



Section: Information Technology Services	Policy Name: Information Security	Policy Number: 17.20
Owner: Chief Information Officer	Reviewed By: Natalie Spivak	Total Pages: 7
Required By: <input checked="" type="checkbox"/> BBA <input type="checkbox"/> MDHHS <input type="checkbox"/> NCQA <input type="checkbox"/> Other (please specify): _____	Final Approval By: <i>Natalie Spivak</i>	Date Approved: Jul 6, 2022
Application: <input checked="" type="checkbox"/> SWMBH Staff/Ops <input type="checkbox"/> Participant CMHSPs <input type="checkbox"/> SUD Providers <input type="checkbox"/> MH/IDD Providers <input type="checkbox"/> Other (please specify):	Line of Business: <input checked="" type="checkbox"/> Medicaid <input type="checkbox"/> Other (please specify): <input checked="" type="checkbox"/> Healthy Michigan <input checked="" type="checkbox"/> SUD Block Grant <input checked="" type="checkbox"/> SUD Medicaid <input checked="" type="checkbox"/> MI Health Link	Effective Date: 12/4/2020

Policy: It is the policy of Southwest Michigan Behavioral Health (SWMBH) that all personnel must preserve the integrity and the confidentiality of Health and other sensitive information pertaining to customers enrolled with SWMBH.

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.

Purpose: To ensure that 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.

Scope: All users of SWMBH computer systems

Responsibilities:

- A. The Chief Information Officer will be the Security Officer responsible for overseeing regulatory compliance, risk assessments and security audits.



- B. The Chief Compliance and Privacy Officer is responsible for overseeing privacy compliance management of protected healthcare information.
- C. All SWMBH employees and affiliates are responsible for protecting the security and privacy of protected health information according to the standards and guidelines of this and other related policies, for completing required security and privacy education and for reporting any suspected breaches to their immediate supervisors and the Security or Privacy officers.

Definitions:

Health Information

Any information, whether oral or recorded in any form or medium that is 1) created or received by SWMBH, providers, participant Community Mental Health Service Provider (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

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 17.0 (Information Management) describe how SWMBH protects Electronic Protected Health Information (EPHI) 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 as amended. 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 (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 Information Technology Services (ITS) Department assigns access rights and provides equipment 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 and any other system resources with the approval of 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 and external users as appropriate.
- e. Streamline Login Accounts: Streamline Login Accounts will be developed for SWMBH staff as appropriate to their job responsibilities.
- f. Workforce Termination: 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. In cases of involuntary termination, the departing employee's manager or HR Department will recover all equipment issued to the employee including laptops, cell phones, id badges, keys, keycards and other SWMBH owned devices and will escort the employee from the building. HR will then immediately notify ITS of the employee's termination via high priority e-mail with an in-person or phone follow-up. ITS will disable the terminated employee's accounts on the same day and reimaged the equipment received as soon as possible. If necessary, ITS will notify the managed services provider and other vendors who might need to disable the terminated employee's access.
- g. It is expected that a participant CMHSP and/or provider that has access to SWMBH's Portal, will 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.



h. 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 will 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 unencrypted EPHI not be included in any e-mail correspondence. Sensitive e-mail should be encrypted using Ecrypt. (See Policy 17.15 E-mail Encryption).
- 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...) 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. Multi-factor authentication is required to access Active Directory on SWMBH servers, the SWMBH data warehouse Microsoft 365 and other critical systems.

D. Electronic Signatures

Electronic signatures with the Electronic Health Record (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 can be 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 with 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 handwritten 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.

References:

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

Attachments: None



Revision History

Revision #	Revision Date	Revision Location	Revision Summary	Revisor
4	12/4/2020	Policy Name	Removed ISM	N. Spivak
4	12/4/2020	Standards & Guidelines	<p>A. added as amended deleted 1996</p> <p>C1a. added and provides equipment</p> <p>C1e. added to their job responsibilities</p> <p>C1f. added section on involuntary termination removed This is a placeholder for when a portal is created/established</p> <p>C1ki. Added unencrypted EPHI not be included in any e-mail correspondence. Sensitive e-mail should be encrypted using Ecrypt. (See Policy 17.15 E-mail Encryption).</p> <p>C1kii Removed with the exception of backup tapes for the purposes of disaster recovery and prevention of data loss.</p> <p>C1l added Multi-factor authentication is required to access Active Directory on SWMBH servers, the SWMBH data warehouse and other critical systems.</p>	N. Spivak
4	12/4/2020	Attachments	Removed 7.4 A- Signature Register/Electronic Signature Notice	N. Spivak



5	10/22/2021	Throughout	Annual Review – No Changes	N. Spivak
6	6/28/2022	Standards & Guidelines	Added Microsoft 365 to list of applications requiring multifactor authentication under section I	N. Spivak



17.20 Information Security

Final Audit Report

2022-07-06

Created:	2022-07-06
By:	Jody Vanden Hoek (jody.vandehoek@swmbh.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAAnpUQ3wr_JvQeNU5dDWu2tmsaoRH3lzy

"17.20 Information Security" History

-  Document created by Jody Vanden Hoek (jody.vandehoek@swmbh.org)
2022-07-06 - 3:15:36 PM GMT
-  Document emailed to Natalie Spivak (natalie.spivak@swmbh.org) for signature
2022-07-06 - 3:16:02 PM GMT
-  Email viewed by Natalie Spivak (natalie.spivak@swmbh.org)
2022-07-06 - 3:21:54 PM GMT
-  Document e-signed by Natalie Spivak (natalie.spivak@swmbh.org)
Signature Date: 2022-07-06 - 3:22:00 PM GMT - Time Source: server
-  Agreement completed.
2022-07-06 - 3:22:00 PM GMT