MSHN
Mid-State Health Network

POLICIES AND PROCEDURE MANUAL

Chapter:	**Information Technology**		
Title:	**Cybersecurity Roles and Responsibilities**		
Policy: □ **Procedure:** ☒ **Page: 1** of 3	**Review Cycle: Biennial** **Author:** Chief Information Officer	**Adopted Date:** 08.12.2022 **Review Date: 09.12.2023**	**Related Policies:**

Purpose

The health insurance portability and accountability act of 1996 (HIPAA) and the Michigan Mental Health code indicate that protected health information (PHI) data and systems are to be secured and that steps should be taken to mitigate any risks related to the unauthorized release of PHI. This procedure outlines the expectations for assurance and monitoring and assigns responsibilities to mitigate risk. This procedure also provides guidance to the assigned individuals if/when a cybersecurity breach is identified.

Procedure

Cybersecurity is everyone’s responsibility. For Mid-State Health Network, that includes all employees, contractors, interns, network providers and any other stakeholder that have access to MSHN data. MSHN contracts with Providence Consulting for the management and protection of information systems and the purchase and set up of MSHN’s hardware (including laptops, servers, hosting, etc.)

There are five (5) parts to cybersecurity; Identify, Protect, Detect, Respond and Recover.

Identify. Identifying security issues/concerns happens in multiple places. Mid-State Health Network (MSHN) Chief Information Officer (CIO) and Providence staff, subscribe to many communication methods to ensure update to date information regarding public security risks. All MSHN staff, providers, system users, and other stakeholders shall identify areas they feel offer a level of security that is a concern. In all cases, if something seems like it might affect MSHN, MSHN CIO works together with Providence to determine the level of concern for that issue and determine next steps.

Protect. Providence maintains MSHN laptops and other software and devices with the latest security updates and provides firewall settings and virus protection to help keep our systems secure from threats. MSHN employees receive security training including cybersecurity at the time of hire and annually thereafter. MSHN employees receive email phishing training and testing monthly beginning at time of hire.

Detect. Providence has a monitoring process that checks MSHN equipment for any security issues. MSHN contractors are required to have mechanisms to control access to systems including detection of an attempt to subvert that control.

Respond. Providence has controls in place so that should a system be compromised, they are able to isolate the equipment, remove the issue and determine if a breach needs to be reviewed.

Recover. Providence and/or MSHN CIO will determine the appropriate steps in recovery that can include but are not limited to the following:

- Recover the service from last backup
- Reset passwords
- Require individual security training
- Public communication regarding the breach (in consultation with Privacy Officer) and
- Creating or amending policies and procedures.

Responsibilities

All MSHN staff have a responsibility to exercise due diligence in recognizing situations that could reduce or illustrate an unacceptable level of security. This means recognizing emails that are not legitimate and not clicking on links or opening attachments from suspect emails or other communications. It also means not going into systems and functions within systems that they do not have a work-related need to access. MSHN staff shall not access protected health information via an open public Wi-Fi. MSHN staff will agree to follow the MSHN Computer Use Agreement. All MSHN staff shall stay up to date on their Relias Security trainings. If staff suspect there is a security related issue it should be reported to the MSHN CIO immediately.

The MSHN IT department staff have responsibility for reviewing systems for whether there is an unacceptable level of security. IT staff must understand when a process needs to be changed to prevent people without the proper knowledge from making the easy mistakes.

The MSHN CIO has responsibility to ensure that everyone has the tools and access to the materials to manage their respective role and responsibility. Additionally, the CIO needs to have the foresight to recognize what steps are needed to manage each situation that presents in the cybersecurity realm.

Product system designers and others at our contracted vendors need to understand how to setup systems/equipment so that compromise of the system or locking of the data by outside entities is not possible, and how to limit any errors to the minimum possible should the security be breached.

Providence, as our technology contractor, must have staff and resources available to handle all the tasks of identifying potential issues, protecting against any reasonable threat, detecting whether a problem is present, responding or resolving any issue that does get past the defenses, and assisting with the recovery by providing input related to policies and procedures that either missed items or were not followed correctly and how to avoid the problem in the future.

Other stakeholders are responsible to report to MSHN any suspected security concerns, removal of access to systems, exposure to MSHN data, etc.

Steps during an incident

When a potential security incident has been reported or discovered, the CIO will review the concern to determine the level of the threat and if needed seek guidance from appropriate resources (e.g. IT provider, Insurance Carrier, Risk Assessor). If immediate action is required to reduce additional exposure/threat, the CIO will take those steps ASAP (e.g., turning off the laptop or disconnecting it from access to other systems or the internet).

When any kind of valid threat is determined, the CIO shall notify the Deputy Director, CEO, Providence, and any other vendors that might be connected to the issue (for example, PCE).

The CIO shall communicate any steps that need to be taken to remediate the situation. Once the threat is resolved, the CIO will review the process and recommend policy or practice changes to avoid similar situations in the future.

Applies to

☒ All Mid-State Health Network Staff

□ Selected MSHN Staff, as follows:

□ MSHN's CMHSP Participants: □Policy Only □Policy and Procedure

☒ Other: Sub-contract Providers

Definitions

Other Related Materials

N/A

References/Legal Authority

N/A

Change Log:

Date of Change	Description of Change	Responsible Party
8.12.2022	New Procedure	Chief Information Officer
5.18.2023	Biennial update	Chief Information Officer