Community Mental Health Partnership of Southeast Michigan/PIHP	*Policy* *Security of Consumer Related Information*
Department: Regional Compliance and EII Operations Committee **Author:**	**Local Policy Number (if used)**
Regional Operations Committee Approval Date **10/11/2017**	**Implementation Date** **11/1/2017**

I. PURPOSE

To establish a policy and procedure to assure reliability of data and security of confidential health information.

II. REVISION HISTORY

DATE	REV. NO.	MODIFICATION
2007	1	Updates
2014	2	Revised to reflect the new regional entity effective January 1, 2014.
8/29/2017		Due for regional review.

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

It is the policy of the Community Mental Health Partnership of Southeast Michigan (CMHPSM)) to protect the confidentiality and security of all consumer related information. This includes the clinical record as well as encounter, demographic, financial data and data from outside sources regarding consumers or services provided through the CMHSPM.

V. DEFINITIONS

Access: The ability to use a computer system or physically secure a copy of the consumer health record. More specifically in regard to electronic health records, the ability to inspect, review, retrieve, store, communicate with, or make use of health information system resources or consumer identifiable data or both.

Community Mental Health Partnership of Southeast Michigan (CMHPSM): The Regional Entity that serves as the PIHP 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.

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.

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.

Consumer Health Record: Any information, whether oral or recorded in any form or medium that: (a) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and that (b) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual. This record includes the electronic health record and any hardcopy/paper clinical information relevant to the consumer's health care.

Health Information Exchange (HIE): the communication of healthcare information electronically across organizations.

Office of Recipient Rights: An office of the local CMH that is responsible for investigating, resolving and assuring remediation of apparent or suspected rights violations and assuring that mental health services are provided in a manner which respects and promotes the rights of recipients as guaranteed by Chapter 7 and 7A of the Mental Health Code, P.A. 258, as amended.

Physical access: The ability to access protected health information.

Physical security: The components of a system that prevent unauthorized access to protected health information.

Protected Health Information (PHI): Health information that contains the consumer's identification (name, Social Security number, date of birth, etc.) or a sufficient amount of other personal information that would allow lead to identification of the consumer.

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.

Recovery Oriented System of Care (ROSC): A ROSC is a coordinated network of community-based services and supports that is person-centered and builds on the strengths and resiliencies of individuals, families, and communities to achieve abstinence and improved health, wellness, and quality of life for those with or at risk of alcohol and drug problems.

VI. STANDARDS

A. CMHPSM shall ensure that all information management practices comply with 45CFR parts 160 & 164 (HIPPA), 42 CFR Part 2 (Substance Abuse), and Michigan Mental Health Code Act 258 of 1974 or any other applicable standards or laws

B. CMHPSM shall assure that adequate security measures exist to prevent inadvertent or unauthorized access to consumer data; and that data will be maintained, used, and transmitted in HIPAA compliant formats and state-wide standardized codes.

C. CMHPSM will provide the mechanisms and resources to the CMHSPs and ROSC providers so that these entities can check for and achieve accuracy and reliability of their data (i.e. encounter reporting, data submissions, performance indicators, and various analyses).

D. CMHSPM will provide monitoring and oversight of data submitted by the CMHSPs, the ROSC providers, and contractual providers to ensure it complies with state and federal standards. The accuracy of the data will be the responsibility of the relevant entity and their contractual providers.

E. CMHPSM will assure compliance with HIPAA regulations by implementing appropriate controls regarding the submission health data regarding individuals receiving services.

F. CMHPSM will provide monitoring and oversight tools to CMHSPs, CMHSP contractual providers, and ROSC providers to ensure the appropriate use of or access to the electronic medical record.

G. CMHPSM will comply with state/federal rules when sending/receiving information through the Health Information Exchange (HIE), re-releasing HIE-obtained information, and providing consumers with electronic access to their record.

H. All staff, students, volunteers and contractual organizations within the provider network of CMHPSM will adhere to the following:

    1. Use or supply of individual consumer information for non-health care uses is prohibited, such as direct marketing, employment or credit evaluation purposes.

    2. Collect and use individual information only:
        a. to provide proper diagnosis and treatment
        b. with the individual's or authorized individual’s knowledge and consent, unless otherwise allowable by law
        c. to receive reimbursement for services provided

d. in the aggregate for research and similar purposes designed to improve the quality and to reduce the cost of care
e. in the aggregate as a basis for required reporting of health information

3. Recognize that information collected about and from consumers must be accurate, timely, complete, and available when needed, by:
    a. ensuring the accuracy, timeliness and completeness of data
    b. ensuring that authorized personnel can access information when needed
    c. completing and authenticating records in accordance with the law, professional ethics and accreditation standards
    d. maintaining records for the retention periods required by law and professional standards
    e. not altering or destroying an entry in a record, but rather designate it as an error while leaving the original entry intact and create and maintain a new entry showing the correct data. Updates and corrections will be noted and tracked historically
    f. implementing reasonable measure to protect the integrity of all data maintained about consumers.
    g. following documented policies and procedures for the routine and non-routine receipt, manipulation, storage, dissemination, transmission and/or disposal of consumer information

4. Remove consumer identifiers when appropriate, such as in statistical reporting and in research studies

5. Report and respond to any actual or potential breach of security/confidentiality in accordance with reporting procedures.

I. Each CMHSP, CMHSP contractual provider, and ROSC providers are responsible for the following security measures:

1. Physical security measures, including physical access controls which limit physical access to program sites and consumer information, while ensuring properly authorized access. Features shall include but not be limited to: equipment and media controls, site security plans for all sites where consumer information is maintained, security of workstation locations, authorization procedures, maintenance procedures and records, need-to-know procedures and sign-in and visitor escort procedures.

2. Personnel security measures, including authorization processes to assure appropriate, need-to-know access to information, background

clearances appropriate to the level of access, adequate training and supervision of all personnel with access to consumer information, maintenance of records of access authorization, and formal discipline procedures including termination.

3. System Security, including ensuring technical security services which guard data integrity, confidentiality and availability and which prevent unauthorized access to all data, including data that is transmitted over a communications network.

J. The CMHSPM shall identify an individual whose responsibilities will include the role of a Security Officer.

K. Immediately report any violations of this policy to the supervisor, Privacy Officer and the Office of Recipient Rights.

L. The EII Operations Committee will run and review the Break Glass Report on a semi-annual basis which will be reported on a semi-annual basis to the Regional Operations Committee.

VII. EXHIBITS

None

VIII. REFERENCES

Reference:	**Check if applies:**	**Standard Numbers:**
42 CFR Parts 400 et al. (Balanced Budget Act)		
45 CFR Parts 160 & 164 (HIPAA) HITECH Act of 2010	X	
42 CFR Part 2 (Substance Abuse)	X	
Michigan Mental Health Code Act 258 of 1974	X	
MDHHS Medicaid Contract		
MDHHS Substance Abuse Contract		
Michigan Medicaid Provider Manual		
CMHPSM Confidentiality and Access to Consumer Records Policy	X	
CMHPSM Privacy and Security of Workstations and Electronic Communication	X	
Privacy and Security of Protected Health Information-Consumer Complaints	X	
Use of Email for Consumer Related	X	

Information		
CMHPSM Sanctions for Breaches of Security or Confidentiality Policy	X	