Community Mental Health Partnership of Southeast Michigan/PIHP	Policy and Procedure Privacy and Security of Workstations and Electronic Communication
Department: EOC	**Local Policy Number (if used)**
Regional Operations Committee Approval Date 3/22/2021	**Implementation Date 3/22/2021**

I. PURPOSE

This policy establishes standards to ensure the confidentiality and security of protected health information (PHI) in the work environment/ an individual's workstation and when using electronic/technology-based forms of communication.

II. REVISION HISTORY

DATE	REV. NO.	MODIFICATION
1/15/2008		
5/12/2010		
8/11/2014		Revised to reflect the new regional entity.
3/22/2021		Reviewed and Updated by EOC

III. APPLICATION

This policy applies to all staff, students, volunteers and contractual organizations within the provider network of the Community Mental Health Partnership of Southeast Michigan (CMHPSM).

IV. POLICY

It is the policy of the Community Mental Health Partnership of Southeast Michigan (CMHPSM) that all communications about or with consumers will be conducted in ways that ensure appropriate privacy and security.

It is the policy of the CMHPSM that consumers, their legal representatives, and families shall be informed of their rights to confidentiality when using electronic/technology-based forms of communication.

V. DEFINITIONS

Cloud Storage: Use of data storage space that is hosted by an entity external to the employer.

Computer-Mediated Communication (CMC): Any communicative transaction that occurs through the use of networked electronic equipment (computers, tablets, etc…). While the term has traditionally referred to those communications that occur via computer-mediated formats (instant messages, emails, chat rooms, etc…), it has also been applied to other forms of text-based interaction such as text messaging and social

networking supported by social software. For the purposes of this policy, the definition of CMC will include activities such as texting and social networking in all its present and future forms that do not meet HIPAA/HITECH privacy and security standards. Telemedicine and videoconferencing are not considered computer-mediated communication, and therefore not prohibited from use by this policy.

Community Mental Health Partnership of Southeast Michigan (CMHPSM): The Regional Entity that serves as the PIHP for Lenawee, Livingston, Monroe and Washtenaw for mental health, developmental disabilities, and substance use disorder services.

Community Mental Health Services Program (CMHSP): A program operated under chapter 2 of the Mental Health Code as a county community mental health agency, a community mental health authority, or a community mental health organization.

E-Mail: or email, is short for "electronic mail" and is a method of composing, sending, and receiving messages over electronic communication systems. Most e-mail systems today use the internet.

Legal Representative: For the purposes of this specific policy, a legal representative is defined as any of the following:

1. A court-appointed guardian,
2. A parent with legal custody of a minor consumer/recipient,
3. In the case of a deceased consumer/recipient, the executor of the estate or court appointed personal representative,
4. A patient advocate under a durable power of attorney or other advanced directive.

Portable Storage Device: Any device that allows the storage of data and can be physically removed from a secure location.

Regional Entity: The entity established under section 204b of the Michigan Mental Health Code to provide specialty services and supports for people with mental health, developmental disabilities, and substance use disorder needs.

Text messaging: also known as “texting,” refers to use of a texting application to exchange of written messages between mobile devices. While the term most often refers to messages sent using the Short Message Service (SMS), it has been extended to include messages containing image, video, and sound content (known as MMS messages). Individual messages are referred to as “text messages” or “texts.”

Social Networking: an online service, platform, or site that focuses on building and reflecting of social networks or social relations among people who share interests and/or activities. A social network service essentially consists of a representation of each user (often a profile), his/her social links, and a variety of additional services. Most social network services are web based and provide means for users to interact over the internet, such as e-mail and instant messaging. Social network service usually means an individual-centered service whereas online community services are group-centered, and can also include online community services.

VI. STANDARDS

Immediately report any violations of this policy to their supervisor and the Privacy Officer or the Office of Recipient Rights

A. Work Station:

Protected health information may be stored on a workstation, and therefore the information should be secured as follows:

1. The agency shall have processes in place to back-up data to a secure storage location in the event of environmental threats, such as fire, water damage, power surges, etc.
2. Any computer equipment, including portable equipment, must require user log-in and access should be appropriate to that user's job functions.
3. All staff must ensure that protected health information at their workstation, such as computer screens, written documents, etc., is visible only to those who have a "need to know."
4. Each computer shall be programmed to generate a screen saver when the computer receives no input for a specified period.
5. Users must log off the system or lock the workstation if he or she leaves the computer terminal for any period of time.

B. Electronic Equipment Protection (computers, tablets, phones, etc.)

1. All staff shall monitor the computers' operating environment by reporting to their supervisor or other specified staff any potential threats to their work-related electronic equipment.
2. All electronic equipment plugged into an electrical power outlet shall use a surge suppresser approved by local information technology staff (IT). Workstations missing an approved surge protector will be reported to IT.
3. All persons shall take appropriate measures to protect electronic equipment from damage due to food or drink.
4. If IT has reason to suspect that security is compromised, they shall issue new passwords to employees.
5. No individual may download any software without express written permission of IT. This rule is necessary to protect against the transmission of computer viruses into the facility's system.

C. Security

1. Each person shall set up a unique password that is updated at specific intervals based on local requirements.
2. If a person believes his/her password has been compromised, he/she will immediately change his/her password.
3. Persons logging onto the system ~~shall~~ ensure that no one observes the entry of his/her password.
4. Individuals shall not log onto the system using another's password.
5. Individuals shall not permit another to log on with his/her password, including ensuring that their password is not auto-saved on any electronic device
6. Individuals shall not enter data under another person's password.
7. Individuals using the computer system shall not write down his/her password and place it at or near the terminal, such as putting his/her password on a note on the screen or under the keyboard.
8. Any electronic equipment used to perform work functions shall be password protected to prevent any non-authorized use.

9. No person may hide his or her identity as the author of the entry or represent that someone else entered the data or sent the message.
10. Individuals must not leave printers/copiers unattended when they are printing confidential consumer or other information if the printer/copier is in an area where unauthorized individuals have access to the printer.
11. No person may access any confidential consumer or other information unless he/she has a need to know. The "need to know" is the minimum information needed to do his/her job.
12. No person may disclose confidential consumer or other information unless properly authorized (see the CMHPSM Confidentiality and Access to Clinical Records Policy).

D. Cloud and Portable Storage

1. Protected health information (PHI) should be stored in a secured location, where it is password-protected, regularly backed up, and maintained by the employer.
2. No individual may store PHI on any portable or cloud-based storage mechanism without prior supervisory authorization.

E. E-mail

1. Electronic mail privacy protections shall be comparable to that which is traditionally afforded to paper mail and telephone communications, in that the use of information through email about consumers/any Protected Health Information (PHI) that is allowable in this policy is protected as private and confidential.
2. Email that is not encrypted and protected in accordance with HIPAA, HITECH, and NIST (National Institute of Standards and Technology) requirements, is not secure and the confidentiality of e-mail exchanges cannot be fully guaranteed.
3. Email communication between staff within the same domain may be used for administrative and operational purposes. Consumer identifiers should be limited to those identified in Section E. 8.
4. As government entities, Community Mental Health Authorities are subject to Freedom of Information Act (FOIA) and as such the protection of email exchanges cannot be fully guaranteed. Therefore, e-mail shall not be used between staff/volunteers to communicate detailed confidential matters about consumers, including attachments to emails, outside he allowable scope of this policy (see E 5, 7 and 8 for more specifics).
5. Email communication in any form/level of detail shall not be used between staff and consumers/legal representatives; the only exception to such communication would be reasonable accommodation as defined in E. 9,10, and 11 in this policy.
6. Email communication in any form/level of detail about consumers shall not be used between staff and the community/general public for any reason.
7. Do not use any identifying information by which a 3rd party might be able to deduce the identity of the client.
8. Staff may:
    a. use the case number
    b. use the initials only
    c. use both case number & initials
9. A consumer or legal representative, who has a disability that precludes all other forms of communication except e-mail, may request e-mail communication as a reasonable accommodation when face-to-face or other forms of contact are not

an option. However, in no situation is e-mail to be used to replace therapeutic face-to-face contacts.

10. In situations where email is used for consumers meeting reasonable accommodation standards, electronic mail should be made a part of the clinical record. Staff will immediately delete the e-mail from inbox and trash folders. Staff should note that even after deleted from the trash, this email may still be retrieved or restored.
11. Staff shall give or mail the agency's "Electronic Statement of Understanding" to the consumer/parent/guardian for signature and inclusion in the consumer's clinical record.

F. Facsimile/Fax

1. Staff may transmit health records by facsimile when expediency is in the best interest of the consumer, when needed for continuity of consumer care, or when required by a third-party payer.
2. Staff shall limit information transmitted to that necessary to meet the requester's needs.
3. Except as authorized by law, a properly completed and signed release of information shall be obtained before sharing consumer information.
4. The cover page accompanying the facsimile transmission shall include:
   a. a fax transmittal receipt or stamp
   b. a confidentiality notice attached to this policy as Attachment A.
5. Protected information shall be faxed to a specific person rather than to an office number with no addressee noted.
6. Staff shall make reasonable efforts to ensure that they send the facsimile transmission to the correct destination. Staff will save frequently used numbers on the machine to prevent misdialing errors.
7. For a new consumer, the sender shall verify the fax number before sending the facsimile and verify the consumer's authority to receive confidential information. Fax machines shall be in secure areas, and the department director/designee is responsible for limiting access to them.
8. Each department is responsible for ensuring that incoming faxes are properly handled, and not left sitting on or near the machine. Faxes should be distributed to the proper consumer expeditiously while protecting confidentiality during distribution, as by enclosing the fax in an envelope as needed.
9. Staff must report any misdirected faxes to their immediate supervisor and privacy officer/Office of Recipient Rights.
10. Supervisors or Administrative Assistants shall periodically or randomly direct a check of all speed-dial numbers to ensure their currency, validity, accuracy, and authorization to receive confidential information.
11. All staff is responsible for immediately reporting violations of this policy to their Supervisor and to the privacy officer.

G. Computer-Mediated Communication (CMC)/Text Messaging/Social Networking

1. Any form of Computer-Mediated Communication CMC/text messaging is not considered secure and as such shall not be used by any staff, students, or volunteers to communicate with or about consumers. This includes communication with consumers, anyone with whom information about consumers can legally be discussed (e.g. written consent, business agreements, contractual arrangements, or legal representatives), or anyone in the general public.

2. CMC in the form of online social networking (i.e. Facebook, Twitter, MySpace, etc) is not considered secure and as such shall not be used by any staff, students, or volunteers to communicate with or about consumers. This includes communication with consumers, anyone with whom information about consumers can legally be discussed (e.g. written consent, business agreements, contractual arrangements, or legal representatives) or anyone in the general public.
3. Use of social media to provide one-way general information from a CMHSP/provider about the agency, behavioral health services, or resource information to the public is allowable. Such use of social media shall prohibit public discussion/interaction about any information related to PHI or confidentiality.
4. Whether staff, students, or volunteers can use CMC for staff-to-staff or personal use is not a component of this policy and is to be determined locally by each CMHSP/provider.
5. Any violation of the use of CMC/text messaging/social networking shall be immediately reported to a supervisor and to the privacy officer.

H. Virtual Services
1. Regional entities may provide telemedicine services to provide consumer services, as Identified through MDHHS service provisions and guidance.
2. If at anytime MDHHS or CMS prohibit the use of teleservices the CMHPSM and its regional partners will comply with that request within the appropriate timeframe provided.
3. Virtual group services allow consumers to opt not to disclose their full name for video access to other participants in group services.
4. Telemedicine platforms utilized with the CMHPSM region will utilize access controls (Passcodes, waiting room, EG) to ensure protection of confidentiality.

VII. EXHIBITS

A. Electronic Mail (E-mail) Statement of Understanding
B. Fax Confidentiality Statement

VIII. REFERENCES

Reference:	Check if applies:	Standard Numbers:
42 CFR Parts 400 et al. Medicaid Managed Care Rules.	X	438.100(d)
45 CFR Parts 160 & 164 (HIPPA)	X	
42 CFR Part 2 (Substance Abuse)	X	
HITECH Act of 2009	X	
Michigan Mental Health Code Act 258 of 1974	X	330.1748
The Joint Commission- Behavioral Health Standards	X	
MDCH PIHP Contract	X	
MDCH CMHSP Contract	X	

CMHSPM Confidentiality and Access to Clinical Records Policy	X	
CMHPSM Sanctions for Breaches of Security or Confidentiality Policy	X	

IX. PROCEDURES

NONE

Attachment A

CONSUMER REQUEST FOR REASONABLE ACCOMMODATIONS
ELECTRONIC MAIL (E-MAIL)
STATEMENT OF UNDERSTANDING

(INSERT ORGANIZATION NAME)
INSERT ADDRESS
Phone: (Insert Number)
Fax: (Insert Number)

I,_____ , am requesting reasonable accommodation in communicating by electronic mail (e-mail) with staff at (INSERT ORGANIZATION NAME). I understand that e-mail will be used as a form of communication about my care/services, but in no situation can e-mail to be used to replace therapeutic face-to-face contacts.

In signing this request I also understand that my confidentiality cannot be assured if I choose to communicate by electronic mail (e-mail) with staff at the (INSERT ORGANIZATION NAME).

_____ _____
Client Signature Date

_____ _____
Parent/Guardian Signature Date

_____ _____
Witness Signature Date

Attachment B

The information contained in this facsimile message is legally privileged and confidential information only for the use of the individual or entity named above. If the reader of this message is not the intended consumer, you are hereby notified that any dissemination, distribution, or copy of this telecopy is strictly prohibited. If you have received this telecopy in error, please notify us by telephone immediately. Thank you.

(INSERT ORGANIZATION NAME)
INSERT ADDRESS
Phone: (Insert Number)
Fax: (Insert Number)