ST. CLAIR COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

ADMINISTRATIVE PROCEDURE

Date Issued 05/24

CHAPTER	**CHAPTER**	**SECTION**	**SUBJECT**
Information Management	08	002	0005

SECTION	**SUBJECT**
Data Management	Protected Health Information – Privacy Measures

WRITTEN BY	**REVISED BY**	**AUTHORIZED BY**
Lisa K. Morse	Tommy Rankin	Telly Delor

I. APPLICATION:

☐ SCCCMHA Board
☒ SCCCMHA Providers & Subcontractors
☒ Direct Operated Programs
☒ Community Agency Contractors
☒ Residential Programs
☒ Specialized Foster Care

II. PURPOSE STATEMENT:

St. Clair County Community Mental Health Authority Board shall ensure that St. Clair County Community Mental Health Authority (SCCCMHA) have policies/administrative procedures in place that are designed to meet the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) privacy standards.

III. DEFINITIONS:

A. HIPAA: A United States law put in place to provide privacy standards to protect patient's medical records and other health information provided to health plans, doctors, hospitals, and other healthcare providers. The HIPAA Privacy Rule requires health plans and covered health care providers to develop and distribute a privacy notice that provides a clear, user-friendly explanation of individuals' rights with respect to their personal health information and the privacy practices of health plans and health care providers.

B. HITECH: A United States law put in place to promote the adoption and meaningful use of health information technology.

C. Protected Health Information: Any information about health status, provision of healthcare, or payment for healthcare that is created or collected by a covered entity that can be linked to a specific individual.

IV. STANDARDS:

Any plans/policies/administrative procedures must address the following:

A. SCCCMHA's Board, officers, employees, agents, and providers shall not use or supply protected healthcare information of an individual receiving services for non-healthcare uses, such as direct marketing, employment, or credit evaluation purposes without their written consent.

CHAPTER	CHAPTER	SECTION	SUBJECT
Information Management	08	002	0005
SECTION	**SUBJECT**		
Data Management	Protected Health Information – Privacy Measures		

B. Protected healthcare information of an individual served will only be used to provide proper diagnosis and treatment; with the individual's knowledge and consent; to receive reimbursement for services provided; for research and similar purposes designed to improve the quality and to reduce the cost of healthcare; and as a basis for required reporting of health information.

C. All staff will store protected healthcare information in a secure manner; which involves logging off or locking workstations when not in use or away from their desk; locking up confidential materials when not being worked on; secure interoffice mail in confidential envelopes marked "confidential"; will not leave an individual's information unattended; staff will not leave visitors unattended in staff only areas; and staff will not fax any identifiable personal information, unless it is an emergency, or electronically transfer any protected healthcare information that is not encrypted.

D. Any device that can potentially be used to store protected health information must set a complex password that contains a minimum of 8 characters including 1 uppercase, lowercase, number, and/or a special symbol. If the device cannot accept a password of at least 8 characters, then it will be set to the maximum number allowed and the auto lock feature must be set to 5 minutes or less.

E. A privacy notice is required. The notice must:

1. Describe the ways SCCCMH may use and disclose protected health information
2. State SCCCMH's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice
3. Describe individuals' rights, including the right to complain to HHS and to SCCCMH if they believe their privacy rights have been violated
4. Include a point of contact for further information and for making complaints.
5. Be provided to an individual receiving services not later than the first service encounter by personal delivery (for in-person visits), by automatic and contemporaneous electronic response (for electronic service delivery), and by prompt mailing (for telephonic service delivery). In emergency treatment situations, the provider must furnish its notice as soon as practicable after the emergency abates.

F. SCCCMH must make its notice available to any person who asks for it, and it must be posted in a clear and easy to find location where patients are able to see it.

G. SCCCMH must prominently post and make available its notice on any website it maintains that provides information about its customer services or benefits.

H. **Acknowledgement of Notice Receipt.** SCCCMH must make a good faith effort to obtain written acknowledgement of receipt of the privacy practices notice and must document the reason for any failure to obtain the patient's written acknowledgement, except for in emergency treatment situations.

CHAPTER	**CHAPTER**	**SECTION**	**SUBJECT**
Information Management	08	002	0005
SECTION	**SUBJECT**		
Data Management	Protected Health Information – Privacy Measures		

V. PROCEDURES:

None Available

VI. REFERENCES:

A. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

B. Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)

C. "Privacy Standards" 45 CFR Parts 160 & 164

VII. EXHIBITS:

None Available

VIII. REVISION HISTORY:

Dates issued 02/02, 08/04, 11/06, 07/09, 03/12, 05/13, 05/14, 05/15, 05/16, 05/17, 04/18, 05/19, 07/20, 05/21, 04/22, 04/23