ST. CLAIR COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

ADMINISTRATIVE PROCEDURE

Date Issued 9/24

CHAPTER Information Management		**CHAPTER** 08	**SECTION** 003	**SUBJECT** 0025
SECTION Electronic Health Record	**SUBJECT** Community Electronic Health Records (CEHR)			
WRITTEN BY Michelle Measel-Morris	**REVIEWD BY** Denise Choiniere and LaTausha Campbell		**AUTHORIZED BY** Telly Delor	

I. APPLICATION:

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

II. PURPOSE STATEMENT:

St. Clair County Community Mental Health (SCCCMH) shall provide individuals and/or their guardians the opportunity to enroll in a secure, confidential, and easy to use website that gives individuals 24-hour access to elements of their health records.

III. DEFINITIONS:

A. Enrollment in CEHR (Community Electronic Health Record): The process of setting up a CEHR Portal Account, including PIN, User ID, password, and clear instructions.

B. Continuity of Care Document (CCD): The CCD is an electronic document type based on the HL7 Clinical Document Architecture (CDA) standard, which specifies that the content of the document consists of text (which ensures human interpretation of the document) and structured parts (for software processing). The structured part provides a framework for SNOMED and LOINC coding, which is required for Meaningful Use. The CCD or transition of care summary contains a core data set of demographic and clinical information. It provides a means for a healthcare practitioner to aggregate all of the pertinent data about a patient and forward it to another practitioner, system, or setting to support the continuity of care. Its primary use is to provide a snapshot in time containing the pertinent clinical, demographic, and administrative data for a specific patient. CCDs are a thorough means of transferring health data on patients based on a standard format, in a specifically designed portable file.

C. Direct Email: Direct secure messaging (DSM) is a secure, encrypted web-based communication system for physicians, nurse practitioners, and other healthcare providers to share protected health information (PHI). Individuals or guardians can send CCDs to providers with a Direct Secure Message through CEHR.

D. "Patient" Portal: A secure website where specific health information about an individual is stored and is available for the individual to securely view. Access is controlled, PIN numbers are

assigned, and a secure password must be chosen to complete access. This tool can benefit patients and providers by enhancing patient access and increasing administrative efficiency and productivity.

E. Protected Health Information (PHI): Individually identifiable health information (1)(i) transmitted by electronic media; (ii) maintained in any medium described in the definition of electronic media or (iii) transmitted or maintained in any other form or medium. (2) Excludes individually identifiable health information in (2)(i) Education records covered by the Family Educational Right and Privacy Act, as amended 20 U.S.C. 1232g; and (ii) records described at 20 U.S.C. 1232g(a)(4)(B)(iv).

IV. STANDARDS:

A. Benefits of the Portal: Individuals can view their Portal accounts anywhere they have Internet access. An individuals can review parts of their medical record, send a message to their Primary Caseholder, access important health information, view their medication lists, obtain educational information, and maintain account information. More features may be added in the future.

B. Providing individual access to electronic health records is intended to meet requirements of Meaningful Use as outlined in the HITECH Act and must be compliant with HIPAA, demonstrate improved quality of care, support administrative efficiencies, and allow access to personal health information.

C. Individuals are able to send a Secure Message to their Primary Caseholder, and the Primary Caseholder can respond via Secure Messaging. Staff are able to send a message to the individual receiving services or guardian through CEHR. Messages are sent to the Primary Caseholder's in-box (Secure Messaging) in OASIS.

D. Individuals are advised that the portal (CEHR) is not appropriate for communicating urgent medical issues, crisis situations or anything that requires immediate attention.

E. There is no direct communication regarding clinical information to an external email address.

F. Utilizing CEHR allows for a method of viewing information that prevents unauthorized parties from being able to access or see specific information. Individuals are responsible for ensuring that their passwords are not shared and should not permit others from accessing their personal health information.

G. Central Intake staff will assign access to CEHR to individuals/guardians at their request.

H. Information in CEHR is updated in "real time," so there is no wait to see updated information.

V. PROCEDURES:

Primary Caseholder

1. Assigns a login PIN to individuals 18 years of age or older, when requested or if not already assigned by Central Intake staff, and when it is deemed clinically appropriate. Staff will print out

CHAPTER	CHAPTER	SECTION	SUBJECT
Information Management	08	003	0025
SECTION	**SUBJECT**		
Electronic Health Record	Community Electronic Health Records (CEHR)		

and provide instructions for creating an account with a user ID and a secure password. PIN numbers can be reassigned if necessary and passwords can be reset by the individual.

2. Creates an account. Individuals should read the Terms of Use and must choose either "Agree" or "Decline" the terms before any access is allowed.

3. Explains to individuals that we serve that CEHR is a secure website and is an optional service. Individual access can be withheld, suspended, or terminated at any time and for any reason. If access is suspended or terminated, the individual will receive notification promptly (within 7 days) from their Primary Caseholder.

4. Assists individuals who receive a PIN. Individuals who login to CEHR using their User ID and secure password should ensure that their personal information regarding contact and emergency numbers are accurate. If any of this information is found to be inaccurate, individuals are instructed to contact their Primary Caseholder for updating either though sending a message in CEHR, by phone or face to face contact.

5. Explains to individuals that through CEHR, they may view parts of their health information, manage their account, and enter requests (e.g., needing an appointment).

6. Explains to individuals that CEHR is not intended for emergency purposes and that any crisis situation or emergency medical situation should be handled through the standard procedures (After hour crisis line, 911, etc.)

7. Responds to Secure Messages sent by individuals in a timely and professional manner. Staff can utilize Secure Messaging as an outreach attempt, for collaborative documentation, setting appointments, updating demographics and to answer basic non-crisis or urgent requests.

8. Explains to individuals that request access to CEHR that SCCCMH is not liable for the security to access CEHR.

9. Monitors individual PIN assignments and notifies their Supervisor if an individual may require suspension or termination of CEHR individual access due to potential of harm. If a clinician or prescriber believes that substantial harm may arise from the disclosure of particular information, access to CEHR can be denied or be suspended at any time.

VI. REFERENCES:

N/A

VII. EXHIBITS:

N/A

VIII. REVISION HISTORY:

Dates issued 10/12, 11/12, 01/14, 01/15, 01/16, 01/17, 01/18, 01/19, 03/20, 03/21, 11/21, 11/22, 11/23.