	<b>Security of Protected Health Information and Safeguarding</b>		
	<b>Customer Clinical Records</b>		
	<b>Chapter:</b>	Recipient Rights	<b>Policy #</b>
<b>Section:</b>	Recipient Rights in all CMH Settings	<b>Revision #</b>	1

- I. **PURPOSE:** To establish policy and procedures for ensuring the security of records and customer information and to assure the security of electronically stored clinical information.
- II. **APPLICATION:** All programs and services operated by the West Michigan Community Mental Health Governing Body.
- III. **REQUIRED BY:** Act 258, Public Acts of 1974, as amended, being MCL 330.1748. Accrediting bodies.
- IV. **DEFINITIONS:**

**Electronic Health Record (EHR)** means a group of records maintained by the agency that are:

- The behavioral, health and billing records relating to an individual maintained by or for a health care provider;
- The enrollment, payment, claims adjudication, and case or clinical and/or health management record systems maintained by or for a health plan, or
- Used, in whole or part, by or for a covered entity to make decisions about individuals.

**Disclosure** means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.


**Legal Representative** means:

- A person legally of age or a governmental agency that, under Michigan law, has authority:
  - ✓ To make decisions related to health care on behalf of an adult or an emancipated or unemancipated minor; or
  - ✓ To act *in loco parentis* for an unemancipated minor; and
- A person vested by order of a court of competent jurisdiction with authority to act on behalf of the estate of a decedent.

**Protected Health Information (“PHI”)** means the privacy, confidentiality, security, or privileged status of individually identifiable health information which is protected under any state or federal law, regulation or rule, including, but not limited to, 42 CFR Part Two, and the Michigan Mental Health Code. Specifically, and without limitation, protected health information includes all health information, whether in oral, written or electronic form, that:

- Is received or created by a WMCMH employee; and
- 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 health care to an individual; and
- That identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

**Treatment, Payment and Health Care Operations (TPO)** shall have the definitions accorded these terms in 45 CFR §164.501 and shall include all of the following:


	<b>Security of Protected Health Information and Safeguarding</b>		
	<b>Customer Clinical Records</b>		
	<b>Chapter:</b>	Recipient Rights	<b>Policy #</b>
<b>Section:</b>	Recipient Rights in all CMH Settings	<b>Revision #</b>	1

- **Treatment** means the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care.
- **Payment** means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collections activities, medical necessity determinations and utilization review.
- **Health Care Operations** includes functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services and auditing functions, business planning and development, and general business and administrative activities.

**Use** means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

V. **POLICY:** It is the policy of the West Michigan Community Mental Health that:

1. All information regarding a customer shall be compiled in one primary electronic health record. Archived health record information is stored and can be retrieved electronically through a request to search to the Director of Corporate Compliance and Risk Management or his/her designee.
2. All individual data and protected health information will be treated as confidential in accordance with professional ethics, accreditation standards, and legal requirements.
3. Information in the record of a customer and other protected health information acquired in the course of providing mental and physical health services to a customer shall be held confidential. The fact that a person is receiving services is confidential.
4. A summary of Section 748 of the Mental Health Code shall be placed in the record of each recipient.
5. West Michigan Community Mental Health and its officers, employees, and agents will collect and use individual clinical information and protected health information only for the purposes of providing clinical services and for supporting the delivery, treatment, payment, integrity, and quality of those services. West Michigan Community Mental Health and its officers, employees, and agents will not use or supply individual clinical and protected health information for non-health care uses, such as direct marketing, employment, or credit evaluation purposes.
6. West Michigan Community Mental Health will maintain electronic health records for the retention periods required by law and professional standards.
7. Financial or other customer information will not be disclosed except as necessary for treatment, payment, billing, health care operations or other authorized purposes as authorized by law and professional standards.

	<b>Security of Protected Health Information and Safeguarding</b>		
	<b>Customer Clinical Records</b>		
	<b>Chapter:</b>	Recipient Rights	<b>Policy #</b>
<b>Section:</b>	Recipient Rights in all CMH Settings	<b>Revision #</b>	1

VI. **PROCEDURES:**

1. Only authorized data users may have records in their possession or access protected health and clinical information. Data users accessing records or electronically stored clinical PHI will be identified and meet WMCMH authorized criteria. Criteria to such access is as follows:
  - 1.1 Clerical functions, e.g., typing, filing, fee determination, processing for release or request for information, etc.;
  - 1.2 Finance/Reimbursement/Quality Assurance, e.g., inputting and/or verifying services activity, including generation of bills through appropriate recording of payment;
  - 1.3 Program staff members assigned to a case and working either with the customer or on the case record itself;
  - 1.4 Consultants working either with customers or on the case record itself;
  - 1.5 Clinical Team Review, Peer and Utilization Review Committee members, and Clinical Oversight Committee; and
  - 1.6 Supervisory and administrative personnel.
2. Access authorization is the process of determining whether a prospective data user should be granted access to WMCMH's data. A data user is a person who has been granted explicit authorization to access WMCMH's data by WMCMH. Access must be granted in accordance with this Access Authorization and other related policies.


Health care providers, such as physicians and other therapists should have access only to data of customers that they have responsibility for, with an emergency override to access other customer data to respond to emergencies. Access would be limited to necessary tasks, such as read-only, ready and copy, read and edit by adding a new entry.

Electronic signatures must comply with WMCMH's electronic signature procedure.

Upon receipt of a request to provide access to a named individual, the Director of Information Services or Designee will determine whether any reason exists to deny the request. Grounds for denial include, but are not limited to, the following:

- A security risk unknown to the requester
- Refusal of prospective data user to sign required documents
- Inability of prospective data user to properly use applications and system assets after training.

The Director of Information of Services or Designee will work with the requester to resolve cases in which the former initially denies access. If the matter cannot be

	<b>Security of Protected Health Information and Safeguarding</b>		
	<b>Customer Clinical Records</b>		
	<b>Chapter:</b>	Recipient Rights	<b>Policy #</b>
<b>Section:</b>	Recipient Rights in all CMH Settings	<b>Revision #</b>	1

resolved, the Director of Information Services or Designee will report the matter to Human Resources for resolution.

No person should have access who does not need access and no person should have more access than necessary, WMCMH may determine that an individual or a group of individuals need more, less, or otherwise changed access because of a change in duties or a change in status, such as full-time to part-time, employee to outside contractor, completion of a project, and the like. When a supervisor makes such a determination, he or she should request that the Director of Information Services or Designee change the current level of access to another level of access.

3. All software applications containing customer related information are separately password protected. Authorized personnel have access to the following SQL database systems. Logging of user access is handled thru the EHR. Security is handled thru Active Directory.
4. The Director of Information Services or Designee will be responsible for auditing data users' access to and use of WMMCH information assets per the Internal Audit Procedures.
5. All WMCMH staff are responsible for establishing and implementing specific procedures at different points of care for the control of electronic health records.
6. West Michigan CMH may invoke the Emergency Access Procedure when an incident occurs that has disabled or will disable, partially or completely, the central computing facilities of West Michigan CMH, the health information system, and/or the communications network for a period of 2 hours or longer or when an incident has substantially impaired the use of health information computers and networks.

The Chief Clinical Officer is responsible for the following tasks:


- a. Establish protocols in the Clinical Oversight Committee that specify the conditions under which physicians and other health care professionals may access customer EHR's for which they have no assigned customer responsibility in emergencies.
- b. Identify to the Director of Information Services or Designee, physicians and other health care professionals that need access or need different access during emergencies.

**VII. SUPPORTING DOCUMENTS:**

WMCMH Internal Audit Procedures

**VIII. POLICY/PROCEDURE REVIEW:**

REV#	APPROVED BY	Policy/Procedure	DATE
NC	Unknown		09/2006
NC	Unknown		09/2014

	<b>Security of Protected Health Information and Safeguarding Customer Clinical Records</b>			
	<b>Chapter:</b>	Recipient Rights	<b>Policy #</b>	5-2-1.1
	<b>Section:</b>	Recipient Rights in all CMH Settings	<b>Revision #</b>	1

NC	Unknown		06/2016
NC	Unknown		08/2017
NC	Unknown		11/2019
1	COC	Title Changes	11/2020
1	COC	Annual Review	01/2022
1	COC	Annual Review	01/2023
1	COC	Annual Review	01/2021
<b>Board Approval Date: 05/22/2003</b>			

**IX. CHIEF EXECUTIVE OFFICER ENDORSEMENT:**

I have reviewed and approved of policy # 5-2-1.1 Revision # 1.

CEO: Lisa A. Williams

Approval Signature: \_\_\_\_\_