DWIHN Provider Cybersecurity Self-Assessment

INTRODUCTION

Cybersecurity is essential for all businesses, including health care provider organizations, such as practices, clinics, and health centers (herein referred to as organizations throughout, to prevent, detect, and respond to cyber threats and attacks. Cybersecurity is not limited to just the technology systems that store and transmit member data; it encompasses people and processes to make sure operations and security are working in tandem. Assessing cybersecurity preparedness helps ensure that cyber threats are treated like any other disaster (e.g., fires, floods, outbreaks), encompassing a review of preventative measures that protect member privacy and safety, and limit disruption to organizational operations should a cyber-attack occur.

The Detroit Wayne Integrated Health Network (DWIHN) is using this Cybersecurity Preparedness Self-Assessment Questionnaire (questionnaire) to assist organizations with assessing cybersecurity. The questionnaire includes select elements from the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF was developed through a collaborative process with experts in the federal government and private sector to create a set of standards, best practices, and recommendations for improving cybersecurity. The five core functions of the NIST CSF include: Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). Each function has a list of categories and subcategories that define specific cybersecurity activities that should be performed continuously and concurrently. Users of the questionnaire are encouraged to review the NIST CSF at: nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

INSTRUCTIONS

The questionnaire consists of a series of self-evaluation statements intended to help users identify potential gaps in cybersecurity and prioritize areas for improvement. Statements are grouped by people, processes, and technology, referencing the NIST CSF function, category, and subcategory, along with applicable page numbers in the NIST CSF (Version 1.1, April 2018). Click on the source for more information.6 For each statement, select one of the following response options that most accurately reflects how you would categorize your organization's ability to effectively detect, understand, and contain cyber threats:

- *Lacking – Unaware or unable to take effective action*
- *Minimal – Some basic structures in place to react if a problem should surface*
- *Satisfactory – Necessary structures in place to address current problems*
- *Advanced – Identifying and implementing structures that anticipate and address emerging problems*
- *N/A – Not applicable*

Following each question, you will need to give a description on why you feel the answer given is appropriate, N/A answer must include a detailed reason as why the question is not applicable.

Thank you for completing this security assessment. This questionnaire helps us understand how you protect data and systems. Your honest and complete responses allow us to evaluate our partnership and identify any areas where we need additional security measures. Please answer every question honestly and completely.

1. Organization Details

What is the company/business name? *

What is the business physical address? (please separate with commas) *

Address Street, Apartment/building/suite, City, State, Zip

What is the country of company/business? *

Name, Title and contact info of person completing assessment: (please separate with commas) *

Name, Title, e-mail, phone

How long has the company been in business? *

What is your HIPAA Security Officer contact's info? (please separate with commas) *

Name, e-mail, phone

What is your HIPAA Privacy officer contact's info? (please separate with commas) *

Name, e-mail, phone

What is your IT Technical contact's info? (please separate with commas) *

Name, e-mail, phone

What is the URL of the company? *

Does the organization utilize the services of 3rd parties for IT services or systems? *

- ◯ Yes
- ◯ No

3rd Party Contact's Info: (please separate with commas) *

Company Name, contact name, address, e-mail, phone(please separate with commas)

Does this assessment include Cloud Hosting Services? *

- ◯ Yes
- ◯ No

Name of Cloud Hosting Services?

Has the organization had a 3rd party IT security assessment

▶ Example: HiTrust, SOC 2, SOC 1, SOC for Cybersecurity, or an equivalent report or certification from an external auditor assessing your information security controls. An equivalent may include a different externally conducted security audit report, or certification such as ISO 27001.
*

- ◯ Yes (e-mail copy of the report/certification)
- ◯ No

Date of report or certification: *

Name or certification or report *

2. People

Cybersecurity roles and responsibilities are coordinated to avoid duplication and are clearly defined in employee position descriptions

▶ Example: IT Operations Manual, Employee Handbook, and Business Associates Agreements outline roles and responsibilities of all
employees and third parties.
*

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

Employees, computer system security workers, and third parties receive training for safeguarding systems and access to information, and preventing, detecting, and responding to cyber threats and attacks

▶ Example: Employee Handbook, position requirements, employee training program including testing and exercises, signed contracts, memorandums of understanding, Business Associate Agreements. *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

Employees and third parties demonstrate understanding of the legal and regulatory requirements governing cybersecurity and their roles and responsibilities related to cyber threats and attacks

▶ Example: HIPAA and HITECH, data security, patient privacy, and breach reporting. *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

The organization shares with employees and third parties the acceptable level of operational risk

▶ Example: Risk assessment is completed and results included in employee training *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

Periodic monitoring and review of IT system activity log, such as Internet use, creation of new users, resetting of passwords, e-mail spam, file downloads, and use of portable external devices (e.g., flash drive)

▶ Sample compliance: Audits of IT system logs and e-mail accounts *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

Information pertaining to cybersecurity processes, testing, threats, and attacks is received and shared with appropriate employees and third parties

▶ Example: Communication plan, cybersecurity plans, cyber incident reports, participation in online forums, stakeholder advisory groups, and other information-sharing sessions *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

Remote access is managed through formal approval and credentialing based on the role of the employee or third-party

▶ Example: IT Systems Operation Manual outlines access requirements for each role, security procedures for encrypting data and using a virtual private network (VPN), remote desktop, or remote database *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

All users and devices undergo a standard approval process prior to use, and all system identities and credentials are authenticated and managed by a designated authorized employee

▶ Example: IT Systems Operation Manual outlines requirements for usernames, passwords, application access, and authentication of credentials in line with risk *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

User permissions and access privileges for IT systems, devices, software, and files are limited to only what is necessary to perform job functions

▶ Example: Configuring user profiles and software based on role, key cards, and fobs, limiting access to sensitive areas/materials *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

All employees and third parties demonstrate adherence to established cybersecurity policies and regulations when using IT systems and software

▶ Example: Employee policies include steps for non-compliance, and all agreements and contracts executed with third parties detail responsibilities and termination clauses for non-compliance *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

3. Processes

The mission, objectives, and activities of the organization have been established and communicated to employees and third parties, as appropriate

▶ Example: Company Operation Manual, Employee Handbook, Memorandums of Understanding, Business Associate Agreements, contracts executed with third parties, and Cyber Supply Chain Risk Management Plans *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

The organization has a mapping of how information and data move through IT systems and networks, and has prioritized all activities, systems, software, and data that are essential for its operation

▶ Example: Workflow charts for communication and data transmission processes, evaluating potential effects from an interruption in critical business operations, and sharing results with employees and third parties *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

The organization has developed incident response and recovery plans that address cybersecurity and is able to execute plans during or after an event

▶ Example: Cybersecurity incident response, business continuity, disaster recovery, and cyber supply chain risk management plans are in place and updated *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

Employees and third parties understand the potential impact of a cyber-attack on delivering timely care to patients and ways to mitigate downtime with a cyber incident response plan

▶ Example: Business impact analysis, cybersecurity risk assessment, business continuity *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

The organization identifies and documents known internal and external cyber threats, links these to results from cyber audits and testing, and uses this information to determine organization's risk level

▶ Example: Business impact analysis, and IT risk assessment report *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

Processes for secure data backup and recovery are implemented, documented, tested, and maintained

▶ Example: Disaster recovery planning *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

Cybersecurity policies are reviewed and tested to ensure defenses against cyber threats and alignment with industry best practices

▶ Example: Business impact and disaster recovery reports are generated and reviewed, conducting mock cybersecurity drills, and lessons learned are communicated to employees and third parties and documented in the IT Operations Manual *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

The organization shares information externally regarding the selection, implementation, and use of technology to protect against cyber threats or attacks

▶ Example: Information sharing through participation in online forums, writing product reviews, developing third-party cyber supply chain risk management plans, and case studies *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

Notifications/alerts from detection systems, such as virus software, intrusion detection systems, or security management systems, are reviewed for suspicious activities, and appropriate actions are taken to remediate potential threats

▶ Example: Risk assessment and business impact analysis to determine risk level by both probability and potential impact *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

The organization contains cyber threats to minimize risk

▶ Example: Use of firewalls, VPNs, email security software, and anti-malware software *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

Information is collected, analyzed, and reported to relevant employees and third parties following a cyberattack to understand the cause and impact on the organization

▶ Example: Business impact analysis and disaster recovery reports *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

Information is collected, analyzed, and reported to relevant employees and third parties following a cyberattack to understand the cause and impact on the organization

▶ Example: Business impact analysis and disaster recovery reports *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

Criteria have been established to report cyber-attacks, monitor compliance with reporting, and remedy non-compliance with reporting policies

▶ Example: Disaster recovery plans, employee handbook and business associate agreements, training, documentation of counseling, and/or termination procedures for non-compliance *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

4. Technology

Physical devices, IT systems, and software that are both owned and not owned by the organization have been inventoried and recorded

▶ Example: Catalogue of all computers, mobile devices, electronic medical devices, printers, scanners, fax machines, copiers, any machines stored off site that are accessed virtually by the organization, programs installed on computers, and electronic health record systems *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

The IT systems, network, software, and third-party activity is monitored and scanned to detect potential unauthorized access and identify the source of the potential cyberattack

▶ Example: Vulnerability scans, penetration testing, and reviews of IT system access audit logs *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

The physical environment outside of IT systems is restricted and monitored for unauthorized access

▶ Example: Security employees, key cards, and fobs for access, and auditing of access and visitor logs *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

All data that is stored, transmitted, or accessed by the organization is protected from unauthorized access

▶ Example: IT Operations Manual includes information on converting data to code (encrypting) and firewalls *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

The IT systems network has the capacity to ensure data and software are always able to be accessed and used by authorized individuals

▶ Example: A calculator to determine the amount of data that can be transferred in one second, mechanisms such as failsafe, loadbalancing, and alternative hardware to prevent failure *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

IT systems used for testing and development are separated from systems that carry out the daily operations of the organization

▶ Example: Internal firewalls, separate internet connections *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

Procedures for purchasing IT systems and software are established using a risk management process and agreed upon by stakeholders

▶ Example: IT Operations Manual outlines the process for analysis, design, development, testing, installation, maintenance, evaluation, and disposal of IT systems and software *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

Restrict changes to the IT system by limiting software installation and connection to external devices, as well as monitoring electronic communications and users of the system

▶ Example: Encryption, virus scans, monitoring of email and Internet use, limiting the ability to install software to dedicated IT employees, blocking external devices (i.e., flash drives and smartphones) from connecting to a computer or network *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

Maintenance and repair of IT systems and software are documented and conducted by authorized individuals, vendors, and tools

▶ Example: List of approved vendors and tools, IT maintenance procedures in the employee handbook, and training *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

Maintenance and repair of IT systems and software is documented and conducted by authorized individuals, vendors, and tools

▶ Example: List of approved vendors and tools, IT maintenance procedures in the employee handbook, and training *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

IT systems and processes for data removal, transfer, storage, and destruction are standard and logged throughout the organization

▶ Example: IT Operations Manual and employee handbook, and training addresses the removal, transfer, and storage of systems and data, and the process for overwriting, de-magnetizing, and shredding data that includes obtaining and logging a certificate of destruction *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

What email service does the organization use?

▶ Example: Gmail, Exchange, Outlook365, Hotmail, AOL, Yahoo, Proton mail, On-Prem *

Is MFA set up on the organization's email service or system? *

- ◯ Yes
- ◯ No

Mobile devices used to access MHWIN or member data are fully encrypted.

▶ Example: Laptop, Tablets, and Mobile phones have full disk or device encryption *

- ◯ Lacking
- ◯ Minimal
- ◯ Satisfactory
- ◯ Advanced
- ◯ Not Applicable

Provide the reason for the above answer: *

Are you using Ai at any of your facilities for any purpose? *

- ◯ Yes
- ◯ No

For what purpose are is AI in use? *

What AI tools are in use? *

5. Attestation

By entering my name below, I hereby certify that I am an authorized representative of my organization with the authority to complete this assessment, and that all information provided in this questionnaire is accurate, complete, and truthful to the best of my knowledge. I understand that this information will be relied upon for security assessment and compliance purposes, and I acknowledge my responsibility to promptly notify DWIHN of any material changes to the responses provided herein. *