

COMMUNITY MENTAL HEALTH PARTNERSHIP OF SOUTHEASTERN MICHIGAN		<i>Policy and Procedure</i> <i>Email, Fax and Workstation Privacy and Security</i>	
Department: Compliance Author: Suzanne Kapica		Local Policy Number (if used)	
Revision Date	Approval Date	Implementation Date	
	1/15/08	2/15/08	
Archive Information			
Date:			
Reason:			

I. PURPOSE

To ensure the confidentiality and security of Protected Health Information (PHI) when using Email, Fax or an individual's Workstation.

II. POLICY

All Protected Health Information shall be kept confidential and secure as required by law, professional ethics and accreditation requirements.

III. APPLICATION

All WCHO, CSSN and CSSN Look-alike staff within the Community Mental Health Partnership of Southeast Michigan (CMHPSM) including students, volunteers, those of organizations under contract with affiliation members.

IV. DEFINITIONS

E-Mail: All electronic forms of communication that use the internet as its means of transmission.

V. STANDARDS

WORK STATION:

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

- A. 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.
- B. Any computer equipment, including portable equipment, in the facility can access confidential consumer information if the user has the proper authorizations.
- C. All computer screens may be visible to individuals who do not have access to confidential information that may appear on the screen.

Computer Equipment Protection

- A. All computer users shall monitor the computers' operating environment by reporting to their supervisor or other specified staff any potential threats to the computer.
- B. All computers plugged into an electrical power outlet shall use a surge suppresser approved by the Information and Technology department (IT). Workstations missing an approved surge protector will be reported to IT.
- C. All persons using computers shall take appropriate measures to protect the workstation from damage due to food or drink.
- D. If systems administration has reason to suspect that security is compromised they shall issue new passwords to employees.
- E. 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.

Logging onto the System

- A. 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.
- B. Individuals shall not log onto the system using another's password.
- C. Individuals shall not permit another to log on with his/her password.
- D. Individuals shall not enter data under another person's password.
- E. 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.

Security

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

- A. 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.
- B. Portable computer devices shall have Security passwords

Confidentiality

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

- A. 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.
- B. No person may disclose confidential consumer or other information unless properly authorized (see the Regional Confidentiality and Access to Clinical Records Policy)
- C. 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.
- D. Each computer shall be programmed to generate a screen saver when the computer receives no input for a specified period.
- E. Users must log off the system or lock the workstation if he or she leaves the computer terminal for any period of time.

Transfer of Data to Non-secure Area

- A. The most secure data is that which is on the individual's personal network drive.
- B. 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.

E-MAIL

- A. E-mail shall not be used to communicate confidential matters, including attachments to emails.
- B. Electronic mail privacy protections shall be comparable to that which is traditionally afforded to paper mail and telephone communications.
- C. Do not use any identifying information by which a 3rd party might be able to deduce the identity of the client.
Staff may:
 - a. use the case number
 - b. use the initials only
 - c. use both case number & initials
- D. A primary or secondary consumer (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.

1. Electronic mail in these situations should be printed and made a part of the clinical record. Staff will immediately delete the e-mail from in-box and trash folders. Staff should note that even after deleted from the trash, this email may still be retrieved or restored.
2. 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.

FAX

- A. 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.
- B. Personnel shall limit information transmitted to that necessary to meet the requester's needs.
- C. Except as authorized by law, a properly completed and signed authorization shall be obtained before releasing consumer information.
- D. The cover page accompanying the facsimile transmission shall include:
 - (1) a fax transmittal receipt or stamp
 - (2) a confidentiality notice attached to this policy as Attachment A.
- E. Protected information shall be faxed to a specific person rather than to an office number with no addressee noted.
- F. 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.
- G. 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.
- H. 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.
- I. Personnel must report any misdirected faxes to their immediate supervisor.
- J. 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.

- K. All staff is responsible for immediately reporting violations of this policy to their Supervisor or to the Privacy Officer.

VI. EXHIBITS

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

VII. REFERENCES

Reference:	Check if applies:	Standard Numbers:
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	
Michigan Mental Health Code Act 258 of 1974	X	330.1748
Joint Commission- Behavioral Health Standards 06-07	X	RI 2.130
MDCH Medicaid Contract 03-04	X	14.0, 15.0
MDCH Substance Abuse Contract (2006)	X	I. 1-7
Confidentiality and Access to Clinical Records Policy	X	
Sanctions for Breaches of Security or Confidentiality Policy	X	

VIII. PROCEDURES

None

Attachment A

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

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

I, _____, 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)

