

<b>WCHO PIHP Policy for the COMMUNITY MENTAL HEALTH PARTNERSHIP OF SOUTHEASTERN MICHIGAN</b>	<b>Policy and Procedure Privacy and Security of Workstations and Electronic Communication</b>
Department: Corporate Compliance Author: CJ Witherow	Local Policy Number (if used)
Approval Date 3/15/11	Implementation Date 3/31/11

**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 such as email, facsimile, text messaging, and/or computer-mediated communication (CMC).

**II. REVISION HISTORY**

DATE	REV. NO.	MODIFICATION
1/15/08		
5/12/10		

**III. PERSONS AFFECTED**

This policy applies to all WCHO, CSSN and staff within the Community Mental Health Partnership of Southeast Michigan (CMHPSM) including students, volunteers, and those providers/ organizations under contract with affiliation members.

**IV. POLICY**

It is the policy of the WCHO as the PIHP, and of the Community Mental Health Partnership of Southeast Michigan (CMHPSM), that all communications about or with consumers will be conducted in ways protected

**V. DEFINITIONS**

Computer-Mediated Communication (CMC): any communicative transaction that occurs through the use of two or more networked computers. While the term has traditionally referred to those communications that occur via computer-mediated formats (e.g., instant messages, emails, chat rooms), 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.

Community Mental Health Partnership of Southeast Michigan (CMHPSM) - An affiliation of the mental health boards for the Counties of Lenawee, Livingston, Monroe, and Washtenaw.

Comprehensive Specialty Services Network (CSSN) – An organization that is certified as a CMHSP, including a recipient rights system, services across all populations, has a publicly appointed Board of Directors, and has accreditation from an accrediting 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 recipient,
3. In the case of a deceased 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.

Text messaging: also known as "texting", refers to the exchange of brief written messages between mobile phones over cellular networks. While the term most often refers to message 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, e.g., 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. RESPONSIBILITIES**

It is the responsibility of all staff, students, and volunteers to:

- Abide by all elements of this policy.
- Ensure consumers, their legal representatives, and families are informed of their rights to confidentiality when using electronic/technology-based forms of communication such as email, facsimile, text messaging, and/or computer-mediated communication (CMC).
- Immediately report any violations of this policy to their supervisor and the Privacy Officer or the Office of Recipient Rights

## **VII. STANDARDS**

### **A. Work Station:**

The information available in workstations is confidential and shall be kept secure because of the factors listed below:

1. It is assumed that every computer workstation in the facility is vulnerable to environmental threats, such as fire, water damage, power surges, and the like.
2. Any computer equipment, including portable equipment, in the facility can access confidential consumer information if the user has the proper authorizations.
3. All computer screens may be visible to individuals who do not have access to confidential information that may appear on the screen.

#### **B. Computer Equipment Protection**

1. All computer users shall monitor the computers' operating environment by reporting to their supervisor or other specified staff any potential threats to the computer.
2. All computers plugged into an electrical power outlet shall use a surge suppresser approved by the Information Management (IM) department. Workstations missing an approved surge protector will be reported to IT.
3. All persons using computers shall take appropriate measures to protect the workstation from damage due to food or drink.
4. If systems administration 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. Logging onto the System**

1. Each person shall set up a unique password. Good practice is to change one's password on a regular basis. If a person believes his/her password has been compromised, he/she shall immediately change his/her password. Persons logging onto the system shall ensure that no one observes the entry of his/her password.
2. Individuals shall not log onto the system using another's password.
3. Individuals shall not permit another to log on with his/her password.
4. Individuals shall not enter data under another person's password.
5. 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.

#### **D. Security**

Each person using a facility's computers is responsible for knowing and practicing the following:

1. 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.
2. Portable computer devices shall have Security passwords.

#### **E. Confidentiality**

Each person using a facility's computers is responsible for knowing and practicing the following:

1. 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.
2. No person may disclose confidential consumer or other information unless properly authorized (see the CMHPSM Confidentiality and Access to Clinical Records Policy)
3. Individuals must not leave printers unattended when they are printing confidential consumer or other information if the printer is in an area where unauthorized individuals have access to the printer.

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.

**F. Transfer of Data to Non-secure Area**

1. The most secure data is that which is on the individual's personal network drive.
2. No individual may transfer consumer or confidential data from the system onto diskette, CD, hard drive, fax or scanner, any network drive or any other hardware, software without authorization.

**G. 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. Therefore, e-mail shall not be used between staff/volunteers to communicate detailed confidential matters about consumers, including attachments to emails, outside the allowable scope of this policy (see G 4, 6 and 7 for more specifics).
3. 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 the allowable scope of this policy (see G 4, 6 and 7 for more specifics).
4. 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 G, 8,9, and 10 in this policy.
5. Email communication in any form/level of detail about consumers shall not be used between staff and the community/general public for any reason.
6. Do not use any identifying information by which a 3rd party might be able to deduce the identity of the client.
7. Staff may:
  - a. use the case number
  - b. use the initials only
  - c. use both case number & initials
8. 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.
9. In situations where email is used for consumers meeting reasonable accommodation standards, electronic mail should be printed and 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.
10. 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.

## **H. Facsimile/Fax**

1. Personnel 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. Personnel shall limit information transmitted to that necessary to meet the requester's needs.
3. Except as authorized by law, a properly completed and signed authorization shall be obtained before releasing 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. Personnel shall make reasonable efforts to ensure that they send the facsimile transmission to the correct destination. Personnel will preprogram frequently used numbers into the machine to prevent misdialing errors.
7. For a new recipient, the sender shall verify the fax number before sending the facsimile and verify the recipient'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 recipient expeditiously while protecting confidentiality during distribution, as by enclosing the fax in an envelope as needed.
9. Personnel must report any misdirected faxes to their immediate supervisor.
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 or to the Privacy Officer.

## **I. 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. 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 CSSN/provider.
4. Any violation of the use of CMC/text messaging/social networking shall be immediately reported to a supervisor and to the Privacy Officer.

**VIII. EXHIBITS**

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

**XI. REFERENCES**

<b>Reference:</b>	<b>Check if applies:</b>	<b>Standard Numbers:</b>
42 CFR Parts 400 et al. (Balanced Budget Act)	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, version 2009	X	330.1748
The Joint Commission- Behavioral Health Standards 09-10	X	
MDCH Medicaid Contract 09/10	X	
MDCH Substance Abuse Contract 09/10	X	
CMHSPM Confidentiality and Access to Clinical Records Policy	X	
CMHPSM Sanctions for Breaches of Security or Confidentiality Policy	X	

**XII. PROCEDURES**

NONE

**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 recipient, 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)