



Section: Information Technology Services	Policy Name: IT Security Review	Policy Number: 17.06
Owner: Chief Information Officer	Reviewed By: Natalie Spivak	Total Pages: 3
Required By: <input 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: Dec 9, 2020
Application: <input checked="" type="checkbox"/> SWMBH Staff/Ops <input checked="" 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 type="checkbox"/> Medicaid <input checked="" type="checkbox"/> Other (please specify): <input type="checkbox"/> Healthy Michigan _____ <input type="checkbox"/> SUD Block Grant <input type="checkbox"/> SUD Medicaid <input type="checkbox"/> MI Health Link	Effective Date: 12/4/2020

Policy: Southwest Michigan Behavioral Health (SWMBH) Information Technology (IT) shall conduct a quarterly review of logs and audit reports for all systems containing either ePHI and/or privileging administration.

- a. Logs and audit reports shall be produced for SWMBH’s review on a regularly scheduled basis, with schedule to correspond to best practice for each system.
- b. Reviews shall be documented by SMWBH IT.
- c. Any findings shall be communicated with the SWMBH Security Officer and Chief Compliance Officer.
- d. SWMBH IT to direct IT Managed Services Provider to address any concerns that are discovered during the reviews if they cannot be resolved by SWMBH staff.

Purpose: To ensure that SWMBH and its officers, employees and agents are monitoring user access by reviewing security logs and audits in furthering the security of its systems and protection of electronic Protected Health Information (ePHI) contained therein.

Scope: All SWMBH staff and authorized users of SWMBH information systems

Responsibilities:

1. Chief Information Officer (CIO) and IT Project Manager will receive and review user account management reports from Managed Services Provider
2. IT Project Manager will audit and communicate if any inappropriate activity has occurred
3. SWMBH IT staff or Managed Services Provider will resolve issues



Definitions: None

Standards and Guidelines:

Procedure for conducting the review:

- a. Obtain the latest system logs from IT vendor or system.
- b. Review logs for any unauthorized or inappropriate changes to permissions, access to ePHI systems, and any other improper management.
- c. Document review and findings, communicating results to the Chief Information Officer, Security Officer, and Compliance Officer as appropriate.
- d. Direct any resulting actions to IT provider as necessary.

Effectiveness Criteria: None

References: None

Attachments: None


17.06 IT Security Review

Final Audit Report

2020-12-09

Created:	2020-12-09
By:	Erin Peruchietti (erin.peruchietti@swmbh.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA3kyNb_VPJz5ui2B5zMsPaNhMIL2ZGYGe

"17.06 IT Security Review" History

-  Document created by Erin Peruchietti (erin.peruchietti@swmbh.org)
2020-12-09 - 3:16:46 PM GMT- IP address: 96.36.47.106
-  Document emailed to Natalie Spivak (natalie.spivak@swmbh.org) for signature
2020-12-09 - 3:17:07 PM GMT
-  Email viewed by Natalie Spivak (natalie.spivak@swmbh.org)
2020-12-09 - 4:18:04 PM GMT- IP address: 104.47.38.254
-  Document e-signed by Natalie Spivak (natalie.spivak@swmbh.org)
Signature Date: 2020-12-09 - 4:18:23 PM GMT - Time Source: server- IP address: 24.247.148.221
-  Agreement completed.
2020-12-09 - 4:18:23 PM GMT