**CAN/DGSI 118:2023**
**NATIONAL STANDARD OF CANADA**

First Edition
2023-11

# Cybersecurity: Cyber resiliency in healthcare

35.020; 35.030

- Page left intentionally blank -

# Table of Contents

- Page left intentionally blank -

## Foreword

The Digital Governance Standards Institute (DGSI) develops digital technology governance standards fit for global use. The Institute works with experts, as well as national and global partners and the public to develop national standards that reduce risk to Canadians and Canadian organizations adopting and using innovative digital technologies in today's digital economy.

DGSI standards are developed in accordance with the *Requirements & Guidance – Accreditation of Standards Development Organizations*, 2019-06-13, established by the Standards Council of Canada (SCC).

Attention is drawn to the possibility that some of the elements of this Standard may be the subject of patent rights. DGSI shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of this Standard are included in the Introduction.

For further information about DGSI, please contact:

**Digital Governance Standards Institute**
500-1000 Innovation Dr.
Ottawa, ON K2K 3E7
www.dgc-cgn.org

A National Standard of Canada is a standard developed by a Standards Council of Canada (SCC) accredited Standards Development Organization in compliance with requirements and guidance set out by SCC. More information on National Standards of Canada can be found at www.scc.ca.

SCC is a Crown corporation within the portfolio of Innovation, Science and Economic Development (ISED) Canada. With the goal of enhancing Canada's economic competitiveness and social well-being, SCC leads and facilitates the development and use of national and international standards. SCC also coordinates Canadian participation in standards development and identifies strategies to advance Canadian standardization efforts.

Accreditation services are provided by SCC to various customers, including product certifiers, testing laboratories, and standards development organizations. A list of SCC programs and accredited bodies is publicly available at www.scc.ca.

- Page left intentionally blank -

## Introduction

This is the First Edition of CAN/DGSI 118:2023, Cybersecurity: Cyber resiliency in healthcare.

CAN/DGSI 118:2023 Cybersecurity: Cyber resiliency in healthcare was prepared by the Digital Governance Standards Institute Technical Committee 5 (TC 5) on cyber security, comprised of over 180 thought leaders and experts in cyber security and related subjects. This Standard was approved by a Technical Committee formed balloting group, comprised of 4 producers, 4 government / regulator / policymakers, 3 users, and 4 general interests.

All units of measurement expressed in this Standard are in SI units using the international system (SI).

This Standard is subject to technical committee review beginning no later than one year from the date of publication. The completion of the review may result in a new edition, revision, reaffirmation or withdrawal of the Standard.

The intended primary application of this Standard is stated in its scope. It is important to note that it remains the responsibility of the user of the Standard to judge its suitability for a particular application.

This Standard is intended to be used for conformity assessment.

The Digital Governance Standards Institute gratefully acknowledges and thanks HealthCare*CAN* for its vision, support and collaboration to co-develop CAN/DGSI 118, Cybersecurity: Cyber resiliency in healthcare. HealthCare*CAN* is the national voice of action for health organizations and hospitals across Canada. They advocate in support of health research and innovation; to enhance access to high-quality health services for Canadians; and empower health professionals through best-in-class learning programs. www.healthcarecan.ca

The Digital Governance Standards Institute acknowledges the financial support of Public Safety Canada.

Public Safety Canada Sécurité publique Canada

ICS 03.100.01; 35.030

CETTE NORME NATIONALE DU CANADA EST DISPONIBLE EN VERSIONS FRANÇAISE ET ANGLAISE

- Page left intentionally blank -

## Context

Canadian healthcare organizations are often the targets of cyber attacks including, but not limited to, business email compromise, social engineering attack, ransomware attacks, and data exfiltration. Outcomes of such cyber attacks include system outages, operational impacts, delays, and increased patient care wait times, redirection of urgent care or critical patients to other facilities, privacy breaches, data loss, data integrity issues, etc. Healthcare organizations lack resources to implement fulsome cybersecurity framework and innovative technological solutions to prevent cyber attack. Recognizing the need for baseline cybersecurity controls that should be established at each healthcare organization, this standard outlines the most impactful cybersecurity controls.

Further contextual details and sample case examples related to cybersecurity breaches at healthcare organizations can be found in Annex A.

**Considerations for Virtual Care (virtual visits, remote patient monitoring, patient apps)**

**Virtual Visits**

Virtual visits are clinical encounters between patients and care providers occurring remotely using various forms of electronic communication, such as radio, audio videoconferencing, secure messaging, or file exchange with the aim of securely facilitating and maximizing the quality efficiency and effectiveness of patient care. A virtual visit may be synchronous (occurring in real-time) or asynchronous which involves intermittent communication between the clinician and patient. Unlike meeting physically in the clinical or hospital setting, each of these new technologies can introduce challenges for ensuring the privacy and security of patient information.

**Remote Patient Monitoring**

Remote Patient Monitoring (RPM) involves the application of technology to enable the monitoring and reporting of a patient's health data in the patient's home or other non-clinical settings. The benefits of these programs include improved patient quality-of-life and better outcomes.

The processes and technologies (i.e., devices and applications) that are prescribed may be owned by the healthcare organization or may be third-party solutions that enable the collection and/or transmission of health information collected in non-clinical, patient-controlled settings to a central point for consolidation. The consolidation point is designated or controlled by the healthcare organization.

In some cases, RPM devices may be considered 'medical devices'. Regulatory agencies in Canada and the U.S. have issued guidance based on medical device definitions, the intended purpose of products and the risks associated with the potential for the device or system to cause harm. In Canada information is available from Health Canada on a dedicated website for guidance documents for medical devices while the United States of America Food and Drug Administration (FDA) issued the "Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff" on September 25, 2013.

The remote patient monitoring devices and applications mentioned above present a unique set of challenges. Healthcare organizations are also encouraged to include mobile application-related considerations when evaluating RPM applications that run on mobile devices.

**Considerations for Health Tech (cloud, IOT, legacy) and operational technology (OT)**

Cybersecurity risks to medical devices are continually evolving, therefore, it is not possible to completely mitigate all risks at the time of installation. Healthcare organizations manage cybersecurity risks associated with medical devices by implementing a separate or parallel risk management program to protect, monitor and respond to vulnerabilities identified in medical devices. Medical devices include considerations around Internet of Things (IOT) devices (e.g., an Xray machine), and wearable devices which may connect via Ethernet, Bluetooth, Wi-Fi and other protocols.

As healthcare organizations adopt interconnected Operational Technology (OT) with its IT to IOT to support physical operations of its environment, appropriate OT security is required to protect the data being collected by OT as well as to ensure availability and reliability of the technology. The cyber resiliency strategies covered in this standard applies to both IT and OT. Considerations should also be given to the necessity of securing artificial intelligence (AI) and machine-learning solutions within OT environments.

# Cybersecurity: Cyber resiliency in healthcare

## 1 Scope

The standard specifies minimum requirements for cyber security in healthcare organizations and supports cyber resiliency of Canada's healthcare system.

NOTE: While organizations are to be encouraged to consider physical security as a key aspect of their cyber security program, given the complexity and resources required, it is out of scope of this Standard.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

CAN/CIOSC 104:2021, *Baseline Cyber Security Controls for Small and Medium Organizations*

## 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply:

**application**
Software or a program that is specific to the solution of an application problem.

[SOURCE: ISO/IEC 20944-1:2013]

**application system failure**
An incident affecting the confidentiality, integrity, or availability of applications.

**code grey**
Is initiated following the loss of a critical system (i.e., electricity, water, heating, medical gas, communications, ransomware, information technology etc.) or any intervention measures (i.e., a combative person) that may pose a health and safety risk to those in the hospital.

**confidentiality**
The ability to protect sensitive information from access by unauthorized people.

**cyber security compensating control**
A safeguard or countermeasure deployed, in lieu of, or in the absence of controls designed by a device manufacturer. These controls are external to the device design, configurable in the field, employed by a user, and provide supplementary or comparable cyber protection for a medical device.

**cyber resiliency**
An entity's ability to prepare for, prevent against, and continuously deliver the intended outcome, despite cyber attacks. Resilience to cyber attacks is essential to IT systems, critical infrastructure, business processes, organizations, societies, and nation-states.

**cyber security incident**
Any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete, or render unavailable any computer network or system resource.

[SOURCE: CAN/CIOSC 104:2021]

**data**
Information collected in the process of normal business practices such as structured and non-structured information generated from production and non-production systems.

**data breach**
The loss of unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards. For the purposes of this document the focus is on cyber related causes.

**denial of service**
See “service interruption”.

**domain name system (DNS)**
Hierarchical, distributed global naming system used to identify entities connected to the Internet

NOTE: The Top-Level Domains (TLDs) are the highest in the hierarchy.

[SOURCE: ISO/TR 14873:2013]

**encryption**
Converting information from one form to another to hide its content and prevent unauthorized access.

[SOURCE: Canadian Centre for Cyber Security]

**firewall**
A security barrier placed between two perimeters that controls the amount and kinds of traffic that may pass between the two.

**healthcare organization**
an organization involved in the direct or indirect provision of healthcare.

NOTE: For the purposes of this standard, referred to throughout as the organization.

[SOURCE: ISO 22886:2020]

**injury**
The damage that businesses suffer from the compromise of information systems and IT assets.

**incident response plan**
A document that establishes processes, procedures, and documentation related to how your organization detects, responds to, and recovers from incidents. Cyber threats, natural disasters, and unplanned outages are examples of incidents that will impact your network, systems, and devices.

[SOURCE: Canadian Centre for Cyber Security]

**integrity**
The ability to protect information from unauthorized modification or deletion.

**IT**
Information technology.

**least privilege**
The principle of giving an individual only the set of privileges that are essential to performing authorized tasks. This principle limits the damage that can result from the accidental, incorrect, or unauthorized use of an information system.

[SOURCE: Canadian Centre for Cyber Security]

**loss of Information**
See “unauthorized disclosure”.

**malicious code**
Programs or code written for the purpose of gathering information about systems or users, destroying system data, providing a foothold for further intrusion into a system, falsifying system data and reports, or providing time-consuming irritation to system operations and maintenance personnel.

NOTE 1: Malicious code attacks can take the form of viruses, worms, Trojan horses, or other automated exploits.

NOTE 2: Malicious code is also often referred to as “malware”.

[SOURCE: IEC/TS 62443-1-1:2009]

**malware**
Malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, spyware, and adware.

[SOURCE: Canadian Centre for Cyber Security, Glossary]

**may**
A keyword that indicates flexibility of choice with implied preference.

**multi-factor authentication**
*Authentication* that uses a combination of two or more different authentication factors – something a user knows (e.g., a password), has (e.g., a physical token), or is (e.g., a biometric) – to verify a user's identity.

**network system failures (widespread)**
An incident affecting the confidentiality, integrity, or availability of networks.

**Operational Technology (OT)**
Programmable systems or managed devices that interact with the physical environment. These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Example of such medical devices are X-ray machines, dialysis machines, patient monitoring devices, simulation technology devices etc.

[SOURCE: NIST 800-37 Rev. 2, modified]

**OWASP**
Open web application security project.

**password manager**
A password manager is a computer program that allows users to store, generate, and manage their passwords for local applications and online services. A password manager assists in generating and retrieving complex passwords, storing such passwords in an encrypted database, or calculating them on demand.

**patching**
The act of applying updates to computer software or firmware.

**phishing**
An attack where a scammer calls you, texts or emails you, or uses social media to trick you into clicking a malicious link, downloading malware, or sharing sensitive information. Phishing attempts are often generic mass messages, but the message appears to be legitimate and from a trusted source (e.g., from a bank, courier company).

[SOURCE: Canadian Centre for Cyber Security]

**privacy breach**
Occurs when personal health information or personal information is collected, used, or disclosed without authorization. This can include theft, loss, or unauthorized copying, modification, or disposal.

**ransomware**
A type of *malware* that denies a user's access to a system or data until real or virtual goods and/or funds are paid.

**sensitive information**
Information that requires protection against loss, modification, and unauthorized disclosure.

NOTE: Sensitive information can include personal information, business information or classified information.

**secure portable media**
Security of portable media devices e.g., USB flash drives, laptops, tablets.

**service interruption**
Incident that prevents access to a service or otherwise impairs normal operation.

**shall**
A requirement for test methods, specifications or implementations.

**should**
A keyword indicating flexibility of choice with a strongly preferred alternative; equivalent to the phrase “it is strongly recommended”.

**spear phishing**
A phishing attack that targets a specific person, group or organization. It uses personal or professional details to further entice you to respond, click on a link or open an attachment.

[SOURCE: Canadian Centre for Cyber Security]

**unauthorized access**
Access to physical or logical network, system, or data without permission

**unauthorized disclosure**
An incident affecting the confidentiality, integrity, or availability of data.

**unauthorized use**
Use of a physical or logical network, system, or data without permission.

**virtual care**
The use of information and communication technologies to provide health care services and health education to patients when the clinician and patient are not at the same location. These technologies are not treatments or Virtual Health interventions in and of themselves, but rather tools that can be used to increase accessibility and access to care, person-centred care, information exchange, and efficiency of care.

[SOURCE: CAN/HSO 83001:2018]

**virtual private network (VPN)**
Restricted-use logical computer network that is constructed from the system resources of a physical network by using encryption and/or by tunnelling links of the virtual network across the real network.

[SOURCE: ISO/IEC 18028-3:2005]

**virtual visit**
Clinical encounters between patients and care providers occurring remotely using various forms of electronic communication such as radio audio videoconferencing secure messaging or file exchange with the aim of securely facilitating and maximizing the quality efficiency and effectiveness of patient care. A virtual visit may be synchronous (occurring in real-time) or asynchronous which involves the intermittent communication between the clinician patient.

**wireless local area networking (WLAN)/(Wi-Fi)**
Wireless local area networking technology that allows electronic devices to network, mainly using the 2,5 GHz and 5 GHz radio bands.

NOTE 1: "Wi-Fi" is a trademark of the Wi-Fi Alliance.

NOTE 2: "Wi-Fi" is generally used as a synonym for "WLAN" since most modern WLANs are based on these standards.

[SOURCE: ISO/IEC 27033-6:2016]

**wi-fi protected access**
Security protocol and security certification program developed by the Wi-Fi Alliance to secure wireless computer networks.

[SOURCE: ISO 20415:2019]

# 4 Organizational Risk Management

## 4.1 Leadership

4.1.1 Leadership of the organization is ultimately accountable for the cyber security program.

4.1.2 Leadership shall demonstrate their commitment to the cyber security program by ensuring cybersecurity policies and objectives are established and are aligned with the strategic direction of the organization.

4.1.3 Leadership shall ensure that the resources (e.g., people, process, technology, finances, authority etc.) needed for the cyber security program are available and are aligned with the cyber security policy and objectives.

4.1.4 Leadership shall communicate the importance of effective cyber security and of conforming to the cyber security program requirements.

4.1.5 Leadership shall be responsible for setting the cyber risk target level for the organization.

4.1.6 Leadership shall establish cybersecurity program metrics and continually track progress.

4.1.7 Leadership shall support other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

**4.2 Delegation of security**

4.2.1 Leadership shall appoint a member of the senior-level leadership team to oversee and be accountable for the organization's cybersecurity. Accountabilities shall include the following:

a. developing and implementing a company-wide information cyber security program to meet baseline cyber security controls;

b. documenting and disseminating information security policies and procedures;

c. coordinating the development and implementation of a company-wide information security training and awareness program;

d. determining and recommending to the leadership team the cyber risk target level of the organization;

e. tracking and providing periodic reports/status on the cyber risk target level of the organization;

f. coordinating a response to actual or suspected breaches in the confidentiality, integrity, or availability of the organization's systems and data;

g. identifying organizational risks and prioritizing risk treatment relative to likelihood and potential impact of cyber threats;

h. participating in information sharing groups or institute a program or capability of remaining aware of evolving nature of cyber threats; and

i. delegating of information security role as required.

NOTE: Please see RACI (as outlined in Annex E).

**4.3 Asset risk assessment**

4.3.1 The organization shall have an inventory of their IT assets (infrastructure, applications, and data) and OT assets (e.g., X-ray, dialysis machines, and patient monitoring devices) and classify these assets based on their criticality to the organization.

4.3.2 The organization shall identify the key assets that need to be protected.

4.3.3 The organization shall carry out a cyber security risk assessment to identify threats and vulnerabilities of concern and in establishing appropriate security controls to ensure uninterrupted delivery of services to key assets.

4.3.4 The organization should align with existing standards for risk management.

4.3.5 The organization shall maintain data flow diagrams and descriptions that address all stages of the data lifecycle for personal health information (PHI), both security and privacy safeguards, from the time it is created and/or collected, moved, used, stored, and destroyed.

NOTE 1: Some jurisdictions may have requirements for data sovereignty. For example: all PHI must reside in province, or within Canada. It is important to know in which country the data is located. The retention period for data in transit should be known and minimized.

NOTE 2: As more healthcare applications move to cloud environments, data flow diagrams and descriptions must include geographical locations for data in the cloud.

**4.4 Identity and access management**

4.4.1 All information systems which provide access to personal health information shall authenticate all access.

4.4.2 The organization shall require potential users of healthcare systems to have a user-registration process. These user-registration procedures shall include requirements to verify the individual against government-issued photo identification, and membership in the appropriate licencing body (as required).

NOTE: Minimum requirements can include verifying communication methods to users (phone, email) and/or integrating with other government digital ID programs, and/or methods to validate users where physical access to the government-issued photo identification is not possible.

4.4.3 The organization shall implement a defined process to regularly review all user access rights, making removal and/or adjustments to access rights in a timely manner when required.

4.4.4 The organization shall provision accounts with role-based access controls with minimum functionality necessary for tasks and shall restrict administrator privileges to an as-required basis.

4.4.5 The organization shall consider the implementation of a centralized authorization control system.

4.4.6 The organization shall implement multi-factor authentication or document all instances where they cannot or make the business decision not to do so.

4.4.7 The organization shall follow a formal verification and approval process and only allow authorized users to access critical Operational Technology (OT).

### 4.5 Visibility tools

4.5.1 The organization should implement an Endpoint Detection and Response (EDR) system, with options for Security Information Event Management (SIEM) integrations and incident response team for both IT and OT environments.

4.5.2 The organization should have threat intelligence and threat management systems in place.

4.5.3 The organization shall have effective audit mechanisms that can reconstruct all create/read/update/delete/share operations on sensitive data within the organization.

## 5 Training (building a cyber-resilient workforce)

### 5.1 Cybersecurity awareness and training

5.1.1 The organization shall train employees on basic security practices, including a focus on the following practical and easily implementable measures to apply appropriate safeguards for data, systems and devices in their care:

a. The use of effective password policies;

b. Identification of malicious emails and links;

c. Use of approved software;

d. Appropriate usage of the Internet;

e. Safeguarding OT from potential cyber threat exposure;

f. Safe use of social media; and

g. Safe data handling based on data sensitivity.

NOTE 1: Cyber security awareness and training is most effective when supported by policy.

NOTE 2: The six items listed are not an exhaustive list, just examples.

NOTE 3: Cyber security awareness and training should be customized based on roles and responsibilities of users or employees.

NOTE 4: All employees should be aware of appropriate, relevant jurisdictional legislation.

5.1.2 The organization shall develop, document, and disseminate to users of information systems a privacy and security training program.

a. Users of information systems shall complete training prior to having access to information systems, and annually,

b. Training shall be updated to address a changing threat landscape.

c. Training should be confirmed using a test with a minimum passing grade.

NOTE 1: Training should include topics such as credential best-practise (see below); identification of malicious emails and links; use of approved software; appropriate usage of the Internet; protection of data, information systems, devices in their care and safe use of social media.

NOTE 2: It may not be practical for all employees to conduct privacy and security training. The Security Policy shall apply to anyone (employees, third-party contractors, directors, researchers, students, and volunteers etc.) who has access to personal health information, confidential business data or who can reasonably affect the security of systems with health information. Training shall include consequences for non-compliance.

NOTE 3: In some cases, physicians operate as legally independent from the clinics and hospitals in which they practise. It may not be practical to require successful completion of a test. In this case organizations may need to rely on including suitable contractual clauses that cover the physicians' obligations to complete the training according to the required frequency and comply with security policy including the need for an email address that has an appropriate vendor management validation system compliant with appropriate privacy regulations.

NOTE 4: Privacy legislation for each province may have additional requirements for topics that must be covered by the privacy and security training program. Organizations should consult their Privacy leads for guidance in both the province(s) in which they reside, and the province(s) in which they operate.

5.1.3 Security awareness programs shall include best practises for not sharing user IDs, passwords, or other means of accessing the healthcare information systems with other users regardless of the organization's credentialling process.

NOTE: The nature of the health care working environment may not allow for the use of passwords. For example, within an operating theatre it may not be practical for a physician to use a keyboard. In these cases, other authenticators such as smart cards may be employed. This requirement is that, regardless of what is used for authentication, all users shall be instructed to not share these authenticators with each other. As another example: physicians within a clinical setting must not allow administrative staff or locum physicians to access the information system with their credentials. Instead, the information system must provide the authorized staff member with unique accounts configured with only the permissions required for the staff to do their job.

**5.2 Phishing**

5.2.1 Organizations who use email services shall implement a training program that includes social engineering threats, such as phishing, vishing, spear phishing and business email compromise as part of ongoing training.

NOTE: In some cases, it may not be practical to conduct phishing simulation exercises, for example when clinicians are using personal email addresses. In this case organizations may need to rely on traditional training approaches for security awareness and include phishing in the topics covered.

### 5.3 Credential hygiene

5.3.1 The organization shall incorporate credential hygiene in their security training program.

5.3.2 The organization shall implement a password manager.

5.3.3 The organization shall implement strong password authenticators in accordance with the best practices available to their system, and to implement multifactor authentication to augment password authenticators wherever possible.

5.3.4 The organization shall enforce password changes upon suspicion or evidence of compromise.

## 6 Technology controls

### 6.1 Data protection

6.1.1 The organization shall implement controls that can detect and prevent data leaks and data loss.

6.1.2 The organization shall ensure that sensitive data such as personal health information is protected when it is in transition from on-premises infrastructure to the cloud environments during initial load and (as in the case of hybrid environments) thereafter.

NOTE: As more services move to the cloud, care should be taken to protect data in cloud environments. Many cloud providers allow tenants to encrypt data using client managed keys to prevent exposure of sensitive data to the cloud administrators.

6.1.3 Organizations shall have a procedure to consider data encryption methodologies to protect sensitive data in motion, data at rest, and data in use.

6.1.4 The organization shall ensure that data collected and stored by various OT and medical devices are also protected at storage in the device and in transit to other IT environment (e.g. cloud) by following industry standard encryption practices.

### 6.2 Reduce personal health information use

6.2.1 The organization shall maintain testing environments that are segregated from production environments.

6.2.2 The organization shall take care to reduce or eliminate the use of production data in lower environments.

6.2.3 The organization shall ensure that when production data cannot be eliminated in a non-production environment, these environments have security controls that meet or exceed the production environment.

NOTE: Some jurisdictions will have requirements around methods of de-identification of PI/PHI, and consent for use of de-identified data. Check with your legal / Privacy lead.

6.2.4 Sensitive production data used in the testing environment shall be anonymized where possible.

### 6.3 Backups

6.3.1 The organization shall backup information, including personal information/ personal health information and ensure they are properly conducted, maintained, and tested.

6.3.2 Backups that contain personal health information shall be stored in encrypted format.

6.3.3 The organization shall backup systems that contain essential business information and ensure that recovery mechanisms effectively and efficiently restore these systems from backups.

6.3.4 The organization shall store backups at a secure offsite location (either physically or via network separated cloud services) at regular intervals to provide diversity in the event of a disaster (fire, flood, earthquake or localized cyber security incident).

6.3.5 The organization shall ensure that resiliency plans address the required recruitment process outsourcing and recovery time objectives for all critical systems.

6.3.6 The recovery point objective shall consider patient safety impact if the data does not include the most current modifications.

6.3.7 Recovery time objectives should also consider the impact on patient safety and continuity of care when critical systems and networks result in patient data being unavailable.

6.3.8 Resiliency plans shall address alternate approaches when recovery time objectives cannot be met.

6.3.9 The organization shall configure critical OT system to ensure OT systems and data are backed up securely.

6.3.10 The organization shall test all data backups on a regular basis to validate the backup and recovery procedures.

### 6.4 Resiliency – uptime

6.4.1 The Resiliency program of an organization shall at minimum include Business Continuity Plan (BCP), Crisis Communication Plan, Disaster Recovery Plan, Cyber Incident Response Plan, etc.

6.4.2 The organization shall define Maximum Tolerable Downtime (MTD), Recovery Time Objectives (RTO) and Recovery Point Objects (RPO) based on the criticality of systems, impact of potential outage of the system and in accordance with organization’s resource availabilities.

6.4.3 The organization shall maintain appropriate level of backup and recovery configurations or strategies (such as hot/warm/cold disaster recovery sites, disk mirroring, cloud vs. on-premises recovery) that support each system’s RTO/RPO and prevent unnecessary outages and downtime.

6.4.4 The organization shall continue to maintain its Resiliency Program by undertaking regular exercises, drills and tests that are aimed at confirming RTOs and RPOs and updating the plans accordingly.

### 6.5 Build books, recovery plans for all critical systems

6.5.1 The organization shall provide for the recovery of the system to a known state within the recruitment process outsourcing and recovery time objectives after a disruption, compromise, or failure.

6.5.2 The organization shall ensure that the recovery plan is executed during or after a cybersecurity incident.

6.5.3 The organization shall ensure that critical systems allow for recover time objective and recovery point objective in their design, build books and recovery plans.

### 6.6 Recovery exercises

6.6.1 The organization shall conduct recovery exercises and disaster recovery testing on a periodic basis.

6.6.2 The organization shall use a sampling of backup data to test and verify recovery procedures at regular intervals to ensure the integrity of the end-to-end backup and restoration process.

6.6.3 The organization shall determine on a case-by-case basis what business information and software (including but not limited to sensitive information) is essential to the functioning of the organization, and how frequently this information changes.

NOTE: As an example, critical workstations and servers may require daily incremental back-ups, whereas desktops may be recovered from one common image.

6.6.4 The organization shall determine on a case-by-case basis what systems to back up and at what frequency since every system will have different back-up and recovery requirements.

6.6.5 The organization shall backup systems that contain essential business information and ensure that recovery mechanisms effectively and efficiently restore these systems from backups.

6.6.6 The organization should consider the use of encrypted backups with securely stored and recoverable key material. Decryption keys and/or unencrypted backups should be stored securely and should be accessible only to authorized employees or officers.

6.6.7 The organization shall use a sampling of backup data to test and verify recovery procedures at regular intervals to ensure the integrity of the end-to-end backup and restoration process.

6.6.8 The organization shall ensure that recovery exercises do not create an exposure of production data.

## 7 Health care technology considerations

### 7.1 Software considerations

7.1.1 The organization shall have and apply data privacy and security patches for all software, hardware and devices installed to protect assets from known vulnerabilities.

NOTE: This includes patch management of critical information technology systems as well as

operational technology.

7.1.2 The organization shall enable automatic updates for all software and hardware when it is safe to do so or document all instances where they make the business decision not to do so.

NOTE: This includes all servers, laptops, desktops, tablets, mobile phones, network equipment products and medical devices.

7.1.3 The organization shall have a procedure to ensure regular manual updates for software, hardware and devices that are not capable of automatic updates.

7.1.4 The organization may establish a testing procedure to ensure patches do not cause a disruption or impact patient safety if a risk analysis determines that such a capability is a sensible risk reduction measure.

### 7.2 Network controls

7.2.1 The organization shall implement appropriate network protection strategies, including firewall, port security, network access controls, remote access controls, wireless access controls, zero trust architecture, cloud network security, etc.

7.2.2 Network segmentation practices shall be adopted to prevent malicious or unauthorized lateral movement activities, including but not limited to, ensuring health care technology, OT and IT are not on the same network.

### 7.3 Legacy technology and compensating controls

7.3.1 The organization shall obtain and review periodic of reports *from the authority having jurisdiction or pre-market approved vendors* concerning cybersecurity vulnerabilities, and device changes and compensating controls required to implement.

NOTE: Examples of authority having jurisdiction include *Health Canada (for approved medical devices in Canada) and from the FDA (in the United States).*

7.3.2 The organization shall perform a risk assessment whether to replace systems incapable of receiving updates.

7.3.3 A resulting risk treatment plan shall be used to document compensating controls to reduce the risk of maintaining legacy technologies.

### 7.4 Cloud

7.4.1 The organization shall evaluate their risk using cloud service providers, cloud services and/or outsourcing IT services, and shall evaluate their risk tolerance level with how their outsourced IT providers handle and access sensitive information.

NOTE: Organizations typically rely on outsourced IT service providers or MSPs for services such as their cloud storage and processing needs, the management and/or hosting of their website, and the management of their online payment systems. It is important for organizations to consider their risk tolerance level with the regulations within the legal jurisdictions where their outsourced providers store or use their sensitive information.

7.4.2 The organization using cloud applications and/or outsourcing IT services shall:

a. require that all their cloud service providers share an AICPA SSAE 18 or equivalent report that states that they achieved Trust Service Principles compliance or provide a documented business case as why they chose not to;

   NOTE: The organization determines equivalence to AICPA SSAE 18 has been met.

b. evaluate their risk tolerance level with the legal jurisdictions where their outsourced providers store or use their sensitive information;

c. ensure that their IT infrastructure and users communicate securely with all cloud services and applications;

d. ensure that administrative accounts for cloud services use multi-factor authentication and differ from internal administrator accounts;

e. ensure that data residency and local laws are respected;

f. ensure appropriate data deletion methods are in use;

g. ensure terms of service prevent cloud provider use of the data for other purposes; and

h. ensure access by cloud administrators is restricted (authorized by organization only) and audited.

7.4.3 The organization using cloud applications and/or outsourcing IT services shall conduct a privacy impact assessment and a have a vulnerabilities management process.

7.4.4 The organization shall establish a procedure to periodically review cloud systems that include a review of security controls, privacy controls and hardening guides. Exceptions shall be documented.

**7.5 Procurement / Vendor Management / Supply chain**

7.5.1 The organization shall have a comprehensive security risk assessment built into its procurement process, including considerations around the following:

a. Access management of data stored in third-party solutions or cloud based solutions;

b. Encryption methodologies and encryption key management;

c. Incident response, management and notification responsibilities and procedures meet expected due care;

d. Backup and disaster recovery procedures, including fail-over site and its location;

e. Sub processors or subcontractors that may have access to your data or environment and their due diligence;

f. Meta data that may be tracked and used without authorization;

g. Demonstration of third-party attestation of security standards or certifications; and

h. Commitment towards ongoing development and innovation to keep abreast with industry standard security requirements.

7.5.2 The organization shall secure assurance as part of the Master Service Agreement that their security practices are auditable, and that the third-party's practices result in a risk profile that complies with healthcare information protection laws and regulations.

7.5.3 All new agreements for suppliers shall include requirements to address the information security risks associated with the handling, processing and communicating of information or services. This includes the risk to the organization's information and its environment as well as any legal and regulatory requirements.

7.5.4 All new agreements with third-party providers that access, process, store or provide information systems and components shall be in compliance with the organization's security requirements and documented in a legal agreement.

7.5.5 The types of access that the third-party (e.g., IT service providers, software developers, financial services) will be allowed should be defined and documented.

7.5.6 Access to the organization's network as well as physical environment by the third-party provider shall be monitored. All third-party access should be routinely reviewed and revoked as necessary (i.e., on a monthly basis).

7.5.7 When buying software, the purchaser should request a bill-of-materials listing all supporting component software, libraries, and systems. The agreement should address the requirements for updating the component parts.

7.5.8 Contracts shall outline all notification requirements and responsibilities of the third-party provider in the Service Level Agreements, including acceptable notification timeframe given any suspected security issues.

7.5.9 The third-party provider's service delivery shall be monitored to assess whether the supplier is meeting appropriate business and security requirements and any contract or SLA requirements on an ongoing basis.

# 8 Cyber incident response plan and protocols

## 8.1 Planning

8.1.1 The organization shall develop, document and maintain a cyber incident response plan, including business continuity and disaster recovery plans.

8.1.2 The cyber incident response plan may detail steps for identifying, containing, and eradicating threats and recovering operations and system.

8.1.3 The cyber incident response plan shall include patient care and non-patient care system downtime procedures detailing manual and paper-based checklists and processes aimed at continuity and resiliency of day-to-day operations.

NOTE: As an example, direct patient care settings will require a paper-based system downtime procedures to support workflows involving medication requests, lab tests, patient handovers, patient transfers, etc.

8.1.4 The cyber incident response plan, including system downtime procedures and disaster recovery plan, are tested and validated on an annual basis.

## 8.2 Incident response team

8.2.1 The cyber incident response plan shall detail roles and responsibilities for handling the cyber incident. At minimum, cyber incident response team will include an incident manager, technical lead, human resources lead, communications lead, a scribe, cyber security and privacy subject matter experts.

8.2.2 The organization shall consider including a legal counsel or breach coach that is an expert at handling cyber incidents to help manage breach investigation, notification, and communication.

8.2.3 The organization shall determine which cyber incident response activities and services can be undertaken internally and which actions can be outsourced.

8.2.4 All third-party incident response and recovery service provider(s) shall be identified by the organization as part of the incident response plan with details of service requirements in the form of service level agreement.

### 8.3 Communications

8.3.1 The organization shall develop a cyber incident communication plan or protocol detailing incident communication strategies for incident response team members as well as internal and external stakeholders.

8.3.2 The communication plan shall include notification requirements and procedures for internal staff, clinicians, and caregivers on site. Alternate method of communication shall be identified to ensure multiple mode of communication for internal staff are available.

8.3.3 The organization shall identify and appoint a protocol for communicating with and responding to patient, family, community, partner, and media.

8.3.4 The organization shall consider including draft internal and external notification templates within the cyber incident communication plan.

### 8.4 Engaging cyber security government bodies and law enforcement

8.4.1 The organization shall include instructions on contacting or engaging law enforcement and other provincial, territorial, and federal government body that provides guidelines on cyber security.

8.4.2 The organization shall report all incidents where there is potential for moderate risk or risk of financial or public harm due to cyber crime to law enforcement.

### 8.5 Notifications – Regulatory and Contractual Requirements

8.5.1 The organization shall identify and develop procedures for notification to those affected of cyber incidents resulting in unauthorized access, use, disclosure or removal of personal information or personal health information.

8.5.2 Requirements and procedures for notifying the office of the applicable provincial or territorial or federal information privacy commissioner shall be developed as part of the incident response plan.

8.5.3 Requirements and procedures for notifying data subjects affected by the cyber incidents shall be developed and included as part of the incident response plan, in line with the applicable privacy law.

8.5.4 Where applicable, the organization shall implement procedures to include cyber incidents as part of the Annual Reporting of Privacy Breach Statistics to the applicable Information Privacy Commissioner.

8.5.5 The individual notification of personal information or personal health information shall include information as required by the applicable provincial or territorial or federal privacy law.

NOTE: For example, a notification letter to an individual affected by a cyber incident may require the following information: date, time and duration of the breach, description of the breach, description of the information affected by the breach, the steps taken to control or reduce the harm, further steps planned to prevent future breaches, etc.

8.5.6 The organization shall be prepared to notify cyber incidents to its partners, vendors, external stakeholders, and third-party service providers as per its contractual obligations.

8.5.7 Cyber incident reporting obligations outlined in its various contractual agreements with its partners, vendors, external stakeholders, and third-party service providers can be identified and tracked in a pro-active manner to meet notification requirements.

### 8.6 Testing and Training

8.6.1 The organization shall run table-top exercises and mock cyber incident scenarios with its incident response team and senior executive members annually.

8.6.2 The organization shall test, revisit, and revise its incident response plan, system downtime procedures, disaster recovery plan and communication plan periodically.

8.6.3 The organization shall consider providing necessary education to its Governing Body so that the Governing Body is aware of its oversight responsibilities during a cyber event.

### 8.7 Insurance

8.7.1 The organization should consider purchasing a cyber security insurance policy that includes coverage for first party losses such as incident response, recovery and forensics related activities or provide rationale for not purchasing one.

## 9 Contingency planning

### 9.1 General

9.1.1 The organization implementing an emergency code procedure shall include in “Code Grey – Critical Infrastructure Failure” procedures for responding to loss of communication systems including both phone and data system failures.

### 9.2 Manual processes and templates

9.2.1 The organization shall prepare for code grey and loss of data systems by preparing a procedure or manual (possibly paper-based) for ensuring patient safety.

NOTE: Examples include paper-based forms accessible in the event that computerized patient intake systems are offline.

9.2.2 Procedures for backfilling data when systems are back online shall be documented in code grey procedures.

### 9.3 Staffing redeployment

9.3.1 Procedures for redeploying staff when systems are offline shall be documented in code grey procedures.

### 9.4 Loss of telecommunications

9.4.1 The organization shall prepare for loss of data systems by ensuring that there is an emergency copy of critical and lifesaving data available in the case of a network outage.

NOTE: Examples: Hospital B uses a redundant server with a recent copy of all patient chart data that is capable of working in “offline” mode. Hospital A will run a nightly print to paper of all patient medication information.

9.4.2 The organization should plan for loss of telecommunication links by ensuring that there is emergency radios or cell phones in the case of an outage.

9.4.3 The organization should plan for loss of computing systems by planning for high availability using redundant networks, redundant data copies, and redundant systems.

### 9.5 Loss of power can lead to computer systems not being available

9.5.1 The organization should plan for loss of power using Uninterruptable Power Supply (UPS) systems.

NOTE: The management of UPS systems may require access to network for monitoring.

9.5.2 Emergency shutdown procedures for non-critical systems shall be documented in the case of unstable or unreliable UPS technology.

9.5.3 The organization shall take into consideration redundant power supply protocols to manage the risk to power management infrastructure which directly impacts safety and availability of healthcare. Smaller organizations with no critical devices may plan for UPS alone. Large organizations shall consider OT cybersecurity elements to protect the power management infrastructure which is critical for safety and availability.

### 9.6 Loss of virtual care technologies

9.6.1 The organization shall include in their emergency procedures a plan for continuity of care for those patients who are not receiving in-person care. These patients may be using, for example, digital health solutions for virtual visits, or remote patient monitoring.

## 10 Monitor and measure

### 10.1 Monitoring

10.1.1 The organization shall implement necessary processes to log, detect and review anomalous activities and cyber related activity monitoring associated with OT and IT environment, including:

a. Collect and retain necessary system, firewall, network, and event logs.

b. Establish baseline systems, networks, and communication channel activities.

c. Establish a process to correlate data collected to identify potential anomalous activities.

d. Establish severity and priority levels for identified anomalous activity.

e. Determine threshold for initiating a formal cyber incident response.

10.1.2 The organization shall consider implementing a continuous security incident and event monitoring to identify cyber incidents in a timely manner. Where possible, automatic alerting of anomalous activities can be established.

10.1.3 The organization shall segregate IT and OT assets based on criticality and use within the healthcare organization, ensuring network or equipment used for patient care is isolated from the organization's business systems.

10.1.4 The organization shall monitor and assess impact of zero-day security vulnerabilities that can be exploited by cyber criminals and follow necessary vendor recommendations to address the vulnerability in a timely manner.

**10.2 Penetration testing**

10.2.1 The organization shall consider undertaking penetration testing on a periodic basis to identify potential vulnerabilities and to establish effective vulnerability management processes.

NOTE: There are various types of penetration testing and vulnerability assessments available to organizations, including internal, external, web application, and Wi-Fi penetration testing, configuration assessment, etc.

10.2.2 Where appropriate, organization shall implement necessary OT focused cyber risk/vulnerability assessments and penetration tests.

NOTE: Some OT devices may fail during penetration testing and/or vulnerability scanning. Extra care is required when dealing with OT devices to avoid possible issues.

The approach to penetration testing and vulnerability scanning in OT environments should be responsible and cautious, considering the potential consequences of device failure. Methodologies differ from standard penetration tests and vulnerability scans because of the peculiarities of OT devices. For instance, MRI/X-ray/Dialysis machines would not be tested in the same way as a regular IT device.

**10.3 Red / Blue team exercise**

10.3.1 The organization shall consider undertaking simulated exercise using Red team and Blue team to train staff to recognize targeted attacks and defend against such attacks.

### 10.4 Threat hunting

10.4.1 The organization shall consider undertaking proactive activities to determine cyber threats that are undetected in its environment.

10.4.2 Threat hunting activities can be supported with on-going knowledge gleaned from various national and international cyber intelligence, including, known attack tactics, and indicators of compromise.

10.4.3 The organization should participate in information sharing groups to increase their awareness of the evolving nature of cyber threats, to improve their capacity to act and improve their resilience.

# Annex A
# (Informative)

## A. Why are Healthcare organizations highly targeted?

Healthcare organizations use and depend on vast amounts of technology and devices to provide direct patient care and indirect patient care supportive services. Historically, security features have not always been built into healthcare technology environment and devices. Additionally, healthcare organizations often fail to apply patch updates or upgrades due to complex issues such as lack of resources, issues around system dependencies and interdependencies, and operational impact/inconvenience associated with extended system downtimes. Healthcare organizations also struggle to prioritize investing in cybersecurity controls or processes due to lack of funding.

Furthermore, ever-changing and evolving threat landscapes have increased threats of cyber attack due to supply chain compromises and operational technology (OT)/industrial control system (ICS) assets.

This leaves the cyber criminals with a broad attack surface comprising of outdated and vulnerable infrastructure environment and a workforce that can be easily exploited and hacked. In addition, when faced with a cyberattack, healthcare organizations are often willing to negotiate and work with cyber criminals upon cyber attack to get the systems back up and running and to avoid privacy breaches.

**Why is Personal Health Information (PHI) so attractive to cyber criminals?**

Personal Health Information (PHI) is considered the most sensitive personal information about an individual with higher sensitivity and risk than credit cards and other financial information about a person. Healthcare organizations collect and store tremendous amount of PHI and sensitive information that can be harmful to individuals if stolen or tampered with. Financial information breach or loss can be replaced or dealt with through activities such as fraud prevention. Breach or loss of PHI cannot be recovered, changed, or replaced.

Cyber criminals use PHI for financial gains the following ways:

- Encrypting and denying access to critical information systems and subjecting healthcare organizations to extortion demands in exchange for decryption keys to gain control back of the affected systems.
- Exfiltrating personal health information and sensitive information and extorting money from healthcare organizations by threatening to publicly disclose such information or promising to delete data that was stolen during a cyber attack.
- Selling financial information combined with PHI in Dark Web, which can be then used to create fake identities.

# Annex B
# (Informative)

## B. Case Study

Provided below is a case study detailing the cyber attack and associated considerations around cyber breach management. This case study intends to inform the reader of the type of risks, impacts and costs that can result from a cyber attack.

**Cyber Attack:**

**Initial attack vector**

An administrative staff received a phishing email with a malicious document containing a macro. When the staff member opened the document, the macro installed multiple malwares, including a ransomware variant known to encrypt and steal data.

Several servers were either encrypted or experienced data corruption. This ultimately impacted the clinical operations of the healthcare organization. Many clinical documentation systems were switched to manual operations and healthcare services were redirected to other healthcare organizations. Email and telephone communications were affected temporarily due to internet access loss.

Fortunately, backups were not affected. A ransom demand was observed in relation to the obtaining decryption key and instructions. The healthcare organization decided not to pay for the decryption key as they were able to restore their systems from available backups.

**Second wave**

Several days after restoring the systems from backups, the threat actor involved in this malware attack sent the ransom demand of $1M USD for the deletion of stolen data from their environment via email to a number of healthcare email addresses. The healthcare organization engaged a forensic firm to investigate potential data exfiltration. The forensic investigation showed evidence of exfiltration of data from several servers. The healthcare organization hired an organization to communicate with the threat actor to obtain proof that the threat actor has actually stolen data from its environment. Following the receipt of the proof of data exfiltration from the threat actor, the healthcare organization decided to pay ransom to have the stolen data deleted.

Following a number of interactions between the breach coach, threat actor, a forensic firm and a ransom negotiator, the healthcare organization was able to negotiate ransom payment down to $300,000 USD. Following the payment of agreed amount, a confirmation was received from the threat actor that the exfiltrated data was deleted. the healthcare organization commenced an e-discovery process to identify the information that was exfiltrated.

Simultaneously, the respective provincial/territorial Information Privacy Commissioner’s office was informed of the ransomware attack incident and data exfiltration.

**Important Considerations:**

**1. Communication**

The healthcare organization reported the incident to its insured within a few hours of discovering the anomalies in their system. With the help of its legal counsel, external breach coach, insurer, media relations and communications department, the healthcare organization-initiated notifications to its Board of Directors, partners, and community. Staff members were communicated through the fan-out process that was in place – as per the Incident Management System (IMS). A message was posted on the website about the unexpected system downtime and the related impact on services.

With the help of the breach coach, several scripts were prepared to respond to questions from stakeholders, partners, patients, families, and the media.

**2. Clinical Impact**

The healthcare organization had a centralized physician order entry system, which was taken offline. This resulted in reverting to paper orders for physician interventions (e.g., treatment orders, medication managements, admissions/discharge, lab test orders, diagnostic imagine orders, etc.). There were potential delays in disseminating clinical information to the circle of care, new referrals, etc. The medication management processes had to be completed manually, including ordering, dispensing, manual logging of inventory of control substances, restocking, management of stat orders, etc. While the systems were down, alternate measures were taken to verify and address care issues and data inaccuracies.

**3. Remediation & Recovery**

The healthcare organization had ~3,500 endpoints and ~300 physical and virtual servers. The organization did not have a segregated operating network; therefore, the whole network was thought to have been compromised. Multiple cybersecurity vendors were brought into complete forensic investigation, isolate and remove the malware. Servers and endpoints were rebuilt from backups or images.

Additional layers of security were implemented to ensure endpoints could continue to be monitored and/or future malware executions were prevented or quarantined. The organization improved its email filtering and web filtering capabilities, widely rolled out multi-factor authentication, implemented network segregation and segmentation of networks, and added stricter firewall rules. In addition, all user passwords were changed.

**4. Overall cost implications:**

Provided below are the type of expenses the healthcare organization incurred as a result of this ransomware attack. Total cost estimated to have been around $5M CAD:

- Ransom payment ($300USD)
- Ransomware containment
- Recovery of systems from backups
- Third-party forensic investigation cost
- New software costs required for intrusion detection
- New software for containment/remediation

- System downtime cellular data usage cost
- Breach coach/legal consultation fees
- Other professional services costs such as breach coach, cybersecurity consultants
- Patient, regulatory, community, partner and stakeholder communication and notification costs
- Additional hardware costs (e.g., replacement of old servers that are no longer useable)
- IT Staff costs for overtime
- Data recovery staff time cost (e.g., manual data entry)
- Additional clerical support during downtime
- Additional clinical staffing required to handle patient care (e.g., to reduce wait time)
- Revenue loss due to diversion of care
- Capital costs associated with software, hardware, and ongoing support requirements (e.g., Firewall, Multi-factor authentication, VPN, End point detection and response, etc.)
- IT vendor costs associated with restoration of systems and data

# Annex C
# (Informative)

## C. Incident response plan template

NOTE: This template is sourced from CAN/CIOSC 104:2021.

### C.1 Scope

C.1.1 This Incident Response Plan applies to all networks, systems, and data, as well as members of the organization including employees and contractors, as well as vendors that access the networks, systems, and data of the organization. Members of the organization who may be called upon to lead or participate as part of the Incident Response Team are to familiarize themselves with this plan and be prepared to collaborate with the goal of minimizing adverse impact to the organization.

C.1.2 This Incident Response Plan assists an organization with establishing incident handling and incident response capabilities and determining the appropriate response for common security incidents that will arise.

### C.2 Requirements

C.2.1 Any employees, contractors, consultants, temporary or other workers of the organization and its subsidiaries that become aware of a data or of the possibility of a cyber security incident are to take immediate action by immediately informing their immediate supervisor and the appointed member of the senior leadership team overseeing the organizations IT security.

C.2.2 The following information is recorded when reporting a real or possible security incident (i.e., breach):

a. What happened;

b. Where the security incident occurred (i.e., in which department);

c. When the security incident occurred;

d. How and when the real or possible security incident was discovered;

e. Type of security incident (if known);

f. What equipment or sections of the information technology environment are impacted; and

g. Whether any corrective action has already been taken.

C.2.3 The appointed member of the senior leadership team overseeing the organization’s IT security verifies the circumstances of the real and/or possible security incident. The security incident or suspected security incident is reported upon discovery, with the above information completed.

C.2.4 The organization investigates all reports concerning a security incident using the PICERL (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned) process or an equivalent process (i.e., security incident handling process):

**a. Preparation**

i. In addition to a soft copy, the Incident Response Plan is always available in hard copy thus ensuring the Plan is always accessible irrespective of the status of the internal information technology infrastructure.

NOTE: The organization's retention policy addresses requirements and obligations for retaining documents and records and verification controls.

ii. The Incident Response Plan is reviewed and updated on an annual basis or after an incident has occurred.

iii. The appointed member of the senior-level leadership team overseeing the organization's IT security assembles a pre-determined team (i.e., security incident response team) deemed necessary to fulfil the security incident handling process.

iv. The security incident response team is listed in the incident response plan.

v. Any employees, contractors, consultants, temporary or other workers of the organization, including the security incident response team is provided with adequate training to ensure understanding of the security incident handling process and their roles within it.

vi. The appointed member of the senior leadership team overseeing the organization's IT security of the organization schedules annual training drills of security incidents with the security incident response team.

NOTE: This annual training will ensure that members of the security incident response team are familiar with the types of incidents in advance, will be prepared for the known so they may focus on the unknown, and so the plan, team, and tools are all fully tested.

vii. The documentation for the organization's information technology environment is kept up to date and always available such that it is accessible for reference, provides information on dependencies, and contains vendor information.

**b. Identification**

i. Any employees, contractors, consultants, temporary or other workers of the organization, including the security incident response team familiarizes themselves with the following security incident types:

- Unauthorized Use or Access
- Service Interruption or Denial of Service

- Malicious Code
- Network System Failures (widespread)
- Application System Failures
- Unauthorized Disclosure or Loss of Information
- Privacy Breach
- Information Security/Data Breach
- Other (i.e., any other incident that affects networks, systems, or data)

ii. The appointed member of the senior leadership team overseeing the organization's IT security determines the severity (see Table 1) of the incident taking into consideration whether a single system is affected or multiple, the criticality of the system(s) affected, whether impacting a single person or multiple, whether impacting a single team or multiple, or impacting the entire organization. The appointed member of the senior leadership team overseeing the organization's IT security considers whether a single business area or multiple and the impact of the incident. The appointed member of the senior leadership team overseeing the organization's IT security considers the relevant business context and what else is happening with the business at the time to fully understand the impacts and urgency of remediation.

iii. The appointed member of the senior leadership team overseeing the organization's IT security considers the available information to determine the known magnitude of impact compared with the estimated size along with likelihood and rapidness of spread. The appointed member of the senior leadership team overseeing the organization's IT security determines the potential impacts to the organization whether financial damage or brand and reputational damage or other harms.

NOTE: The security incident may be the result of a sophisticated or unsophisticated threat, automated or manual attack, or may be nuisance/vandalism.

iv. The appointed member of the senior leadership team overseeing the organization's IT security determines whether there is a vulnerability, whether there is an exploit, whether there is evidence of the vulnerability being exploited, and whether there is a known patch. The appointed member of the senior leadership team overseeing the organization's IT security determines if this is a new threat (i.e., day zero) or a known threat and the estimated effort to contain the problem.

| **Category** | **Indicators** | **Scope** |
|---|---|---|

| | | |
|---|---|---|
| **1 – Critical** | Data loss, Malware | Widespread and/or with critical servers or data exfiltration |
| **2 – High** | Theoretical threat becomes active | Widespread and/or with critical servers or data exfiltration |
| **3 – Medium** | Email phishing or active spreading infection | Widespread |
| **4 - Low** | Malware or phishing | Individual host or person |

**Table 1: Severity Matrix**

v. The appointed member of the senior leadership team overseeing the organization's IT security prepares a security incident communications plan such that during such an incident all contact information for the organization's staff, the security incident response team, and any relevant third parties, such as cyber security insurance vendors, is readily available.

vi. The appointed member of the senior leadership team overseeing the organization's IT security assesses the situation and determine if a privacy breach has occurred by answering the following two critical questions:

- **Is Personally Identifiable Information involved?** Identify the type of information affected by the incident in order to determine if a breach has occurred.
- **Has an unauthorized disclosure occurred?** Whether it is intentional, inadvertent or as a result of criminal activity, an unauthorized disclosure constitutes a privacy breach.

NOTE 1: If the answer is yes to both questions, a privacy breach has occurred.

NOTE 2: If a privacy breach has occurred, the organization may be required to report the privacy breach to the authority having jurisdiction.

vii. With the definition of Incident Type, Severity, and if a Privacy Breach has occurred or not, the appointed member of the senior leadership team overseeing the organization's IT security is now able to ascertain if a security incident has occurred. If it is concluded that a security incident has occurred, the following requirements of the incident response plan is followed.

viii. The appointed member of the senior leadership team overseeing the organization's IT security immediately assembles the security incident response team to further identify and gather data on the security incident.

ix. The security incident response team triages the security incident and document information gathered and decisions, including but not limited to:

- The original report of security incident, incident type, incident severity, privacy breach identification, and any actions taken;
- Analysis of the precursors and indicators;
- Research the possible matching known security incidents; and
- Any possible identification of actor, mechanism, application, attack vector, or other information which will assist in the containment and eradication of the root cause of the security incident.

**c. Containment**

i. The security incident response team documents all information gained and actions taken as they take the following actions to contain the security incident:

- Immediately isolate the security incident where possible, via isolation of the impacted infrastructure;
- Determine the source of the security incident, including what vulnerability was exploited;
- Immediately resolve any identified vulnerabilities or implement workarounds to mitigate the system(s) affected;
- Continue impact and damage assessment and confirm the scope of the incident;
- Determine what environment changes have made, such as but not limited to files, connections, processes, accounts, access, etc.; and
- Acquire, preserve, secure and document evidence and preserve chain of custody.

**d. Eradication**

i. The security incident response team documents all information gained and actions taken as they take the following actions to eradicate the impact of the security incident:

- Remove all traces of the infection or other incident;
- Identify and mitigate all vulnerabilities which have been identified during the investigation, whether they were exploited within this security incident or not;
- Remove malware, virus, inappropriate material, and other components introduced by the Security Incident. If necessary, utilize backup restore processes to ensure no trace of any malicious code exists within the environment;

- If more devices within the organization environment are discovered to be impacted, ensure to perform the identification steps on the newly identified examples, then rerun the containment process;
- Continue research and investigation until the full attack vector is understood; and
- Ultimately take all steps necessary to ensure the Security Incident cannot reoccur.

**e. Recovery**

i. The security incident response team documents all information gained and actions taken as they take the following actions to recover from the impact of the security incident:

- Return affected systems to an operationally ready state, one by one to ensure operation with reduced risk of the security incident reoccurring;
- Monitor each system brought online, and all environment network edge appliances, closely to ensure incident does not re-occur or is not still ongoing;
- Ensure systems are restored from a trusted and clean source;
- Confirm the affected systems are functioning normally; and
- Implement additional monitoring to look for future related activity if necessary.

**f. Lessons Learned**

i. The appointed member of the senior leadership team overseeing the organization's IT security is responsible for the creation of a follow up security incident report.

ii. The appointed member of the senior leadership team overseeing the organization's IT security meets with the security incident response team within 2 weeks to hold lessons learned meeting and to review the security incident report. The outcome of the lessons learned meeting include, but not be limited to:

- A walk through and review play-by-play of the security incident report;
- Understanding of how the security incident was detected, by whom, and when;
- Understanding of the scope and severity of security incident;
- Discuss the methods used in containment and eradication of the security incident;

- Identify any opportunities for improvement to better prepare for future security incidents; and
- Ensure accountability to follow up on identified opportunities.

iii. The outcome of the lessons learned meeting are documented and stored with the security incident documentation.

# Annex D
# (Informative)

## D. Cyber security risk assessment questionnaire

The following cyber security risk assessment questionnaire is targeted at raising awareness within healthcare organizations. It is not intended to provide feedback or an overall risk score. The member of the senior-level leadership team appointed to oversee the organization's cyber security should consult cyber security experts to review and provide input into the risk assessment and in the selection of controls to safeguard against cyber security risks identified and assessed. For the purposes of this document, a policy is defined as the rules and procedures that need to be followed for all individuals using an organization's IT assets and resources. An answer of NO for any of the below questions could mean that your organization is at risk.

| | |
|---|---|
| 1. Are all IT and IT security roles and responsibilities clearly outlined in your organization? | YES/NO |
| 2. Does your organization have an incident response plan?<br>2a. Are OT devices (e.g., X-ray, dialysis machines, patient monitoring, etc.) included in an incident response plan? | YES/NO<br>YES/NO |
| 3. Does your organization have cyber insurance?<br>3a. If cybersecurity insurance exists, does your organization include OT devices in the insurance policy? | YES/NO<br>YES/NO |
| 4. Has your organization assessed the potential injury to the confidentiality, integrity and accessibility of information systems and assets? https://lih-cai.cse-cst.gc.ca/login/index.php | YES/NO |
| 5. Does your organization store or collect confidential data (credit cards, social security numbers, employee information, etc.)? | YES/NO |
| 6. Does your organization know its responsibilities under the Privacy Act? https://laws-lois.justice.gc.ca/ENG/ACTS/P-21/index.html | YES/NO |
| 7. Has your organization classified the data that is being stored? | YES/NO |
| 8. Does your organization train employees on your cyber security policies and procedures? | YES/NO |
| 9. Does your organization have a company policy for cyber security spending based on the total IT budget? | YES/NO |
| 10. Does your organization provide cyber security training for IT personnel? | YES/NO |
| 11. Is automatic patching turned on where possible? | YES/NO |

| | |
|---|---|
| 12. Does your organization have a policy for backing up and encrypting essential business data? | YES/NO |
| 13. Does your organization have a policy for strong user authentication? | YES/NO |
| 14. Does your organization have a policy for access control and authorization? | YES/NO |
| 15. Does your organization have a policy for securing websites? | YES/NO |
| 16. Does your organization have a security policy for mobility? | YES/NO |
| 17. Does your organization have a policy to establish basic perimeter defense?<br><br>17a. Does your organization have a policy to establish network segmentation between IT and OT firewall protocols? | YES/NO<br><br>YES/NO |
| 18. Does your organization rely on third parties for outsourced IT? (e.g. Cloud, SaaS, remote backups, etc.) | YES/NO |
| 19. Does your organization have a policy for outsourced IT services? | YES/NO |
| 20. Does your organization audit the current set of security controls at least once a year? | YES/NO |
| 21. Does your organization perform vulnerability and penetration tests on information systems and OT devices at least once a year? | YES/NO |

# Annex E
# (Informative)

## E. RACI

An effective security program emphasizes that everyone has a role to play and clarifies how each person is responsible for security. While high level policy statements are important, additional details about roles and responsibilities can be captured in a RACI matrix to improve clarity on exactly who (either role or team) is accountable for each aspect of security.

Segregation of duties can be difficult to achieve for small organizations, where a single person is required to cover multiple roles. In these circumstances, the principle can still be applied by taking alternate approaches to having a second person aware of critical activities, such as:

- monitoring/alerting administrator actions (e.g., alerts can be set up to go to the manager whenever the IT person logs into administrator accounts).
- peer reviews and signoffs to approve changes to production.

The RACI (Responsible, Accountable, Consulted and Informed) ensures that various security functions are clearly identified and assigned ownership within the organization.

Definitions of the RACI terms are provided below.

| Term | Definition | Answers the question… |
|---|---|---|
| **Responsible** | Individual or team who will have to do the work to complete the task or implement the control successfully. This includes responsibility for the sustainment of or operationalizing the solution. | Who is getting the task done? |
| **Accountable** | Individual who is ultimately responsible for a subject matter, process or scope. This person is accountable for the success of the security control or task, and has the final say on if the implementation of the security control meets the intended goal. | Who is accountable for the success of the task? |
| **Consulted** | Individual or team whose opinions are sought on an activity (two-way communication). These are key roles that provide input. Note that it is up to the accountable and responsible roles to obtain information from any other applicable groups, but input from the **consulted** roles listed should be considered and, if required, taken for action. | Who is providing input? |
| **Informed** | Individual who is kept up to date on the progress of an activity (one-way communication). Informed individuals are not providing approval but are informed of the achievements and/or deliverables of the task. These individuals need to be | Who is receiving the |

| | | |
|---|---|---|
| | kept in the loop on the progress of the activities, rather than roped into the details and ongoing operations. Note that the accountable and responsible roles shall also be informed. | information/output of the activity? |

The roles outlined at the top, the activities in the first column, and the completed template are provided as an example only. Every organization is different, and it is important that the roles be clearly aligned to departments/teams in your organization for clarity.

Each team represented in the RACI should have the opportunity to review, understand, and approve their part in ensuring information security for the organization. Below is a sample of what a RACI matrix may look like.

| Activity | CISO | Security Team | LOB Operation Support | IT Team / Help Desk | Exec leadership Team |
|---|---|---|---|---|---|
| **Security Strategy** | A | R | C | C | I |
| Planning for the currency of Information systems and infrastructure | I | I | | A/R | C |
| **Security Risk Assessment** | A | R | A ( R ) | C/I | |
| Conduct Threat and Risk Assessments (TRA) as required | A | R | C | R | R |
| Ensure appropriate and timely approval of all information security policy exemptions, risks and risk mitigation plans. | I | C | R | I | A |
| Track and report to Exec Leadership Team / Management on the status of open security risks | A | R | C/I | C/I | I |

As the column headers, note any group that has a role to play in the security of the organization, including the Lines of Business (LOB), managed service providers (MSPs), and managed security service providers (MSSPs).

The list below is not exhaustive but provided as a reference for activities to include in the RACI matrix.

- Security Strategy
    - Planning for the currency of Information systems and infrastructure
- Security Risk Assessment
    - Conduct Threat and Risk Assessments (TRA) as required
    - Ensure appropriate and timely approval of all information security policy exemptions, risks and risk mitigation plans.
    - Track and report to Executive Leadership Team / Management on the status of open security risks
- Security Awareness and Training
    - Develop, manage, and deliver annual privacy and security training

    - Provide role-based security training / mentoring for secure development
    - Role-based training for others (privileged users, finance, HR, etc.)
    - New hire training
- Phishing exercises
    - Ensure compliance with annual security training requirements.
- Security Policies
- Security Incident Response
    - Management of information security problems, incidents and breaches including security incident management
    - First level support
    - Incident Response External (LOB Service Desk) - first call, triage
    - Incident Response Internal (IT Service Desk) - first call, triage
    - IRP - Security Lead
    - SLA for third parties for incident response
    - Initiating the Insurance Claims Protocol
- Security Architecture
    - Research, decide, security solutions
    - Approve security solutions
    - Roadmap for delivery of security solutions
    - Deliver on the Security Roadmap
    - Provisioning of access to security tools
    - Ensures new systems integrate with security tooling
    - Develops metrics for security reporting
- Application Security
    - Internal security testing
    - External security testing
- Infrastructure Security

    - Maintain secure configuration of devices

- Security Operations
    - Enable information security monitoring / detection
    - Analysing and as appropriate correlating logs to detect potential information security breaches.
    - Applying security patches within designated time frame.
    - Digital Certificate management.  Domain registration.
    - Operating and monitoring anti-virus and anti-malware solutions.
    - Applying and monitoring end-point security controls. (expand to EDR)
    - Backup and restore functionality (on prem, in cloud)
- Network Security
    - Provisioning of security services according to security service definitions (in Security Architecture)
    - Configure Firewalls, Routers, Switches and Wireless
    - Changes to FW, Routers, Switches, Wireless
    - Configure infrastructure, and cloud infrastructure
    - Apply network segmentation between IT and OT networks
- Vulnerability Management
    - Conduct vulnerability scanning
    - Remediation of security vulnerabilities within an agreed to time frame.
    - Conduct penetration testing
- Regulatory compliance
    - Ensure security controls are implemented in support of the company's security goals and meeting regulatory compliance
    - Monitoring compliance to security controls
    - Monitoring vendor compliance to security controls
- Employee Lifecycle
    - Background checks

    - Employee Add, changes, moves
- Procurement
    - Reviews of new suppliers
    - Security risk assessment of vendors
    - Security clauses in contracts

# Bibliography

[1] CAN/CIOSC 103-1, Digital Trust and Identity – Part 1: Fundamentals

[2] Canadian Centre for Cyber Security. Baseline Cyber Security Controls for Small and Medium Organizations.

[3] Cyber Essentials UK

[4] Cyber Essentials New Brunswick

[5] Post Market Management of Cybersecurity in Medical Devices

https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

[6] IEC TS 62443-1-1:2009, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models

[7] ISACA. Cybersecurity Guidance for Small and Medium-Sized Enterprises, 2015

[8] ISACA. Implementing Cybersecurity Guidance for Small and Medium-sized Enterprises, 2015

[9] ISO 19731:2017, Digital analytics and web analyses for purposes of market, opinion and social research — Vocabulary and service requirements

[10] ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity

[11] ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary

[12] ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements

[13] ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls

[14] ITSAP.30.032, Best Practices for Passphrases and Passwords

[15] Open Web Application Security Project. Application Security Verification Standard.

[16] Open Web Application Security Project. Top 10 Vulnerabilities.

[17] National Institute of Standards and Technology (NIST) Cyber Security Framework

[18] Payment Card Industry. Payment Card Industry Data Security Standard (PCI DSS).

[19] The IASME Governance Standard for Information and Cyber Security