ST. CLAIR COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

ADMINISTRATIVE PROCEDURE **Date Issued 09/23**

CHAPTER Information Management		**CHAPTER** 08	**SECTION** 002	**SUBJECT** 0006
SECTION Data Management	**SUBJECT** Health Care Information - Privacy & Security Measures (HIPAA)			
WRITTEN BY Lisa K. Morse	**REVISED BY** Tommy Rankin		**AUTHORIZED BY** Tracey Pingitore	

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 (SCCCMHA) shall ensure that all staff preserve the integrity and the confidentiality of client information.

SCCCMHA will maximize safeguards against unauthorized access to Protected Health Information (PHI). In the event that these safeguards are breached, SCCCMHA shall notify all necessary parties, including the individual(s) whose records have been compromised, as well as appropriate state and federal offices and available media outlets. The notification process will be executed pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act of the American Recovery and Reinvestment Act of 2009, including subsequent regulatory amendments published at 78 CFR 5566, and handle SUD information as required of 42 CFR Part 2. (Exhibit A).

III. DEFINITIONS:

A. Breach: The unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of such information. Breach exceptions include:

1. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under HIPAA.

2. Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA.

CHAPTER	CHAPTER	SECTION	SUBJECT
Information Management	08	002	0006
SECTION	**SUBJECT**		
Data Management	Health Care Information – Privacy Measures (HIPAA)		

a. A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

B. Business Associate: An individual, group or agency with whom SCCCMHA has a relationship and the Business Associate role is that of a non-covered entity and PHI is shared as part of doing business.

C. Covered Entity: St. Clair County Community Mental Health Authority (SCCCMHA).

D. Health Information: Any information, including genetic information whether oral or recorded in any format or medium that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) 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 the provision of health care to an individual in 45 CFR § 160.103.

E. Individual: The person who is the subject of PHI and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502 (g).

F. Privacy Rule: The Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

G. Protected Health Information: (1) "Protected Health Information (PHI)" shall have the same meaning as the term "protected health information" in 45 CFR §164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity, and (2) "Protected Health Information (PHI)" means individually identifiable health information: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. For PHI exclusions see 45 CFR §160.103.

H. Unsecured Protected Health Information: If rendered unusable, unreadable, or indecipherable to unauthorized individuals by one or more of the methods identified per the technologies and methodologies in the HITECH Act, then PHI is not unsecured.

I. Workforce: Employees, volunteers, trainees, and other persons under the direct control of SCCCMHA, whether or not they are paid by SCCCMHA.

IV. STANDARDS:

A. SCCCMHA strives to ensure that its officers and employees have the necessary confidential individually identifiable health information to provide the highest quality care possible. SCCCMHA protects the confidentiality of individuals' information to the highest degree possible so that individuals are not concerned with providing information to the agency for purposes of treatment.

CHAPTER	CHAPTER	SECTION	SUBJECT
Information Management	08	002	0006
SECTION	**SUBJECT**		
Data Management	Health Care Information – Privacy Measures (HIPAA)		

B. SCCCMHA officers and employees will not use or supply individual or employee confidential or privileged information for non-health care uses, such as direct marketing, employment, or credit evaluation purposes without the appropriate consent.

C. PHI will only be used to provide proper diagnosis and treatment; to receive reimbursement for services provided; for research and similar purposes designed to improve the quality and to reduce the cost of health care; and as a basis for required reporting of PHI.

D. PHI collected must be accurate, timely, complete, and available when needed.

E. All staff will employ reasonable safeguards to prevent impermissible disclosures of PHI. Some of these include:

1. Storing PHI in a secure fashion
2. Logging off or locking workstations when not in use
3. Encrypting all electronic communications which include PHI
4. Protecting passwords and locking desktop and mobile devices when not in use
5. Securing material away when not being worked on
6. Securing interoffice mail in confidential envelopes
7. Will not leave visitors unattended in staff only areas
8. Will not leave PHI unattended
9. Will avoid discussing PHI in public area, and if not possible, will speak quietly when discussing PHI in public areas
10. Will not routinely fax any individual identifiable health information
    a. In accordance with the HIPAA Security guideline 45 CFR § 164.530(c), 45 CFR § 164.306, staff must verify that the individual, clinician, or employee has submitted a request to release PHI to another party.
    b. The HIPAA Privacy Rule does permit physicians to disclose PHI to another health care provider for treatment purposes.
    c. For treatment purposes PHI can be disclosed by secure fax or other means.
    d. Covered entities must have in place reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of PHI that is disclosed using a fax machine. Examples of measures that could be reasonable and appropriate in such a situation include the sender confirming that the fax number to be used is in fact correct for the receiver's location, and placing the fax machine in a secure location to prevent unauthorized access to the information.

F. As required, SCCCMHA will notify individuals whose unsecured PHI has been inappropriately accessed, acquired, used, or disclosed, compromising the security or privacy of the PHI. The notification requirements will only apply to breaches of unsecured PHI. If PHI is encrypted or destroyed in accordance with HIPAA guidelines, there is a "safe harbor" and notification is not required.

CHAPTER	CHAPTER	SECTION	SUBJECT
Information Management	08	002	0006
SECTION	**SUBJECT**		
Data Management	Health Care Information – Privacy Measures (HIPAA)		

G. Employees must:

1. Treat all individually identifiable health information as confidential in accordance with professional ethics, accreditation standards, and legal requirements.
2. Not divulge individually identifiable health information for purposes other than treatment, payment, coordination of care, or operation of the agency, unless the individual (or his or her authorized representative) has properly consented to the release or the release is otherwise authorized by law.
3. Follow the Release of Case Record Information administrative procedure #03-002-0030 to request a release of information. Take appropriate steps to prevent unauthorized disclosures, such as specifying that the recipient of the PHI may not further disclose the information without the individual's consent or as authorized by law.
4. Remove individual identifiers when appropriate, such as in statistical reporting and in medical research studies.
5. Not disclose financial or other individually identifiable health information except as necessary for billing or other authorized purposes as authorized by law and professional standards.

H. Acknowledgement by the individual or guardian of receipt of the Privacy Notice Brochure is covered under the annual Informed Consent administrative procedure #05-002-0006.

I. Violation of this administrative procedure is grounds for disciplinary action, up to and including termination of employment in accordance with SCCCMHA's Personnel: Corrective/Disciplinary Action administrative procedure #06-001-0055.

J. All electronic transmissions of PHI must be encrypted to meet the security regulations of HIPAA and the HITECH Act of the American Recovery and Reinvestment Act (ARRA) of 2009.

K. SCCCMHA designates the Chief Operating Officer as its Privacy Officer.

L. Following the discovery of a potential breach, SCCCMHA shall begin an investigation, conduct a risk assessment as needed, and, based on the results of the risk assessment, begin the process of notifying each individual whose PHI has been, or is reasonably believed by SCCCMHA to have been, accessed, acquired, used, or disclosed as a result of the breach. SCCCMHA shall also begin the process of determining what notifications are required or should be made, if any, to the Secretary of the U.S. Department of Health and Human Services (HHS), media outlets, or law enforcement officials.

M. For breach response and notification purposes, a breach is presumed to have occurred unless SCCCMHA can demonstrate that there is a low probability that the PHI has been compromised based on, at minimum, the following risk factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification such as:
   a. Social security numbers, credit cards, financial data

CHAPTER	CHAPTER	SECTION	SUBJECT
Information Management	08	002	0006
SECTION	**SUBJECT**		
Data Management	Health Care Information – Privacy Measures (HIPAA)		

   b. Clinical detail, diagnosis, treatment, medications
   c. Mental health, substance abuse, sexually transmitted diseases, pregnancy
2. Regarding the unauthorized person who used the PHI or to whom the disclosure was made:
   a. Does the unauthorized person have obligations to protect the PHl's privacy and security?
   b. Does the unauthorized person have the ability to re-identify the PHI?
3. Was the PHI actually acquired or viewed? For example, does analysis of a stolen and recovered device show that PHI stored on the device was never accessed?
4. The extent to which the risk to the PHI has been mitigated: Can SCCCMHA obtain the unauthorized person's satisfactory assurances that the PHI will not be further used or disclosed or will be destroyed?

N. Notice to affected individuals shall be written in plain language and must contain the following information:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
2. A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).
3. Any steps the individuals should take to protect themselves from potential harm resulting from the breach.
4. A brief description of what SCCCMHA is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
5. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, email address, website, or postal address.

O. Notice to affected individuals shall be made without unreasonable delay, and in no case later than 60 calendar days after the discovery of the breach. If SCCCMHA determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate, in addition to the methods stated below. It is the responsibility of SCCCMHA to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of any delay.

P. The notification letter shall be sent to the individual‘s last known address, or by electronic mail (if the individual has agreed to electronic notice and such agreement has not been withdrawn at time of breach notification). If SCCCMHA is aware that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification shall be sent to the next of kin or personal representative.

Q. If individuals’ contact information is insufficient or out of date, not allowing for direct written or electronic notification, a substitute form of notice to reach individuals shall be provided. If there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, by telephone, or by other means.

CHAPTER	CHAPTER	SECTION	SUBJECT
Information Management	08	002	0006
SECTION	**SUBJECT**		
Data Management	Health Care Information – Privacy Measures (HIPAA)		

If there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of SCCCMHA's website, or a conspicuous notice in major print or broadcast media in SCCCMHA's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where individuals can learn whether their PHI may have been included in the breach.

R. Notification to Michigan Department of Health and Human Services (MDHHS) Regarding Breach

1. In the event of any suspected or confirmed unauthorized use or disclosure of PHI (as defined by HIPAA definition), SCCCMHA will notify and collaborate with MDHHS to mitigate the breach, and will provide to MDHHS a plan of corrective actions to prevent further unauthorized uses or disclosures of PHI (Exhibit C).

S. Notification to U.S. Department of Health and Human Services (HHS) Regarding Breach

1. In the event a breach of unsecured PHI affects 500 or more of SCCCMHA's individuals, HHS will be notified at the same time notice is made to the affected individuals, in the manner specified on the HHS website or via letter (Exhibit D).
2. If fewer than 500 of SCCCMHA's individuals are affected, SCCCMHA will maintain a log of the breaches to be submitted annually to the Secretary of MDHHS no later than 60 days after the end of each calendar year, in the manner specified on the MDHHS website. The submission shall include all breaches discovered during the preceding calendar year (Exhibit F).

T. Notification to Media Regarding Breach

1. In the event the breach affects more than 500 residents of a state, prominent media outlets serving the state and regional area will be notified without unreasonable delay, and in no case later than 60 calendar days after the discovery of the breach. The notice shall be provided in the form of a new/press release (Exhibit E).

U. SCCCMHA shall maintain a process to record or log all breaches of unsecured PHI, regardless of the number of individuals affected. The following information shall be collected for each breach (Exhibit F):

1. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of individuals affected, if known.
2. A description of the types of unsecured PHI that were involved in the breach (such as full name, social security number, date of birth, home address, account number, other).
3. A description of the action taken with regard to notification of individuals regarding the breach.
4. Steps taken to mitigate the breach and prevent future occurrences.

CHAPTER	CHAPTER	SECTION	SUBJECT
Information Management	08	002	0006
SECTION	**SUBJECT**		
Data Management	Health Care Information – Privacy Measures (HIPAA)		

V. PROCEDURES:

A. **Obtaining and processing PHI**

Staff

1. Provides individuals receiving services with Privacy Notice.
2. Collects and uses individually identifiable health information only for the purposes of providing mental health, or co-occurring disorder services and for supporting the delivery, payment, integrity, and quality of those services.
3. Uses their best efforts to ensure the accuracy, timeliness, and completeness of data and ensure that authorized personnel can access the data when needed.
4. Completes and authenticates records in accordance with the law, ethics, and accreditation standards.
5. Maintains records for retention periods required by law, professional standards, and according to SCCCMHA policy/administrative procedure.
6. Does not alter or destroy an entry in a record, but rather designates it as an error while leaving the original entry intact and create and maintain a new entry showing the correct data.
7. Permits individuals, guardian, or parent of minor individual access to their records, within 30 days of the request, except when access would be detrimental to the individual under therapeutic exception in the Mental Health Code.
8. Provides individuals receiving services, guardian, or parent of a minor individual after having gained access to treatment records an opportunity to request correction of inaccurate data in their records in accordance with the law.
9. Ensures that faxing of PHI is done in accordance with the HIPAA guidelines as noted in the Standards section within this administrative procedure, and the requirements of the HITECH Act of the American Recovery and Reinvestment Act (ARRA) of 2009.
10. Reports all improper disclosures of PHI to the SCCCMHA Privacy Officer and follows the Corporate Compliance Complaint, Investigation & Reporting Process policy #01-002-0020.

B. **Breaches**

Staff/Person Discovering Breach

1. Counts day one of discovery as the first day, when breach is known to SCCCMHA, or would have been known to SCCCMHA or any person, other than the person committing the breach, who is a workforce member or agent of SCCCMHA.
2. Notifies Supervisor, Chief Executive Officer or the SCCCMHA Privacy Officer, when believes that individual information has been used or disclosed in any way that compromises the security or privacy of that information.
3. Reports their good faith belief of any violation of the SCCCMHA Corporate Compliance Program.

CHAPTER	CHAPTER	SECTION	SUBJECT
Information Management	08	002	0006
SECTION	**SUBJECT**		
Data Management	Health Care Information – Privacy Measures (HIPAA)		

C. **Breach Investigation**

SCCCMHA Privacy Officer

1. Acts as the lead investigator of the breach and shall be responsible for the management of the breach investigation, completion of the risk assessment, and coordinating with others at SCCCMHA as appropriate (e.g., administration, information technology, human resources, risk management, public relations, and legal counsel). SCCCMHA Privacy Officer shall be the key facilitator for all breach notification processes.
2. Documents the Risk Assessment and the outcome of the Risk Assessment Process. Based on the outcome of the Risk Assessment, SCCCMHA will determine the need to move forward with breach notification. All documentation related to the breach investigation, including the Risk Assessment, must be retained for a minimum of ten years.

D. **Notification to Individuals Affected by Breach**

SCCCMHA Privacy Officer

1. Sends SCCCMHA standard breach notification to all affected individuals (Exhibit B). NOTE: SCCCMHA also has the discretion to provide notification following an unauthorized use or disclosure of PHI without performing a risk assessment.

2. Maintains a copy of all individual's correspondences required by state and federal law record retention requirements.

E. **Notification to Regulatory Agencies and Media**

SCCCMHA Privacy Officer

1. Notifies and collaborates with Michigan Department of Health and Human Services (MDHHS) to mitigate the breach and provides a plan of correction to prevent further unauthorized uses or disclosure of PHI (Exhibit C).
2. Notifies U.S. Department of Health and Human Services (DHHS) when breach of unsecured PHI affects 500 or more individuals served by SCCCMHA. Sends notification letter simultaneously with individual notifications (Exhibit D).
   a. Maintains a log, if less than 500 of SCCCMHA's individuals are affected, of the breaches to be submitted annually to the Secretary of MDHHS no later than 60 days after the end of each calendar year (Exhibit F).
3. Notifies, within 60 calendar days, prominent media outlets via press release, when 500 or more residents of a state, are affected by a breach of PHI (Exhibit E).

CHAPTER	CHAPTER	SECTION	SUBJECT
Information Management	08	002	0006
SECTION	**SUBJECT**		
Data Management	Health Care Information – Privacy Measures (HIPAA)		

F. **Business Associates Responsibilities Regarding Breach**

Business Associate

1. Notifies SCCCMHA's Chief Executive Officer without unreasonable delay, within 15 calendar days, after discovery of a breach of unsecured PHI. Such notice shall include the identification of each individual whose unsecured PHI or is believed to have be impermissible, accessed, acquired, used or disclosed.
2. Provides SCCCMHA with all available information required by SCCCMHA for notification to the individual served. SCCCMHA shall be responsible for notifying individuals affected by the breach unless it has been previously agreed that the business associate will send out necessary notifications.

VI. REFERENCES:

A. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
B. Privacy Standards 45 CFR Parts 160 & 164
C. HITECH Act of the American Recovery and Reinvestment Act (ARRA) of 2009
D. Release of Case Record Information administrative procedure #03-002-0030
E. ,Informed Consent administrative procedure #05-002-0006
F. Personnel: Corrective/Disciplinary Action discipline administrative procedure #06-001-0055
G. Corporate Compliance Complaint, Investigation & Reporting Process policy #01-002-0020
H. Mental Health Code, Sections 330.1748 and 330.1749

Note: Other security measures can be found in other SCCCMHA policies/administrative procedure.

VII. EXHIBITS:

A. HIPAA Compliance/HITECH Act Notification
B. SCCCMHA Breach Notification Individual Letter Template
C. SCCCMHA Breach Notification MDHHS Letter Template
D. SCCCMHA Breach Notification HHS Letter Template
E. SCCCMHA Breach Notification Media Release Template
F. SCCCMHA Unsecured PHI Breach Log

VII. REVISION HISTORY:

Dates issued 06/02, 10/04, 06/08, 04/10, 09/12, 11/13, 03/15, 03/16, 03/17, 03/18, 03/19, 07/20, 09/22, 09/23.

EXHIBIT A

HIPAA COMPLIANCE / HITECH ACT NOTIFICATION

Background:

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009. This act has many provisions and applies to entities and their Business Associates. In particular, it requires HIPAA Covered Entities to notify any discovery of a breach of unsecured Protected Health Information (PHI). If disclosure involves electronically transmitted PHI, it must be transmitted in a manner that meets the HIPAA security regulations and the breach notification provisions of the HITECH Act. A Business Associate of a Covered Entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses unsecured PHI shall, following the discovery of a breach of such information, notify the Covered Entity of such breach. Notification requirements, methods and exceptions are listed in the HITECH Act of the American Recovery and Reinvestment Act of 2009. Business Associates / Contractors mush comply with the new laws, and should become familiar minimally with the procedures, methods, risk assessments, and notification processes.

Definitions all Employees & Business Associates / Contractors should know:

- Protected Health Information (PHI) – Means individually identifiable health information (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium (45 CFR 160.103).
- Breach – In general, means the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of the PHI.

Now What?

- Breach Occurs – If you suspect or discover that a breach of PHI occurs, notify your designated Compliance Officer and Supervisor *immediately.*
- Give Notice – The Compliance Office will provide notice to the appropriate individuals.

Recommended Reading:

- The Health Insurance Portability & Accountability Act of 1996 (HIPAA)
- HITECH Act of the American Recovery and Reinvestment Act (ARRA) of 2009
- 45 CFR Parts 160 and 164

Corporate Compliance Offices

Fines for unauthorized disclosure under the HITECH Act vary depending on the violation. For each violation, the fines can range from $100 to a maximum penalty of $1.5 million for all violations of an identical provision. ***Disclose information in any format with great caution.***

Lapeer CMH
Lisa Ruddy
(810) 245-8550
lruddy@lapeercmh.org

Sanilac CMH
Beth Westover
(810) 648-0330
bwestover@sanilaccmh.org

St. Clair CMH
Tracey Pingitore
(810) 966-7836
tpingitore@scccmh.org

SUD Network
Kristen Potthoff
(810) 966-3399
potthoff@region10pihp.org

St. Clair County Community Mental Health Authority

Promoting Discovery & Recovery Opportunities for Healthy Minds & Bodies

Debra Johnson
Chief Executive Officer

Brandon Moore, MD
Medical Director

Nancy Thomson
Board Chairman

[Date]

[Name]
[Address]

Re: Notice of Unauthorized Disclosure

Dear [Patient Name (or guardian, if applicable)]:

St. Clair County Community Mental Health Authority ("SCCCMHA") is writing to make you aware of a recent incident that may affect the security of your [or your ward's] personal information. We take patient privacy very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so. As you know, SCCCMHA is a provider of healthcare services.

What Happened? On or about [Date] SCCCMHA became aware that [describe breach event]. Upon discovery, SCCCMHA launched an investigation to determine [focus of investigation]. The investigation determined [results of investigation and identification of breach]. There have thus far been no findings to indicate any misuse of patient data beyond the unauthorized access [include this sentence if applicable].

What Information was Involved? [List what protected health information was breached.]

What Are We Doing? We take the security of information that our patients entrust in us very seriously. Upon our investigation's confirmation of [list how breach occurred and corrective action taken immediately and all future plans for securing PHI]. As part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and security measures to enhance the privacy and security of information in our systems [include this sentence if applicable]. In addition to providing this notice to you, we are providing notice to Region 10 PIHP and the U.S. Department of Health and Human Services.

We want to make sure you have the information you need so that you can take steps to help protect yourself from identity theft. We encourage you to remain vigilant and to regularly review and monitor relevant account statements and credit reports and report suspected incidents of identity theft to local law enforcement, your state's Attorney General, or the Federal Trade Commission (the "FTC"). We have included more information on these steps in this letter.

What Can You Do? You can review the enclosed Steps You Can Take to Protect Your Information for additional information on how to better protect against identify theft and fraud.

For More Information. We are genuinely sorry that this incident occurred and sincerely apologize for any inconvenience this matter may cause you. St. Clair County Community Mental Health Authority is committed to providing quality care, including protecting your personal information, and we want to assure you that we are doing everything we can to protect you and your information and to minimize any recurrence of this situation. If you have questions about this notice or this incident or require further assistance, you can reach Tracey Pingitore, Privacy Officer, at 3111 Electric Avenue, Port Huron, MI 48060, 810-985-8900 between the hours of 8:30 a.m. and 5:00 p.m. (ET) or you can send an email to tpingitore@scccmh.org. Please reference this letter when contacting us.

Again, we sincerely apologize for any inconvenience this may cause.

Respectfully,

Debra Johnson
Chief Executive Officer

Encl.

St. Clair County Community Mental Health Authority
Promoting Discovery & Recovery Opportunities for Healthy Minds & Bodies

Debra Johnson
Chief Executive Officer

Brandon Moore, MD
Medical Director

Nancy Thomson
Board Chairman

[Date]

Michigan Dept. of Health and Human Services
333 S. Grand Avenue
P.O. Box 30195
Lansing, MI 48909

Re: Notice of Unauthorized Disclosure

Dear Bureau Personnel:

St. Clair County Community Mental Health Authority ("SCCCMHA") is writing to make you aware of a recent incident that may affect the security of SCCCMHA individual personal information.

What Happened? On or about [Date] SCCCMHA became aware that [describe breach event]. Upon discovery, SCCCMHA launched an investigation to determine [focus of investigation]. The investigation determined [results of investigation and identification of breach]. There have thus far been no findings to indicate any misuse of patient data beyond the unauthorized access [include this sentence if applicable].

What Information was Involved? [List what protected health information was breached.]

What Are We Doing? We take the security of information that our patients entrust in us very seriously. Upon our investigation's confirmation of [list how breach occurred and corrective action taken immediately and all future plans for securing PHI]. As part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and security measures to enhance the privacy and security of information in our systems [include this sentence if applicable]. In addition to providing this notice to MDHHS, we are providing notice to Region 10 PIHP and to all individual individuals we serve.

For More Information. St. Clair County Community Mental Health Authority is committed to providing quality care, including protecting personal information, and we want to ensure that we are doing everything we can to protect private health information and to minimize any recurrence of this situation.

If you have questions about this notice or this incident or require further assistance, you can reach Tracey Pingitore, Privacy Officer, at 3111 Electric Avenue, Port Huron, MI 48060, 810-985-8900 between the hours of 8:30 a.m. and 5:00 p.m. (ET) or you can send an email to tpingitore@scccmh.org. Please reference this letter when contacting us.

Respectfully,

Debra Johnson
Chief Executive Officer

St. Clair County Community Mental Health Authority

Promoting Discovery & Recovery Opportunities for Healthy Minds & Bodies

Debra Johnson
Chief Executive Officer

Brandon Moore, MD
Medical Director

Nancy Thomson
Board Chairman

[Date]

U.S. Dept. of Health and Human Services
200 Independence Avenue, S.W., Room 336E
Washington, D.C. 20201

Re: Notice of Unauthorized Disclosure

Dear Bureau Personnel:

St. Clair County Community Mental Health Authority ("SCCCMHA") is writing to make you aware of a recent incident that may affect the security of SCCCMHA individual personal information.

What Happened? On or about [Date] SCCCMHA became aware that [describe breach event]. Upon discovery, SCCCMHA launched an investigation to determine [focus of investigation]. The investigation determined [results of investigation and identification of breach]. There have thus far been no findings to indicate any misuse of patient data beyond the unauthorized access [include this sentence if applicable].

What Information was Involved? [List what protected health information was breached.]

What Are We Doing? We take the security of information that our patients entrust in us very seriously. Upon our investigation's confirmation of [list how breach occurred and corrective action taken immediately and all future plans for securing PHI]. As part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and security measures to enhance the privacy and security of information in our systems [include this sentence if applicable]. In addition to providing this notice to U.S. HHS, we are providing notice to MDHHS, Region 10 PIHP, and to all individual individuals we serve.

For More Information. St. Clair County Community Mental Health Authority is committed to providing quality care, including protecting personal information, and we want to ensure that we are doing everything we can to protect private health information and to minimize any recurrence of this situation.

If you have questions about this notice or this incident or require further assistance, you can reach Tracey Pingitore, Privacy Officer, at 3111 Electric Avenue, Port Huron, MI 48060, 810-985-8900 between the hours of 8:30 a.m. and 5:00 p.m. (ET) or you can send an email to tpingitore@scccmh.org. Please reference this letter when contacting us.

Respectfully,

Debra Johnson
Chief Executive Officer

EXHIBIT E

Tracey Pingitore, Privacy Officer
St. Clair County Community Mental Health
Contact: 810-985-8900
tpingitore@scccmh.org

MEDIA NOTIFICATION—FOR IMMEDIATE RELEASE

SCCCMHA NOTIFIES PATIENTS OF SECURITY BREACH INCIDENT

P1: (Port Huron, Michigan-Date of Report) What SCCCMHA is announcing.

P2: Statement by designated SCCCMHA spokesperson.

P3: Description of security breach.

P4: Description of what information the breach includes.

P5: Resolution to security breach.

EXHIBIT F

St. Clair County Community Mental Health Authority Unsecured PHI Breach Log					
Updated:					
Date of Breach	**Date of Discovery of Breach**	**Number of Individuals Affected**	**Information that was Breached**	**How Individuals Were Notified**	**Mitigation and Prevention**