V.E.

ST. CLAIR COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

Date Issued 06/02
Date Revised 10/04;06/08;04/10;09/12;11/13;03/15;03/16;
03/17;03/18;03/19

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** ~~Mike Medrano~~Tommy Rankin		**AUTHORIZED BY** Tracey Pingitore	

I. APPLICATION:

- ☐ SCCCMHA Board
- ☒ SCCCMHA Provider & Sub-Contractors
- ☒ Direct Operated Programs
- ☒ Community Agency Program
- ☒ Residential Programs
- ☒ Specialized Foster Care
- ☐ SUD Providers

II. POLICY STATEMENT:

It is the policy of the St. Clair County Community Mental Health Authority (SCCCMHA) that all personnel must preserve the integrity and the confidentiality of client information.

III. DEFINITIONS:

A. Breach: "Breach" in general means the unauthorized acquisition, access, use, or disclosure of protected health information ~~which~~ that compromises the security or privacy of such information. The breach must not only constitute a violation of the HIPAA Privacy Rule, but must also pose a significant risk of financial, reputational, or other harm to the individual. Exceptions to the term "breach" are listed in Title XIII of Division A, Subtitle D, section 14300 of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111-5).

B. Business Associate: "Business Associate" shall mean an individual, group or agency with whom St. Clair County Community Mental Health Authority has a relationship and the Business Associate role is that of a non-covered entity and Protected Health Information is shared as part of doing business.

C. Covered Entity: "Covered Entity" shall mean St. Clair County Community Mental Health Authority.

D. Health Information: "Health Information" means any 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.

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

E. Individual: "Individual" shall have the same meaning as the term "individual" in 45 CFR § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502 (g).

F. Privacy Rule: "Privacy Rule" shall mean 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. Required By Law: "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR §164.501.

I. Unsecured Protected Health Information: "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 such information is not unsecured.

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.

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. Protected health information will only be used to provide proper diagnosis and treatment; with the individual's knowledge 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 protected health information.

D. Protected health information collected must be accurate, timely, complete, and available when needed.

E. All staff will store protected health information in a secure fashion; log off or lock workstations when not in use; encrypt all electronic communications which include protected health

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

information; password protect and lock mobile devices when not in use; secure material away when not being worked on; secure interoffice mail in confidential envelopes; put away protected health information when left temporarily; will not leave visitors unattended in staff only areas; will not leave protected health information unattended and will not routinely fax any individual identifiable health information. 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 protected health information to another party. The HIPAA Privacy Rule does permit physicians to disclose protected health information to another health care provider for treatment purposes. This can be done by secure fax or other means. Covered entities must have in place reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information 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. 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. To request a release of information, follow policy #03-002-0030, Release of Case Record Information. Take appropriate steps to prevent unauthorized disclosures, such as specifying that the recipient of the protected health information 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.

G. Acknowledgement by the individual or guardian of receipt of the Privacy Notice Brochure is covered under the annual Informed Consent policy, #05-002-0006.

H. Violation of this policy is grounds for disciplinary action, up to and including termination of employment in accordance with SCCCMHA's discipline policy.

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

I. All electronic transmissions of protected health care information must be encrypted to meet the security regulations of HIPAA and the HITECH Act of the American Recovery and Reinvestment Act (ARRA) of 2009.

J. SCCCMHA designates the Associate Director of Administration as its Privacy Officer.

V. PROCEDURES:

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.

6. Does not alter nor destroy an entry in a record, but rather designate 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. Reports all improper disclosures of protected health care information to the Privacy Officer and follows policy #01-002-0020, "Corporate Compliance Complaint, Investigation & Reporting Process."

10. Ensures that faxing of protected health information is done in accordance with the HIPAA guidelines as noted in the Standards section within this policy, and the requirements of the HITECH Act of the American Recovery and Reinvestment Act (ARRA) of 2009.

VI. REFERENCES:

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

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. #03-002-0030 "Release of Case Record Information" policy#05-002-0006 "Informed Consent" policy
E. Corporate Compliance policy #01-002-0020 "Corporate Compliance Complaint, Investigation & Reporting Process"
F. Mental Health Code, Sections 330.1748 and 330.1749

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

VII. EXHIBITS:

A. HIPAA Compliance/HITECH Act Notification

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:

- Breach – in general means the unauthorized acquisition, access, use, or disclosure of Protected Health Information. The breach must not only constitute a violation of HIPAA, but must also pose a significant risk of financial, reputational, or other harm to the individual to trigger the notice requirement. (Title XIII of Division A, Subtitle D, section 14300 of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111-5)).
- 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).

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

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
Lauren Emmons
(810) 667-0500
lemmons@lapeercounty.org

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

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

SUD Network
Todd Anglebrandt
(810) 667-0243
tanglebrandt@lapeercounty.org