ST. CLAIR COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

ADMINISTRATIVE PROCEDURE

Date Issued 05/23

<table>
<tr><td colspan="2"><b>CHAPTER</b>
Information Management</td><td><b>CHAPTER</b>
08</td><td><b>SECTION</b>
002</td><td><b>SUBJECT</b>
0005</td></tr>
<tr><td><b>SECTION</b>
Data Management</td><td colspan="4"><b>SUBJECT</b>
Protected Health Information – Privacy Measures</td></tr>
<tr><td><b>WRITTEN BY</b>
Lisa K. Morse</td><td colspan="2"><b>REVISED BY</b>
Tommy Rankin</td><td colspan="2"><b>AUTHORIZED BY</b>
Tracey Pingitore</td></tr>
</table>

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.

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.

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.

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.