Subject: ISM Workstation Use	**Accountability:** Information Technology	**Effective Date:** 1/1/2014	Pages: 4
REQUIRED BY: **BBA Section** 164.310 Physical Safeguards **PIHP Contract Section** _____ **NCQA/URAC Standard** _____ **SA SARF** _____ **Other** _____		Last Reviewed Date: 9/6/16	Past Reviewed Dates: 6/18/15
LINE OF BUSINESS: ☒ Specialty Waiver (B/C) ☒ I Waiver ☒ ABW Waiver ☒ SUD Medicaid ☒ SUD CA Block Grant ☐ OTHER: _____	**APPLICATION:** ☒ SWMBH Staff and Operations ☐ Participant CMHSPs ☐ SUD Providers ☐ MH / DD providers ☐ DD providers ☐ Other: _____	Last Revised Date: 9/6/16	Past Revised Dates: 6/18/15
Approved : Robert Moeland By: ROBERT MOELAND, CIO Date: 8-14-17		Required Reviewer: Chief Information Officer	

I. Purpose

To comply with Health Insurance Portability and Accountability Act (HIPAA) as well as to protect the confidentiality and integrity of confidential behavioral healthcare information as required by law, professional ethics and accreditation agencies.

II. Policy

Southwest Michigan Behavioral Health (SWMBH) shall protect the confidentiality and integrity of Protected Health Information (PHI) as related to workstation use and as required by law, professional ethics and accreditation requirements. Violation of this or any other SWMBH policy may result in disciplinary action up to and including termination of employment.

III. Standards and Guidelines

A. General Expectations

1. Users will be granted access to SWMBH workstations, based on need. Use of electronic resources at each workstation is limited by restrictions that apply to all SWMBH property and by constraints necessary for the reliable operation of electronic communications systems and services. The Information Technology Services (ITS) department reserves the right to deny use of electronic services when necessary to satisfy these restrictions and constraints.
2. The primary function of the equipment is to perform SWMBH business functions.
3. Any computer workstation in the organization can access confidential customer information if the employee has the proper authorization. Care must be taken by all computer users to ensure they do not jeopardize SWMBH or customer information.
4. Non Employees (persons and organizations that are not direct employees but are affiliated through program, contract, license relationships, etc.) may, as authorized by the Chief Information Officer, be eligible to use a SWMBH workstation or web portal for purposes of collaboration and communication.

5. Each computer will be programmed to generate a screen saver when the computer receives no input for a specified period.

B. User Responsibility
1. Employees may, as authorized by the Chief Information Officer, be eligible to use SWMBH's electronic resources and services for purposes in this section.
2. All Users must review and sign this policy prior to use of SWMBH's workstations and electronic resources.
3. All computer users will monitor the workstation's operating environment and immediately report potential threats to the computer and to the integrity and confidentiality of data contained in the computer system.
4. Personnel using the computer system will comply with the Passwords Requirements policy, SWMBH policy 17.3 (Password Requirements).
5. Users logging onto the system will ensure that no one observes the entry of their password. Personnel will neither log onto the system using another's password nor permit another to log on with their password. Nor will personnel enter data under another person's password. For additional information regarding logging onto the system see SWMBH policy 7.4 (Information Security).
6. Each person using SWMBH'S computers is responsible for the content of any data he or she inputs into the computer or transmits through or outside SWMBH'S system. 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. All personnel will familiarize themselves with and comply with SWMBH policy 7.3 (Internet Acceptable Use).
7. No employees may access any confidential customer or other information that they do not have a need to know. No employee may disclose confidential customer or other information unless properly authorized. For more information regarding confidential information see SWMBH policy 7.4 (Information Security).
8. Employees must not leave printers unattended when they are printing confidential customer or other information. This rule is especially important when two or more computers share a common printer.
9. Employees may not use SWMBH'S system to solicit for outside business ventures, organizational campaigns or political or religious causes. Nor may they enter, transmit or maintain communications of a discriminatory or harassing nature or materials that are obscene or x-rated. No person shall enter, transmit or maintain messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference or health condition. No person shall enter, maintain or transmit any abusive, profane or offensive language. For more information see SWMBH policy 7.3 (Internet Acceptable Use).
10. Users must log off the system at the end of the day or whenever the user leaves his/her office or the building and is not expected to return within the hour.

C. Acceptable Use

Use of SWMBH'S workstations and electronic resources is allowable subject to the following conditions:
1. Workstations and electronic resources may be provided in support of the agency mission and of the administrative functions that support this mission.
2. Electronic resources shall not be provided to outside individuals or organizations except by approval of the Chief Information Officer. Such services shall support the agency mission.

D. Unacceptable Use

SWMBH workstations and electronic resources may not be used for:

1. Unlawful activities.
2. Downloading or transmission of any communications where the meaning of the message or its transmission could reasonably be construed as being offensive to the recipient or recipients. These would include, but not be limited to, messages that contain profanity, sexually explicit content, race, national origin or gender specific comments, threats or harassment. Receipt of such information from an unsolicited source will not be cause for sanction.
3. Purposes that violate any applicable laws or regulations or are for personal profit or benefit. These would include, but are not be limited to:
    a. Unencrypted transmission of Protected Health Information (PHI) - sending person-served specific PHI over the Internet (web, file transfer, email, etc.) that has not first been encrypted is strictly prohibited
    b. Improper Release of Information - sending information that is confidential without first receiving the appropriate person's authorization.
    c. Purposes other than business of the organization, commercial or otherwise
    d. Copyright infringement, plagiarism, forgery, vandalism and software piracy
    e. Circumventing the Open Meetings Act
    f. Lobbying
    g. Religious or political advocacy
    h. Gambling, betting pools
    i. Chain letters, Ponzi schemes
    j. Use which involves misrepresentation of one's identity to compose, send and or intercept messages
    k. Any other uses that may create liability for the organization or harm its professional image
4. Port scanning or security scanning is expressly prohibited unless this activity is a part of the employee's normal job/duty.
5. No personnel may download any software without express permission from the CIO or his/her delegate. This rule is necessary to protect against the transmission of computer viruses into SWMBH'S system.
6. Executing any form of network monitoring which will intercept data not intended for the employee, unless this activity is a part of the employee's normal job/duty.
7. Monopolizing computer resources through excessive use shall be expressly prohibited. Such use detracts from the productivity of others. (i.e., streaming video/audio, web TV, etc.)
8. Personal use.
9. Executing any form of network monitoring which will intercept data not intended for the employee, unless this activity is a part of the employee's normal job/duty.
10. Circumventing user authentication or security of any host, network or account.
11. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
12. Improper use of thumb/flash drives. For more information see SWMBH policy 7.4 (ISM Information Security).

It is impossible to outline every example of acceptable or unacceptable use. The ITS Department reserves the right to allow for exceptions to the above guidelines on an as-needed basis. Requests for exceptions to any of the guidelines listed in this policy must be

submitted in writing (email or memorandum) to the Chief Information Officer, or his/her designee, for approval.

IV. References

BBA Section 164.310 (b)
BBA Section 164.310 (c)

V. Attachments

7.2A- User Acknowledgement

SOUTHWEST MICHIGAN BEHAVIORAL HEALTH
USER ACKNOWLEDGEMENT

I have read the SOUTHWEST MICHIGAN BEHAVIORAL HEALTH (SWMBH) "**WORKSTATION USE**" policy. I understand that failure to comply with or misuse of SWMBH's Workstation Use Policy will be subject to disciplinary action up to and including termination, and may be subject to penalties under state and federal laws and regulations.

By signing this, I agree that I have read, understood and will comply with this notice.

Employee's printed name: _____

Employee's Signature: _____