

Community Mental Health Partnership of Southeastern Michigan/PIHP	Policy Notice of Privacy Practices and Consumer Complaints for Protected Health Information
Committee/Department: Customer Services Committee	Local Policy Number (if used)
Implementation Date 07/08/22	Regional Approval Date 06/24/2022

Reviewed by:	Recommendation Date:
ROC	03/09/2022
CMH Board:	Approval Date:
Lenawee	03/31/2022
Livingston	03/29/2022
Monroe	03/23/2022
Washtenaw	06/24/2022

I. PURPOSE

To establish guidelines for informing consumers/individuals served of the circumstances under which Protected Health Information will be used and disclosed, and their rights regarding their protected health information

II. REVISION HISTORY

DATE	MODIFICATION
01/12/2015	Revised to reflect the new regional entity effective January 1, 2014.
05/17/2018	Revised to reflect updates to the Mental Health Code (330.1748)
06/24/2022	Revised to reflect EQR requirements, regulations, and updates to notification requirements.

III. APPLICATION

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

IV. POLICY

All consumers/individuals served of CMHPSM services have the right to notice of the uses and disclosures of protected health information that may be made in the course of providing services to the consumer/individual served. Furthermore, a consumer/individual served has the right to know the CMHPSM and service provider's legal duties with respect to the use and disclosure of confidential information.

V. DEFINITIONS

Community Mental Health Partnership of Southeast Michigan (CMHPSM): The Regional Entity that serves and is comprised of the four-county affiliation of 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.

Complaint: Any written documentation received that expresses concern that a consumer/individual's right to confidentiality and security of protected information has been violated.

Complainant: A consumer/individual served or anyone acting on behalf of a consumer/individual served, who files a complaint that the consumer/individual's right to confidentiality and security of protected information has been violated.

Protected Health Information: Medical, mental health, and substance abuse information that is individually identifiable and that is transmitted in any form or medium.

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.

VI. STANDARDS

- A. All CMHPSM Board members, employees, students and volunteers shall be apprised of its policies and procedures protecting the confidentiality and integrity of its consumer/individuals' protected health information and be required to sign a Confidentiality Statement.
- B. Each CMHSP will designate a Privacy Officer/designee at each CMHSP to receive complaints concerning the Community Mental Health's (CMH) compliance with policies and procedures related to protecting the confidentiality and security of protected health information.
- C. The CMHPSM will designate a Privacy Officer at the regional entity level to receive complaints concerning substance use disorder (SUD) providers' compliance with policies and procedures related to protecting the confidentiality and security of protected health information.

NOTICE OF PRIVACY

- D. All Notice of Privacy Practices shall comply with section 164.520 of the Health Insurance Portability and Accountability Act of 1996, the Michigan Mental Health Code, 42 C.F.R. (Code of Federal Regulations) Part 2,

Confidentiality of Alcohol and Drug Abuse Patient Records; Final Rule, and any other applicable laws, explaining the allowable uses of protected health information

- E. A Notice of Privacy Practices (see exhibit A) shall be posted at all CMHPSM service delivery sites, and the service delivery sites of all contractual providers. Notice must be posted in a clear and prominent location where it is reasonable to expect consumers/individuals served and those seeking services from the CMHPSM to be able to read it.
- F. Copies of the Notice of Privacy Practices shall be available at each service delivery location to be given to consumers/individuals served or others upon their request.
- G. A Notice of Privacy Practices shall be given to each new consumer/individual served, guardian, or parent of a minor during his or her initial visit along with a brief explanation of the Notice and an opportunity for the consumer/individual served to have questions answered.
- H. If services are provided in an emergency situation, a good faith effort must be made to provide the consumer/individual served with a copy of the Notice Privacy Practices; such efforts must be documented in the consumer/individual's record. A copy of the Notice of Privacy Practices shall be given to the consumer/individual served as soon as reasonably practical after treatment of the emergency situation.
- I. Each consumer/individual served who receives a Notice of Privacy Practices shall be asked to sign an Acknowledgement of Receipt (see exhibit A), which will be made a part of the consumer/individual's record. If the consumer/individual served cannot or will not sign the Acknowledgment of Receipt, a good faith effort to obtain such signature must be documented in the consumer/individual's record, as well as the reason why the acknowledgement was not obtained.
- J. Whenever the Notice of Privacy Practices is revised, the revised Notice of Privacy Practices must be promptly posted at all CMHPSM service delivery sites and made available upon request on or after the effective date of the revision.
- K. The Notice of Privacy Practices and policy shall be reviewed annually at a minimum or otherwise updated as needed.
- L. In the CMHPSM, the Rights Office appoints a local Privacy Officer for each county. The Rights Office Contact will ensure that the Privacy Officer is informed and begins necessary follow-up and/or actions as needed.
- M. The CMHPSM Compliance Officer shall oversee any regulatory changes with notice of privacy practices, and ensure the regional notice is revised and redistributed to the local CMHSPs.

CONSUMER/INDIVIDUAL SERVED COMPLAINTS

- N. A consumer/individual served, who feels that his /her confidentiality has been violated, or his /her protected health information has been improperly used, has the right to a thorough and confidential investigation.
- O. A consumer/individual served, or anyone acting on behalf of a consumer/individual served, who feels that any Board member, employee, student, volunteer or those of organizations under contract with the CMHPSM, has violated the confidentiality and security of their protected health information should contact the Privacy Officer to file a complaint.
- P. There shall not be any retaliation or reprisals against any consumer/individual served, or any person acting on behalf of a consumer/individual served, who reports a suspected violation of its policies protecting the confidentiality and integrity of protected health information. Nor will the CMH require consumers/individuals served to waive their right to a complaint to the Secretary of Health and Human Services as a condition of receiving treatment.
- Q. The Privacy Officer/designee will conduct a thorough and confidential investigation of the allegation in a timely manner and will recommend corrective action to the CMHSP Executive Director. Investigations will be conducted in a manner that will not violate employee rights, e.g. the Bullard-Plawecki Employee Right to Know Act.
- R. The Privacy Officer will inform their CMHSP Risk Manager and/or Compliance Officer at the time a complaint is received and notifies the Risk Manager and/or Compliance Officer of the results of the investigation and any corrective action taken.
- S. The Privacy Officer/designee will inform the complainant in writing of the results of the investigation and any corrective action taken and will ensure the complainant understands that he/she also has the option of contacting the Office of Civil Rights to file a complaint against the CMH.
- T. The Privacy Officer/designee will maintain a system for logging all complaints received and for the secure storage of all investigative documents and evidence.
- U. The Privacy Officer will provide a quarterly aggregate report of complaints and investigations to the Regional Compliance Committee for the purpose of trend analysis.
- V. The Privacy Officer will maintain documentation related to an investigation, and any corrective action taken, for a minimum of six years from the date of its creation or the date it was last in effect, whichever is later.

W. The CMHSP Compliance Liaison will ensure compliance with all notification requirements made to consumers/individuals served and collaborate with the CMHPSM Compliance Officer to ensure all notification requirements are provided to the media, HHS, and legal entities where applicable.

VII. EXHIBITS

Notice of Privacy Practices and Acknowledgement of Receipt, effective date 4/13/03.

VIII. REFERENCES

Reference:	Check if applies:	Standard Numbers:
42 CFR Parts 400 et al. (Balanced Budget Act)	X	
45 CFR Parts 160 & 164 (HIPPA)	X	
42 CFR Part 2 (Substance Abuse)	X	
Michigan Mental Health Code Act 258 of 1974	X	
CMHPSM Confidentiality and Access to Records Policy	X	
CMHPSM Sanctions for Breaches of Security or Confidentiality Policy		
CMHPSM Ethics and Conduct Policy	X	
CMHPSM Corporate Compliance Policy	X	

NOTICE OF PRIVACY PRACTICES (Insert Name of Organization)

This notice describes how medical, mental health and substance use information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

OUR PLEDGE REGARDING PROTECTED HEALTH INFORMATION

We understand that health information about you is personal. We are committed to protecting it. We refer to this information as “Protected Health Information” or “PHI.” We created a record of the care you receive from (insert name of organization). We need this record to provide you with quality care and to comply with certain legal and payment requirements.

This notice will tell you about the ways in which we may use and disclose your PHI. It also describes your rights and certain obligations we have regarding the use and disclosure of PHI. We are required by law to:

- make sure that PHI that identifies you is kept private,
- notify you if there is a breach of your PHI,
- give you this notice or our legal duties and privacy policies concerning your PHI and
- follow the terms of the notice that are currently in effect.

The privacy practices in this notice apply to all staff, students and volunteers and to all contract providers in our region, the Community Mental Health Partnership of Southeast Michigan (CMHPSM)

We reserve the right to change the terms of this notice and will post the revised notice. Upon your request, we will give you a copy of the revised notice. The new notice would be effective for any health information that we hold at that time or receive from that time on.

YOUR RIGHTS REGARDING YOUR PROTECTED HEALTH INFORMATION

- **Confidential Communications.** You may ask that we communicate with you in a particular way or at a certain location, such as calling you at work rather than at home, to maintain confidentiality.
- **Inspect and Copy.** You have the right to review and/or receive a copy of the information in your record. Under very limited circumstances we may deny access to the record or to portions of the record. For instance, if disclosing this information would endanger you or someone else. If any access is denied, you can request a review of this decision by contacting your local customer services staff.
- **Addendum.** You may ask us to include an addendum to the information in your record if you feel it is incorrect or incomplete. You may prepare a correcting statement that will be included in your record.

- **Accounting of Disclosures.** You may request a list of disclosures that we have made of your protected health information. We are not required to track certain disclosures such as those made for treatment, payment and coordination of care described in this notice below, or disclosures made with your signed authorization.
- **Reporting Restrictions.** You may ask us to limit our use or disclosure of your health information. We are not required to agree to your request, but if we do agree to it, we will honor your request unless the information is needed to provide emergency treatment to you.
- **Receiving a Copy.** You may receive a paper copy of this notice at any time upon request.

HOW WE MAY USE AND DISCLOSE YOUR PROTECTED HEALTH INFORMATION

Uses and Disclosures for Treatment, Payment and Coordination of Care

- **For Treatment.** We may use and disclose your protected health information to provide your services. Information about you may be shared with staff, students or volunteers, and with contract providers or regional staff who may be involved in your or your family's treatment. For example, a staff person may need to review your record in order to respond to your emergency. We may also use your health information to remind you about an appointment or to provide information about treatment alternatives or other health-related benefits and services that may be of interest to you.
- **For Payment.** Your health information will be used and disclosed as needed to obtain payment for your services. For example, a bill for services sent to you or to a third-party payer such as Medicaid might include identifying information about you, such as your name, your diagnosis and services received.
- **For Healthcare Operations and Quality Improvement.** We will use or disclose, as needed, your health information to support and improve the activities of our community mental health services. For example, staff may use information in your clinical record to evaluate the care you received.
- **Coordination of Care.** Your health information may be used and disclosed, as needed, to coordinate and manage your mental health and related services by one or more providers involved in your treatment. For example, a staff of community mental health may provide information about you when submitting referrals to providers related to your services.

Uses and Disclosures That May Be Made Only with Your Authorization

- **Individuals Involved in Your Life.** We may disclose PHI about you to a family member or other persons you designate if you give permission to do so. There may be other service providers/agencies not directly involved in your care for whom we would require your permission to share PHI.
- **For Health Information Exchanges (HIE).** Along with other healthcare providers in our area, we may participate in a health information exchange. An HIE is a

community-wide information system used by participating healthcare providers to share health information about you for treatment coordination purposes. Should you require treatment from a participating healthcare provider who does not have your medical records or health information, that healthcare provider can use the system to gather needed health information to treat you. For example, he or she may be able to get laboratory or other test results that have already been performed or find out about the treatment that you have already received. We will include your PHI in this system only if you give us special written permission to do so.

- **Psychotherapy Notes.** We may disclose psychotherapy notes only with your permission unless an exception applies. For example, we may disclose these notes without your permission if required or permitted by law for reasons such as preventing or lessening an imminent threat to someone's health and safety, a state or federal audit of our organization, to defend a legal action brought by you, or to provide training to mental health practitioners.
- **Marketing.** The PIHP does not engage in marketing. Marketing does not include our communication to you about our own products and services, or communication for treatment or case management purposes.
- **Sale of PHI.** The PIHP will not sell your "Protected Health Information" (PHI).
- **Other Uses and Disclosures.** These will happen only with your written authorization, unless otherwise permitted by law as described below.

Uses and Disclosures That May Be Made without Your Authorization

- **As Required by Law.** We may be required by federal, state or local law to disclose your health information.
- **Organizations Involved in Your Care.** If you are a Medicaid enrollee, we may disclose PHI about you to another service provider involved in your care. This would include healthcare data available to providers through the state database.
- **For Public Health Activities.** We may need to disclose your health information to a public health authority that is required by law to receive the information. Such disclosures would be made for the purpose of controlling disease, injury or disability.
- **Abuse or Neglect.** We may be required to disclose your health information if we suspect that you or another person has been abused or neglected.
- **Health Oversight.** We may be required to disclose your health information for an audit, inspection, investigation or other healthcare oversight activity.
- **Judicial or Administrative Proceedings.** We may have to disclose your health information if we receive a court order or subpoena or for risk management purposes.
- **Law Enforcement.** We may have to disclose your health information in connection with a criminal investigation by a federal, state or local law enforcement agency or disclose it to authorized federal officials who provide protective services for the President or other persons.

- **Serious Threat to Health or Safety.** We may be required to disclose information about you to prevent a serious threat to your health and safety or that of another person or of the public.
- **Coroner of Medical Examiner.** We may need to disclose your health information to help identify a deceased person or to determine the cause of death.
- **Research.** We may disclose your health information to researchers only if their research proposal includes protocols to hide your identify and to ensure the privacy of your health information. The research project and its procedures must be approved by a CMHPSM review board.
- **Business Associates.** There are some services provided in our organization through contracts with business associates. To protect your health information, however, we require these business associates to appropriately safeguard your information.
- **Food and Drug Administration (FDA).** We may disclose to the FDA health information relative to adverse events with respect to food, supplements, product and product defects, or post marketing surveillance information to enable product recalls, repairs, or replacement.
- **Special Situations.** Consistent with applicable law, we may disclose health information to funeral directors, coroners and medical examiners, as required by military command authorities, and for national security activities. A mental health services recipient's information will be disclosed only as allowed by law.

If you believe your rights have been violated, contact the (insert name of your organization) Privacy Officer or the Office of Civil Rights. Your services will not be affected in any way if you file a complaint.

- To file a complaint with (insert name of organization) or if you have any questions or want more information, call or write: Privacy Officer, (insert name, address and phone number of your organization).
- To file a complaint with the Office of Civil Rights, call or write:

Office for Civil Rights, U.S. Department of Health and Human Services, 233 N. Michigan Ave., Suite 240, Chicago, IL 60601
 Voice Phone (800) 368-1019, FAX (202) 619-3818, TDD (800) 537-7697
OCRComplaint@hhs.gov

HHS OCR Complaint Portal: <https://ocrportal.hhs.gov/ocr/portal/lobby.jsf>
 HHS OCR website for complaints
<http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html>

(Insert name of organization)

ACKNOWLEDGEMENT OF RECEIPT OF NOTICE OF PRIVACY PRACTICES

I, _____, acknowledge that I have received a copy of the Notice of Privacy Practices.

My signature below indicates that I have received the notice, that I have been provided an opportunity to ask questions, and that I understand the organization's privacy practices as they pertain to my protected health information.

Signature

Date

Witness

Date

(Insert name of organization)

Documentation of Good Faith Efforts

Consumer Name: _____

Date: _____

The consumer presented for services on this date and was provided with a copy of the Notice of Privacy Practices. A good faith effort was made to obtain a written acknowledgement of receipt of the Notice, however, an acknowledgement was not obtained because:

_____ Consumer refused to sign

_____ Consumer was unable to sign or initial because:

_____ There was a medical emergency. Staff will attempt to obtain acknowledgement at the next available opportunity.

_____ Other reason:

Signature of Employee completing form:

(Insert name of organization)

SECURITY AND CONFIDENTIALITY AGREEMENT

As an employee of (Insert name of organization) and as a condition of my employment, I agree to the following:

1. I understand that I am responsible for complying with the HIPAA policies which were provided to me.
2. I will treat all information received in the course of my employment with (Insert name of organization), related to the consumers of services, as confidential and privileged information.
3. I will not access consumer information unless I have a need to know this information in order to perform my job.
4. I will not disclose information regarding (insert name of organization) consumers to any person or entity other than as necessary to perform my job and as permitted under the Community Mental Health Partnership of Southeast Michigan (CMHSPM) HIPAA/Confidentiality policies.
5. I will not log on to any of the computer systems that currently exist or may exist in the future using a password other than my own.
6. I will safeguard my computer password and will not post it in a public place, such as the computer monitor or a place where it will be easily lost, such as on my ID badge.
7. I will not allow anyone, including other employees, to use my password to log on to the computer.
8. I will log off of the computer as soon as I have finished using it.
9. I will not use e-mail to transmit consumer information outside of the CMHPSM, unless I am instructed to do so by the Privacy Officer.
10. I will not take consumer information from the premises in paper or electronic form without first receiving permission from my supervisor and ensuring it is secure.
11. Upon cessation of my employment, I agree to continue to maintain the confidentiality of any information I learned while an employee, and agree to turn over any keys, key fobs, or any other device that would provide access to the agency or its information.

I understand that violation of this agreement could result in disciplinary actions.

Employee Printed Name

Date

Employee Signature

Supervisor Signature