Subject: ISM Information Security	**Accountability:** Information Technology	**Effective Date:** 1/1/2014	Pages: 6
REQUIRED BY: **BBA Section** 164.312 Technical Safeguards **PIHP Contract Section** _____ **NCQA/URAC Standard** _____ **SA SARF** _____ **Other** _____		Last Reviewed Date: 6/18/2015	Past Reviewed Dates:
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: 6/18/2015	Past Revised Dates:
Approved : By: Date: 06/25/2015		Required Reviewer:	

I. Purpose

To ensure that Southwest Michigan Behavioral Health (SWMBH) and its officers, employees and agents have the necessary access to health and other information to manage behavioral health services while protecting the confidentiality of that information in accordance with all rules and regulations.

II. Policy:

A. It is the policy of SWMBH that all personnel must preserve the integrity and the confidentiality of Health and other sensitive information pertaining to customers enrolled with SWMBH.

B. SWMBH does not intend to create any third party rights by adopting these policies and procedures. Nor are these policies intended to create any expectation of privacy on behalf of any SWMBH workforce members with respect to information that they create, transmit and/or store using resources owned or controlled by SWMBH. SWMBH may amend or change these policies and procedures at any time, even retroactively, without notice. They are designed to allow flexibility in the way that SWMBH safeguards the sensitive information on its electronic information systems, and will be interpreted consistently with HIPAA and other laws that may apply. To the extent that the policies and procedures exceed what may be legally required, they are aspirational and not binding upon SWMBH.

III. Standards and Guidelines

A. SWMBH, in its role as a benefits manager, receives information that it is required to protect under federal or state law, by contract, or through its ethical responsibilities. The SWMBH policies and procedures in section 2.3 (Information Systems Management) describe how SWMBH protects electronic Protected Health Information (PHI) and other sensitive information, including any confidential customer information, on its electronic information systems. PHI in electronic form (EPHI) includes individually identifiable health information protected by the Health Insurance Portability and Accountability Act of 1996. Specifically, these policies and procedures address the steps that SWMBH uses to keep the EPHI available on a timely basis, to protect the integrity of the data, and to limit access to those who have a need to use the information. The policies and procedures were developed taking into account security practices described in the Health Information Portability and Accountability Act of 1996 (HIPAA) security regulations (Security Rules), and they are meant to coordinate with other SWMBH policies also designed to protect the confidentiality of EPHI.

B. No set of policies and procedures can ensure that information is always available, that determined individuals will not gain inappropriate access to sensitive information, or that individuals will never make mistakes. In order to reduce the likelihood that security incidents will occur, the Information Management policies and procedures use a risk-based model to identify and focus on those risks perceived as most likely to occur and having the most significant adverse impact.

C. Passwords and User Access

1. Authorization and/or Supervision
   Access to SWMBH information systems and specific documents containing EPHI will be granted as follows:

   a. Newly Hired Employees
      The ITS department assigns access rights based on the job function. ITS will not create the initial login account or provide access to information system resources until notified by the hiring manager.

   b. Change in Job Responsibilities
      When an existing employee changes job functions to a position that requires a different level of access to EPHI in SWMBH's systems, the hiring manager will provide the ITS department information about the change in job function and the effective date of the change.

      i. When an existing employee changes job functions to a position that no longer requires access to EPHI, the hiring manager will provide corresponding information to the ITS Department.

c. Third Party Access

As a general rule, the ITS Department does not grant third parties access to system resources. Visitors may be granted access to the Internet through a server that sits behind a separate firewall from other system resources. Before any third party will be granted access to system resources, access rights must be cleared by the Chief Information Officer. If the third party will have access to sensitive information, the third party will first have to sign a HIPAA Business Associate Agreement, if applicable.

d. SWMBH Portal Access

SWMBH portal access and permissions will be developed for SWMBH staff as appropriate.

e. Streamline Login Accounts

Streamline Login Accounts will be developed for SWMBH staff as appropriate.

f. Workforce Termination

i. When a SWMBH workforce member employment ends, that individual's privileges to access the information system will be disabled on a timely basis. The HR Department and/or hiring manager will report the termination to the ITS Department which will immediately terminate the individual's access privileges.

ii. It is expected that an participant CMHSP and/or provider that has access to SWMBH's Portal, notify ITS in a timely manner when they have staff turnover. As a safeguard ITS will automatically disable login accounts that have not been used for more than 30 days (this is a placeholder for when a Portal is created / established).

g. Access Control

i. User Names and Passwords

- Users are given unique user identification and passwords when they are first granted access rights. Users are able to change their password at any time and required to change their password every 90 days.

- When a user forgets his or her user name or password the ITS Department is not able to provide the password to the user. The ITS Department does not have access to any user's password, but can reset the password and allow the user to establish a new password.

- When ITS resets a user's password, it is expected that the user change their password at their earliest opportunity.

h. Automatic Log-Off
The SWMBH ITS department utilizes a screen saver that has an automatic lock-out feature that will activate within 10 minutes of inactivity prior. The screen saver is enabled as a default feature of the system.

j. Emergency Access
The Information Security Officer or Chief Information Officer is authorized to override access controls and provide appropriate individuals access to EPHI that would otherwise be barred by access controls that are generally in place.

k. Encryption/Decryption
i. The ITS Department will implement appropriate encryption and decryption technology to protect EPHI. It is SWMBH's policy that EPHI not be included in any e-mail correspondence.

ii. It is the policy of SWMBH that data shall not be saved or transported using any form of removable media (USB drives, CD's etc...) with the exception of backup tapes for the purposes of disaster recovery and prevention of data loss. Exceptions to this require approval by the employee's Senior Leader and CIO.

l. Authentication
The ITS Department will put processes in place to confirm that a person or entity seeking access to SWMBH's EPHI is who he/she or it claims to be. For internal or external access by workforce members, the individual's identity will be authenticated by the user's unique user identification name and password. The identity of any entity (e.g., another computer system) seeking access to SWMBH's EPHI will be authenticated by a unique user identification name and password that SWMBH provides to the entity when the entity is authorized to access the EPHI.

D. Electronic Signatures
Electronic signatures with the EHR application and/or any other applications that could utilize an electronic signature will have appropriate procedures.

1. Definitions
a. Legal/Written Signature
The signature of the individual recorded in the signature register. All signatures must include at least the first initial, surname and credentials/title.

b. Electronic Signature
The unique user identification (i.e. Network Login ID) along with the date and time that a particular individual took a conscious action to agree with a contract or other record and used as the legal equivalent of a written/legal signature.

2. Use
a. Once unique user identification has been established, it will be recognized as the electronic equivalent to the individual's actual (legal/written) signature. The ITS Department will apply the level of security as outlined by the individual's supervisor in accordance to the application security model. Once an individual has signed onto the SWMBH computer network, all activity entered into the computer system requiring a signature will utilize the stored sign-on along with the current date and the time as acknowledgment that the data, form or other computerized documents has been signed. The individual's sign-on will be accepted as if it were a hand written signature.

b. The Signature Register/Electronic Signature Notice (Form 2 3 D) is to be used so that the employee understands electronically signing documents is considered confidential. He/She must not disclose their password to anyone else or permit another user to use it. Additionally, the employee agrees that he/she will not use another person's password.

E. Policy Violations
Violations discovered by SWMBH personnel will be reported to the CIO and/or HIPAA Security Officer. Violations of this policy may result in discipline, up to and including termination.

IV. Definitions

Health Information

Any information, whether oral or recorded in any form or medium that is 1) created or received by SWMBH, providers, participant CMHSP or entities under contract; and 2) related 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.

Protected Health Information

The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."

"Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,

- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

System Resources
Hardware, Software, Data, and Networking Services owned and operated by SWMBH

V. References

BBA Section 164.308 (a) (7) and Section 164.312

VI. Attachments

7.4 A- Signature Register/Electronic Signature Notice

SOUHWEST MICHIGAN BEHAVIORAL HEALTH

SIGNATURE REGISTER/ELECTRONIC SIGNATURE NOTICE

I understand that the SOUTHWET MICHIGAN BEHAVIORAL HEALTH (SWMBH) computer network login account (User ID and password) assigned to me by the Information Technology Systems (ITS) department is confidential. This login account may be used to access electronic medical record information and for electronically signing documents. I certify that I will not disclose my password to another person or permit another person to use it. I further certify that I will not utilize another person's password.

I understand that my password is equivalent to my signature and that I am accountable for all entries and actions recorded under it.

I understand that failure to comply with or misuse of SWMBH's Electronic Signatures 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.

Printed Name	Credentials
Signature	Date