
	<b>Security of Electronically Stored Clinical Information</b>			
	<b>Chapter:</b>	Board Services and Program Administration	<b>Policy #</b>	2-2-5
	<b>Section:</b>	Assessment, Service Planning and Documentation	<b>Revision #</b>	3

- I. **PURPOSE:** To establish policy and procedures for assuring 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:** HIPAA.
  
- IV. **DEFINITIONS:**  
  
Security Group: Levels of data security which fall in one of two categories: protection of data and protection of data from unauthorized access.
  
- V. **POLICY:** It is the policy of West Michigan Community Mental Health to ensure that all electronically stored clinical data is protected from unauthorized access via password protection, restricted network and directory access and, when necessary, data encryption.
  
- VI. **PROCEDURES:**
  1. IT shall assign each individual CMH user a log-in name and password required for access to the network. This log in name and password shall be held confidential to prevent unauthorized access to the computer systems within CMH. These methods include, but are not limited to, individualized username and password and built-in security within the software. This password shall be changed by the user upon first login. Users are to use multi-factor authentication where possible.
  
  2. IT shall implement computer network security by restricting user access to certain parts of the network by creating and maintaining permissions. A “permission” is a set of rules that identifies a certain part, or subset, of a computer network. Each user will be assigned a specific set of permissions to access the parts of the network that pertain to their job. The permissions for West Michigan Community Mental Health shall be created as determined necessary by IT, with the approval of the IT Director and as third party software design permits.
  
  3. The IT Team shall be responsible for recommending specific regulatory compliant procedures for the control of electronically stored clinical information. This includes but is not limited to security concerning the access to and storage of the information.
  
  4. Electronic communication of any customer individually identifiable personal health information (PHI) with outside sources, such as the PIHP, Health and Human Services or the Department of Community Health, shall all be transmitted following HIPAA compliant patient confidentiality rules.
  
  5. Where possible, access to the information shall be protected with a firewall.
  
- VII. **SUPPORTING DOCUMENTS:** Not applicable.

	<b>Security of Electronically Stored Clinical Information</b>			
	<b>Chapter:</b>	Board Services and Program Administration	<b>Policy #</b>	2-2-5
	<b>Section:</b>	Assessment, Service Planning and Documentation	<b>Revision #</b>	3

VIII. **POLICY/PROCEDURE REVIEW:**

REV#	APPROVED BY	Policy/Procedure	DATE
			10/2007
			04/2018
2	Corp. Comp. Comm	Procedure	10/2021
2	Corp. Comp. Comm	Annual Review	12/2022
3	Corp. Comp. Comm	Annual Review	11/2023
<b>Board Approval Date: 04/16/1996</b>			

IX. **CHIEF EXECUTIVE OFFICER ENDORSEMENT:**

I have reviewed and approved of policy # 2-2-5 Revision # 3.

CEO: Lisa A. Williams Approval Signature: \_\_\_\_\_