherwise be invisible from outside the envelope or package.

Storage
All documents containing Social Security numbers shall be stored in a physically secure manner. Social Security numbers shall not be stored on computers or other electronic devices that are not secured against unauthorized access.

Access to Social Security Numbers
Only staff that has a need to know for legitimate business reasons shall have access to records containing Social Security numbers. Staff using records containing Social Security numbers must take appropriate steps to secure such records/**i**nformation when not in immediate use.

Disposal of Documents with an SSN
Documents containing Social Security numbers will be retained in accordance with the requirements of state and federal laws. At such time as documents containing Social Security numbers may be disposed of, such disposal shall be accomplished in a manner that protects the confidentiality of the Social Security numbers, such as shredding. See the CMHPSM Record Retention policy for more specific information on state and federal disposal/destruction requirements.

Unauthorized Use or Disclosure of Social Security Numbers
The CMHPSM shall take reasonable measures to enforce this policy and to correct and prevent the occurrence of any known violations. Any staff who knowingly obtains, uses or discloses Social Security numbers for unlawful purposes or contrary to the requirements of this policy shall be subject to discipline up to and including termination*.* Additionally, certain violations of the Act carry criminal and/or civil sanctions. If such a disclosure meets the HITECH definition of a breach it will also be reported according to the breach reporting requirements set forth in this policy. The CMHPSM will cooperate with appropriate law enforcement or administrative agencies in the apprehension and prosecution of any person who knowingly obtains uses or discloses Social Security numbers through the CMHPSM for unlawful purposes.

Disclosure of Information for Purposes of Evaluation, Accreditation, Compilation of Statistical Information, or Research
Confidential information may be disclosed at the discretion of the holder of the record for the purposes of evaluation, accreditation, or compilation of statistical information:

1. Only when it is essential to achieve the purpose for which the information is sought, or

2. When preventing such identification would clearly be impractical.
3. Confidential information shall not be released if the subject of the information is likely to be harmed by its release.

Whenever possible, aggregate data shall be provided which does not identify consumers or disclose confidential information.

Requests for information in connection with evaluation, accreditation or statistical compilation shall be reviewed by the Director's office, which shall ensure that:

1. Confidential information is not disclosed in any manner, including inspecting or sampling of information, unless such disclosure is essential to achieve the purpose and allowed by law.
2. Disclosure is not to be made when identification would be harmful to a consumer.
3. When an evaluator, an accreditor or compiler of statistical information asserts that withholding confidential information about a consumer would be too impractical to be prevented, documentation is provided which verifies this assertion before approval for disclosure is given.
4. Consumer confidentiality shall be safeguarded in any document which is to be disseminated outside the CMHSP.

Requests for information in connection with research, investigative activities, and/or utilization of experimental intervention methods or medication are subject to review by the local Institutional Review Board will be disclosed without a Release of Information authorization only if:

1. An authorization waiver is approved by an Institutional Review Board, OR
2. Disclosure is limited to a limited data set where there is a data use agreement in place.

J. Report of Potential Physical Harm and Duty to Warn

If a staff member assesses that a situation exists or that information received indicates that "substantial or serious physical harm may come to the consumer or to another person in the near future" s/he shall immediately inform the CMH Director/Designee and complete the standard form on Report of Potential Physical Harm (see Exhibit A). The CMH Director/Designee shall be immediately notified and the Report of Potential Physical Harm submitted to him/her. At the discretion of the CMH Director/Designee, confidentiality policies may be waived to disclose the minimum necessary mental health information to the local police agency or to others. Information related to substance use remains confidential.

If the threat of physical violence is against a reasonably identifiable person, and the consumer has the apparent intent and ability to carry out that threat in the foreseeable future, the staff member or Director/designee has a duty to take one or more of the following actions in a timely manner:

1. Hospitalize the consumer or initiate proceedings to hospitalize the consumer.
2. Make a reasonable attempt to communicate the threat to the threatened person and communicate the threat to the local police department for the area where the threatened person resides.
3. If the staff member or Director/designee has reason to believe that the threatened person is a minor or is incompetent by other than age, they will communicate the threat to the threatened person’s parent, legal guardian, or whomever is appropriate

and in the best interests of the threatened person, in addition to communicating the threat to the threatened person, if appropriate, and to the local police department.

A copy of the Report of Potential Physical Harm (see Exhibit A) shall be included in the consumer's record.

K. Delay in Release of Confidential Information

Confidential information entered into the mental health clinical record on or after March 28, 1996 shall be promptly disclosed to a third party, without regard to possible detriment, upon an adult consumer's legally competent request. Information in the record will be re-disclosed only to an extent consistent with the authorized purpose for which the original disclosure was made.

Confidential information related to substance use will be released to a third party who is not the consumer or the consumer's legal representative only as allowed by 42 CFR, Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records.

Except as provided above, disclosure of confidential information entered into the clinical record on or before March 27, 1996 may be delayed if:

1. Staff has determined, in the exercise of professional judgment, that such disclosure would produce a substantial probability of detriment to the consumer or others; or
2. The consumer, guardian or parent of a minor requests that information not be released or declines to consent.

The release of information cannot be delayed if:

1. A consumer or legal representative has given consent to have their attorney receive the information (even if the legal representative requests a delay).
2. There is an order or a subpoena of a court or the legislature for non-privileged information,
3. The information is necessary for the prosecutor to participate in a proceeding governed by the Mental Health Code
4. The information is to be disclosed to the auditor general
5. The information is necessary to comply with another provision of law

If a staff member believes that the disclosure of information contained in the record to a person or agency would produce a substantial probability of detriment to the consumer or others, the staff member must obtain permission of the CMH Director/Designee for any delay in the disclosure. The CMH Director/Designee shall review the request and make a determination whether the disclosure will be allowed within three business days if the record is located on-site and within ten business days if the record is at another location. The record will be released if the benefit of disclosure to the consumer outweighs the risk. The CMH Director/Designee shall also determine whether part of the information can be released without risk.

If information is not disclosed, a statement shall be included in the record explaining why the information was not disclosed. The requestor shall be given written notification of the determination regarding detriment and the justification for the determination. If the requestor disagrees with the determination, s/he may file a Recipient Rights Complaint.

L. Notification of Breaches

A breach is considered as discovered by a Covered Entity (CE)/Business Associate (BA) on the 1st day the breach is known to an entity/associate or should reasonably have been known to such entity or associate (or person) to have occurred.

Effective 2/22/2010, if a breach occurs with information from a consumer's personal health record/electronic health record, and the breach occurred on or after 9/23/09, the following actions must be taken:

- Any suspected breach must be reported immediately to the Office of Recipient Rights and the CMHSP Privacy Officer.
    - The CMHSP Privacy Officer will notify the CMHSP Compliance Liaison of any suspected breach.
- The local CMHSP Compliance Liaison will review all suspected confidentiality breaches to determine if it meets the definition of a breach. The CMHSP Compliance Liaison will consult with the CMHPSM Compliance Officer if needed for the determination of breaches.
- The local HIPAA Privacy Officer/Rights Officer will intervene or investigate suspected confidentiality breaches as required.
- The CMHSP Compliance Liaison will notify the CMHPSM Compliance Officer if a breach occurs that requires state or federal reporting.
- The CMHPSM Compliance Officer will ensure compliance with all notification requirements to individuals, media, HHS and legal entities where applicable
- Individuals will be notified when their unsecured protected health information has been or is reasonably believed by the CE/BA to have been, accessed, acquired, or disclosed as a breach. Notification will be provided by the local Privacy Officer, local Compliance Liaison, or the CMHPSM Compliance Officer, as the situation dictates. Notification will occur without delay and no later than 60 days from when the breach was discovered.
    - Notification provided by a CE/BA shall be in plain language and include:
    - A brief description by the of what happened, including the date of the breach and the date of the discovery of the breach, if known
    - 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).
    - Any steps individuals should take to protect themselves from potential harm resulting from the breach.
    - A brief description of what the CE/BA involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.
    - Contact procedures for individuals to ask questions or learn additional information, to include a toll-free telephone number, an email address, website, or postal address.

    - CMHSPs will report to the CMHPSM Compliance Committee if a PHI breach has occurred, and provide a copy of the letter of notice that was sent to the affected member(s) :
    - Notice can be by mail, email, or multiple forms. Notice should be given by phone if urgent then followed up in writing
    - If the consumer is deceased the next of kin will be notified

- If the consumers cannot be contacted for over 10 days general notice shall be posted on the website or with major media for 90 days and include a toll-free contact number.

See Exhibit C, titled Template Letter for Notification of Breaches

If over 500 consumers are affected, the following additional actions must also be taken:

- The media will be notified within 60 days, and include the same information noted above for notification of individuals.
- The Secretary of Health and Human Services (HHS)will be notified within 60 days

M. Consumer Access to His/Her Own Record

A consumer has the right to request a hard copy of his/her paper record. A consumer also has the right to request an electronic version of their electronic health record (EHR)
A consumer requesting access to his/her own record shall be asked to provide a written request to see part or all of the record and provide appropriate identification before seeing the record (see Exhibit B). The assigned staff, supervisor, Program Administrator/Department Head, or designee shall be available to review the contents of the record with the consumer.

If a consumer requests a copy of his/her paper record, the record shall be copied onto watermarked paper and made available to the consumer within thirty days of receipt of the request. A reasonable amount for photocopying may be charged. The cost per page shall be calculated annually.

If a consumer requests a copy of his/her EHR, the record shall be copied in electronic format and made available to the consumer within thirty days of receipt of the request.

Whenever a consumer/legal representative requests a copy of the consumer's record (regardless of whether the request is for a hardcopy or electronic format) the assigned staff shall assure any necessary accommodations, supports, and/or alternative formats are offered and provided to the consumer to ensure the consumer is able to physically access and understands the contents of his/her clinical record.

Upon receipt of either a hardcopy or electronic copy of one's record, the consumer shall sign a statement that confirms receipt and advises the consumer that the CMHSP cannot protect the confidentiality of records that are released into his/her possession; the consumer will be responsible for protecting the confidentiality of those records.

A competent adult consumer has the right to see all information entered into his/her clinical record on or after March 28, 1996, including reports obtained from other agencies, without regard to possible detriment unless such access is prohibited by 42 CFR Part 2.

Substance use treatment information obtained by consumer access to his or her consumer record is subject to the restriction on use of this information to initiate or substantiate any criminal charges against the consumer or to conduct any criminal investigation of the patient as provided for under 42 CFR.

A consumer has the right to see all information entered into his/her clinical record on or before March 27, 1996, including reports obtained from other agencies. Access will be denied in whole or in part, however, if in the judgment of the CMH Director/Designee:

1. The access is reasonably likely to endanger the life or physical safety of the consumer or another person; or
2. The record makes reference to another person (who is not a health care provider) and providing access to the record is reasonably likely to cause substantial harm to such other person; or
3. If the request is made by the consumer's legal representative and the provision of access to such personal representative is reasonably likely to cause substantial harm to the consumer or another person.

If a request from a consumer for access to his/her record is denied in whole or in part, the CMHSP must provide the consumer with a written denial and offer the consumer the option of obtaining a review of the denial. The written denial must describe the basis for the denial and a description of how the consumer can complain to the CMHSP or to the Secretary of Health and Human Services, including the name, title, and telephone number of the contact person at the CMHSP who will handle such complaints.

If the consumer chooses to have the denial reviewed, the Director/Designee will designate a licensed psychologist, master's level social worker, or master's level psychologist, who did not participate in the original decision to deny access, to act as a reviewing official.

The CMHSP must provide written notification to the consumer of the reviewing official's determination and must provide or deny access in accordance with the determination made by the reviewer.

If the CMHSP does not maintain the record that is the subject of the consumer's request for access, and the CMHSP knows where the requested record is maintained, the CMHSP must inform the consumer where to direct the request for access.

N. Consumer's Right to Amend His/Her Own Record

A consumer, guardian, or parent of a minor may add a notation at any time in the clinical record, and this statement shall become part of the clinical record. A consumer, guardian or parent of a minor may challenge the accuracy, completeness, timeliness, or relevance of factual information in the record and may insert into the record a statement correcting or amending the information at issue, and this statement shall become part of the clinical record within 30 days of its receipt.

The CMHSP must make reasonable efforts to inform and provide the amendment to any healthcare provider the consumer identifies as being in need of the amendment, and to persons, including business associates, that the CMHSP knows have the record that is subject to amendment and that may have relied, or could foreseeably rely, on the information to the detriment of the consumer.

The CMHSP has the right to deny a consumer's request for an amendment if the information that is subject to the request was not created by the CMHSP, unless the consumer provides a reasonable basis to believe that the originator of the record is no longer available to act on the request for amendment. If the request is denied in whole or in part, the CMHSP must:

1. Provide a timely written denial containing the basis for the denial and, if possible, informing the consumer where to direct the request for amendment.
2. Notify the consumer that he/she may either submit a statement of disagreement or that he/she may request the CMHSP to reveal the consumer's request for

amendment, and the CMHSP's denial, with any future disclosures of the confidential information which was the subject of the original request for amendment.

3. Provide a description of how the individual may complain to the CMHSP or to the Secretary of Health and Human Services, including the name, title, and telephone number of the contact person at the CMHSP who will handle such complaints.

O. Record Storage

Hardcopy consumer records shall be stored in locked file cabinets or a locked record room under the supervision of one person designated by the CMH Director/Designee. File cabinets or record rooms containing consumer records shall be kept locked overnight and when unattended to control access to records.

Each program shall institute a system to control the location of consumer records on the premises. No records are to leave the program site unless explicit permission has been granted by the CMH Director/Designee. Consumer records shall be signed out by staff when the record is removed from the office. Sign-out forms shall be placed in the appropriate file when the consumer record is removed.

Consumer records in electronic form shall be maintained and protected under the same state and federal laws and guidelines as outlined in this policy. The electronic health record (EHR) shall be stored and maintained as outlined in the CMHPSM Security Policy and in accordance with federal and state security measures, including the minimum requirements set forth by the National Institute of Standards and Technology.

The Michigan Department of Health and Human Services Guidelines on Record Retention and disposal shall be followed for all consumer records (paper and electronic). Consumer records will be retained until the last date of service plus 20 years. Records closed for 20 years or longer from the last date of service will be destroyed by shredding, burning or chemical recycling. Confidential electronic records should be destroyed in accordance with the U.S. Department of Defense "Standard Industrial Security Program Operating Manual" (DoD 5220.22). Refer to the MDHHS Policy, Records Retention and Disposal Schedules, 07-C-1746/GL for more specific information on the retention and disposal/destruction of consumer records.

VII. EXHIBITS

A. CMHPSM form on Report of Potential Physical Harm
B. Request for Access to Review or Receive a Copy of a Clinical Record form
C. Template Letter for Notification of Breaches

VIII. REFERENCES

Reference:	**Check if applies:**	**Standard Numbers:**
45 CFR Parts 160 & 164 (HIPPA)	X	
HITECH Act of 2009	X	
Federal Information Security Management Act of 2002 (FISMA)	x	

42 CFR Part 2 (Substance Abuse)	X	
Michigan Mental Health Code Act 258 of 1974	X	
The Joint Commission (TJC) Behavioral Health Standards	X	
MDDHS Medicaid Contract	X	
Michigan Medicaid Provider Manual	X	
CMHPSM Policy Review Schedule		
MDHHS Policy, Resident Records: Release to Protection and Advocacy, 07-C-1748/GL-00	X	
Confidentiality of HIV/AIDS Information, MCL 333.5131; Michigan Public Health Code, Public Act 488 of 1988, as amended	X	
Michigan Social Security Number Privacy Act, Public Act 454 of 2004, MCL 445.81	X	
CMHPSM Policy on Sanctions for Breaches of Security or Confidentiality	X	
MDHHS, Records Retention and Disposal Schedules, 07-C-1746/GL	X	
Public Act 129 of 2014	X	

.

IX. PROCEDURES

None

Exhibit A

REPORT OF POTENTIAL PHYSICAL HARM

In the event of imminent danger, all steps necessary and appropriate to protect the immediate health and safety of consumers, staff and the public should be initiated.

Per the CMHPSM, if a staff member assesses that a situation exists or that information received indicates that "substantial or serious physical harm may come to the consumer or to another person in the near future" s/he shall immediately inform the Program Administrator/Department Head or his/her designee and complete a "Report of Potential Physical Harm. The Director/Designee shall be immediately notified, and the Report of Potential Physical Harm be submitted to him/her. Then, confidentially policies may be waived to disclose necessary information to the local police agency or to others under Duty to Warn".

This form is divided into three sections:
(1) Report of Potential Harm
(2) Director or Director's Designee Response
(3) Documentation of Notifications Made

Please be sure to complete *all three* sections.

I. Report of Potential Harm

Report Date:		
Consumer Name:	ID #:	D.O.B.
Date of Threat:	Threat Made to:	
Description of Consumer:		
Description of Threat:		
Identity of person(s) threatened:		
Nature of Threat:		
Assessment of *intent* to carry out threat in foreseeable future:		

Assessment of *ability* to carry out threat in foreseeable future:	
Have procedures been initiated to hospitalize consumer?	
Rationale for waiving confidentiality policy:	
Who has been consulted in making this recommendation?	
Is contact information available for threatened person(s)? If not, what attempts have been made to secure this information?	
Law enforcement agency to be notified:	
Signature and Credentials of Staff:	
Date:	Time:

II. Director or Director's Designee Response:

Waiver of confidentiality approved?	
Rationale:	
Signature:	
Date:	Time:

III. Documentation of Notifications Made:

Person Notified (include description of/relationship to consumer):	Date:	Time:

Description of information provided:
Description of individual's response:

Law Enforcement Agency Notified:		
Agency Contact Name:	Date:	Time:
Description of information provided:		
Response:		

Health & Safety Alert Placed in Electronic Record: Yes No	Date:

Describe any additional follow up action planned/steps taken to protect others: (If minor is involved, include any reports to DHS, parent (custodial or non-custodial), legal guardian)
Signature and Credentials of persons completing notification:

Cc: Office of Recipient Rights
Program Administrator/Department Head
Legal Section of Client File

Exhibit B

Request for Access to Review or Receive a Copy of a Clinical Record
And/Or Request for an Accounting of Disclosures

I, _____ request access to review or receive a copy of the clinical
(Person making request - Print)
record for _____.
(Consumer name)

I confirm that I am either the person identified as the consumer, the consumer's guardian, legal representative, or parent of a minor. I am aware that in order for this request to be reviewed I must show proof of my identity and/or legal ability to make this request.

I am requesting to:

- ☐ Receive an Accounting of Disclosures for the period from _____ to _____
  - ☐ In hard copy
  - ☐ In electronic form (for any accounting recorded in Electronic Health record)

- ☐ Receive a copy of the clinical record
  - ☐ In whole
  - ☐ In part
  - ☐ In electronic form (for any part of the record that is an Electronic Health Record)

  If the request is in part, I am requesting a copy of the following portions of the record:

  _____
  _____
  _____

And/Or:

- ☐ Be given access to review the record

I understand that if I am requesting a copy of or access to the clinical record (either in whole or in part) or an accounting of disclosure:

- I may be charged a reasonable fee for the cost of photocopying the record.
- I will need to sign a statement that I received a copy, that the community mental health services provider cannot protect the confidentiality of any records that are released into my possession, and that I will be responsible for protecting the confidentiality of those records.
- If I am requesting access to review the record, a CMH staff person will be available to review the record.

I also understand I may be denied access to or a copy of the records in whole or in part. If this occurs, I will be informed in writing of the reason that this request is denied and be given information on how to file a complaint.

_____ _____
Signature of Requestor Date

****

For Staff Use Only:

- ☐ Proof of Identification Shown (with picture, i.e. police ID or driver's license; including guardianship/court papers where applicable)

Type of ID shown: _____

Staff Name/Signature: _____

Exhibit C

Template Letter for Notification of Breaches

Agency Letterhead

Date

Consumer/Guardian Address

Dear ,

You are receiving this letter because there has been a breach of your confidential personal health information (PHI) and you have a right to know what occurred, what steps our agency has taken to address the breach, and what options you have related to this matter.

On (date of discovery) it was found that (description of what happened).

This breach occurred on (date of the breach).
OR
We are unable to determine that exact date this breach occurred; based in the information we have it appears it occurred on or around (give approximate date or month and year at the least if the exact date is unknown but you're aware of a timeframe)
OR
At this time we are unable to identify when the breach occurred, If we discover this information in the future we will make sure to let you know.

The types of your personal health information (PHI) that was involved in the breach includes:

- ☐ Full name,
- ☐ Social Security number
- ☐ Date of birth,
- ☐ Home address,
- ☐ Account number,
- ☐ Diagnosis,
- ☐ Disability code
- ☐ Other Specify information involved:

  _____
  _____

The following actions have been taken to investigate this breach:

The following actions have been taken to lessen any harm to you as a result of this breach

The following actions have been taken to make sure we are creating protections from any further breaches:

In order to protect yourself from potential harm as a result of this breach, we recommend you take the following steps:

We understand you may have some more questions or concerns about this information. If you have any questions or want additional information about this matter, you can contact the following staff at your local provider:
Customer Services phone number and address

Office of Recipient Rights phone number and address
Compliance Officer phone number and address

You can also contact the following regional, state, and federal offices:

Regional Compliance Officer
Community Mental Health Partnership of Southeast MI
3005 Boardwalk, Suite 200
Ann Arbor, MI 48103
734-

MDHHS Behavioral Health & Developmental Disabilities Administration Customer Services Hotline:
1-844-275-6324

US Department of Health and Human Services Complaint Line:
https://www.hhs.gov/hipaa/filing-a-complaint/complaint-process/index.html

Sincerely,

(Name and Title)