William Osler Health System

Privacy & Cybersecurity: Best Practices Reference Guide for Community Physicians and Small Health Care Organizations in Ontario

William Osler Health System

About this Reference Guide

Community health care settings often face challenges in managing their privacy and cybersecurity practices due to limited time, staffing, technical expertise, and budget constraints. At the same time, they are responsible for protecting sensitive Personal Health Information (PHI) of their patients and are increasingly being targeted by cyber threats. To help address these challenges, the **Information Security and Privacy team** at **William Osler Health System (Osler)** developed this guide to support community-based health care organizations across Ontario, including physician practices, interprofessional clinics, and other small health care settings (collectively referred to as "**Community Clinics**"), in strengthening their privacy and cybersecurity practices.

This reference guide is designed to help Community Clinics protect patient information without requiring specialized expertise in privacy or information technology. It provides clarity on Community Clinic responsibilities for safeguarding PHI under the ***Personal Health Information Protection Act*** **(PHIPA)** and outlines practical, achievable steps to reduce privacy and cybersecurity risk in day-to-day operations.

The guidance in this document is based on practical privacy and cybersecurity experience across healthcare organizations in Ontario and reflects regulatory expectations, lessons learned from real incidents, and common challenges observed in community clinical settings. It is not meant to be read from start to finish, and each chapter can be reviewed independently based on a clinic's role, responsibilities, and immediate needs. No prior privacy or cybersecurity expertise is required to use this document.

Throughout this document, readers will find:

- Plain-language explanations addressing specific privacy and cybersecurity concerns.
- Clearly identified action items outlining practical, achievable steps clinics can take.
- Self assessment checklists to help clinics understand what reasonable safeguards may look like in small clinical settings.
- References to relevant frameworks, standards, and guidelines used to explain why certain practices are recommended — without requiring formal implementation or certification.

Definitions and References

Key terms used in this document are defined in the Definitions section. A complete list of referenced source materials, standards and guidance documents are provided in the Reference section at the end of this document.

Important Disclaimer: Document Use & Distribution

This document provides practical guidance based on recognized standards and applicable regulatory requirements. Privacy and cybersecurity risks continue to evolve, and no reference guide can fully inform on how to eliminate all risks. Each organization remains responsible for implementing appropriate privacy and security safeguards based on its specific circumstances. This guide does not guarantee the prevention of privacy breaches or cybersecurity incidents, nor does it replace professional judgment, legal, technical, or regulatory advice. Osler assumes no liability for any direct or indirect losses resulting from the use of this document. This document is intended solely for the identified audience and must not be shared, reproduced, or distributed (in whole or in part) without prior written permission from Osler.

Frameworks, Standards and Guidelines ("FSG")

Certain frameworks, standards and guidelines ("FSG") are referenced throughout this guide to explain why certain privacy and security practices are recommended. The key cybersecurity FSG referenced include guidance from the following:

- **Canadian Centre for Cyber Security (CCCS)**;
- The **National Institute of Standards and Technology Cybersecurity Framework Version 2 (NIST-CSF 2.0)**;
- **ISO/IEC 27000 Series; and**
- **Ontario Health (OH)**.

Reference to these FSG does not imply a requirement for formal implementation or certification. Instead, they provide a structured and practical way to identify, assess, and manage risks associated with information systems and technology. These FSG help organizations focus on priority risk areas, how to take reasonable and proportionate steps, and demonstrate due diligence. This guide can be used effectively without detailed knowledge of these FSG. Alignment with these FSG also supports consistency with regulatory, insurance and industry expectations across Ontario and Canada.

Chapter 1 – Why Community Clinics are Prime Cyber Targets

Community Clinics are sometimes surprised to learn that they are at risk of cyber attacks. A common misconception is "we're too small to be a target." In reality, Community Clinics are targeted because they hold highly sensitive, permanent patient information and depend on uninterrupted access to clinical systems to deliver patient care. Cyber attackers exploit the urgency clinics face when systems go offline, knowing that delays in access to records, results, or schedules can directly affect patient care. This pressure to restore systems quickly is frequently leveraged during ransomware attacks, turning cybersecurity incidents into immediate clinical and patient safety challenges.

Figure 1 below illustrates a ransomware attack sequence in a clinical setting, demonstrating how a seemingly minor event, such as a single phishing email, can escalate into a significant operational disruption. The timeline progresses from left to right, highlighting how attackers may perform a ransomware attack on a Community Clinic, beginning with a simple phishing email and how a well-prepared clinic would respond and recover.

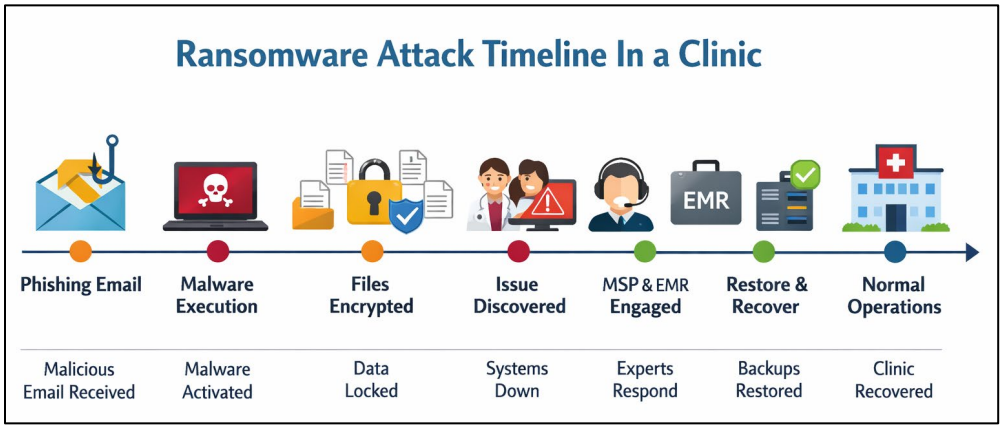

Figure 1: Ransomware Attack Timeline in a Clinic. Image generated using OpenAI (ChatGPT), 2026.

Chapter 2 – Protecting Community Clinics from Cyber Attacks

2.1 Common Cybersecurity Attacks Affecting Community Clinics

Community Clinics face many common cybersecurity threats that can disrupt patient care, expose sensitive information and impact daily operations. These threats often take advantage of busy clinical environments, limited technical resources, and the heavy reliance on digital systems for day-to-day Community Clinic operations. Cybersecurity incidents do not begin with highly sophisticated attacks. In many cases, they start with everyday habits and assumptions such as clicking on familiar-looking emails, using shared accounts, reusing passwords or assuming a vendor is fully responsible for security. Over time, these small gaps can quietly weaken a clinic's security posture. Understanding these common threats helps Community Clinics focus their efforts where they will have the greatest impact.

(i) Phishing, Email-Based Attacks and Social Engineering

Phishing is the most common entry point for cyber attacks. Attackers send emails that appear legitimate, such as referrals, invoices, lab results, or system notices to trick staff into clicking links or opening attachments. Once a staff member interacts with the message, attackers (threat actor) may steal login credentials or install malicious software. Community Clinics rely heavily on email for care coordination, communication with hospitals, and vendor interactions, making suspicious emails harder to spot during busy workflows.

Figure 2.1 (i) below illustrates the common elements of a phishing email, and the warning sings staff members should watch for.

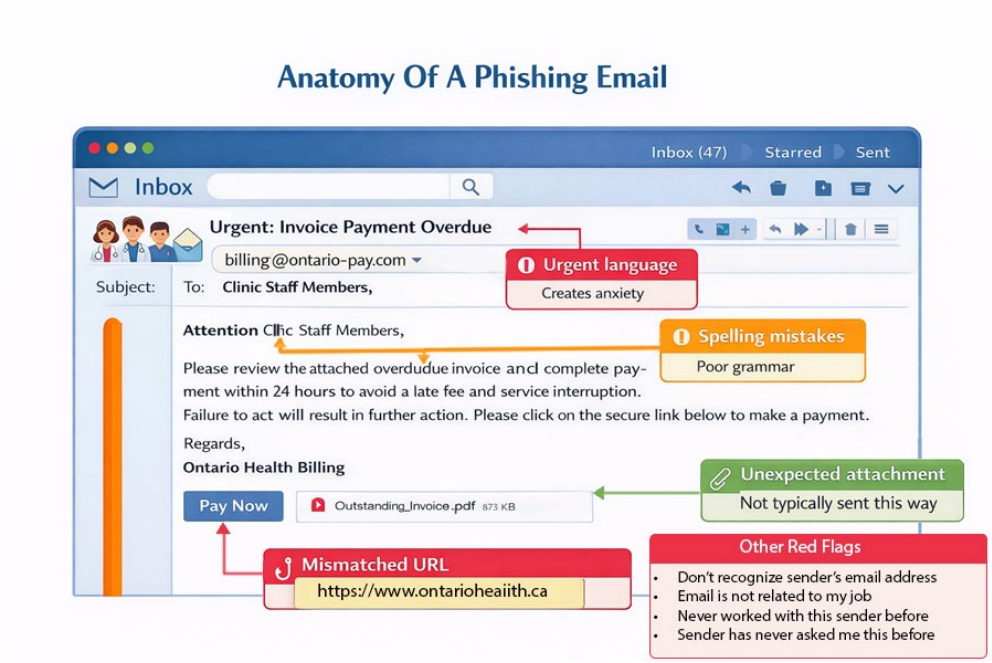

Figure 2.1 (i): Anatomy of a Phishing Email. Image generated using OpenAI (ChatGPT), 2026.

How to spot a Phishing Attempt

1. The email or call creates urgency or pressure; “act now”, “click here”, “your access will be removed”.
2. The domain of the email (after the “@”) is slightly misspelled or inappropriate for the sender.
3. Links or attachments seem odd or unexpected; don’t click or open them.
4. Asking for information, passwords, or access the sender shouldn’t need.
5. Sender uses a real name or department from the organization to sound legitimate.
6. Logos, signature, or layouts look blurry, stretched or out of place.

What is Social Engineering?

Social engineering relies on conversation and persuasion; convincing you to share information, click a link, or open an attachment. Social engineering can happen by phone, by text or other communication method. Figure 2.1 (ii) shown below demonstrates social engineering through text messages. Someone might call or message you pretending to be from another department or organization to gain your trust. Once they do, they might ask for your password, patient details, OR send a follow-up text or email with a link or attachment they want you to open. If a request seems unusual or unexpected, always verify the person's identity. Ask for their full name and employee ID or badge number, then call the organization they claim to be from using a verified, publicly listed phone number - not the one they give you.

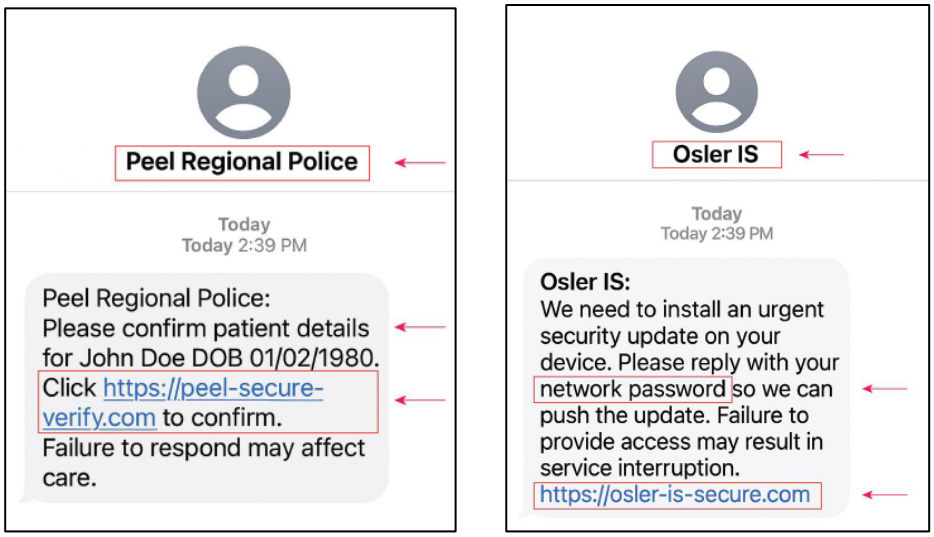

Figure 2.1 (ii): Example Social Engineering SMS Messages (Osler), 2026.

(ii) Ransomware

Ransomware is a type of malicious software that locks or encrypts clinic systems or files, preventing staff from accessing critical information until a ransom is paid. When a ransomware attack occurs, access to the Electronic Medical Records (EMRs), appointment schedules, billing systems, and other critical operational tools may be disrupted, often forcing a rapid transition to paper-based processes. Attackers understand that Community Clinics feel significant pressure to restore systems quickly to support patient care. This urgency is often exploited to help create pressure for paying ransom or making rushed decisions during a cyber incident.

(iii) Credential Theft and Account Compromise

Credential theft happens when attackers obtain usernames and passwords and use them to log in as legitimate users. Credentials are commonly stolen through phishing emails, weak passwords, or password reuse across multiple systems. Once inside systems, attackers may access patient records, send fraudulent emails from trusted accounts, or use the compromised account as a stepping stone to reach additional systems and data. Community Clinics are particularly vulnerable because staff often manage multiple systems and logins as part of their daily work.

(iv) Malware and Infected Devices

Malware is a malicious software designed to damage systems, steal information, or disrupt operations. In Community Clinics, malware is most commonly introduced through email with infected attachments, malicious links, visits to compromised or malicious websites, or by exploiting unpatched or outdated software. Once malware is installed on a clinic computer, it can spread to other devices on the same network, including systems that store or access PHI. This may result in unauthorized access to sensitive information, data theft, system slowdowns, or, in more serious cases, ransomware that encrypts files and makes systems unusable. Community Clinics are particularly vulnerable because clinic computers often run critical applications such as EMRs, imaging systems, and billing software, and they may not always receive timely updates or security protections.

(v) Third-Party and Vendor-Related Cyber Incidents

Community Clinics often rely heavily on external providers - such as an Electronic Medical Record (EMR) vendor, cloud storage providers, managed IT service providers, and billing or administrative platforms to store, access or process PHI on behalf of the clinic. While these services are essential to modern care delivery, they also introduce risks beyond the clinic's own systems. A common misconception is that vendors are fully responsible for protecting

information once services are outsourced. In reality, accountability for safeguarding PHI remains with the provider who sought the third-party service, that is, the accountability remains with the Community Clinic. Without proper oversight, this misunderstanding can create gaps in security monitoring, vendor accountability, risk management and incident response.

2.2 How to Protect Your Practice from Cyber Attacks

Protecting a Community Clinic from cyber attacks does not require expensive technology or advanced technical expertise. Once common risks are understood, many vulnerabilities can be addressed through a small number of practical privacy and cybersecurity safeguards:

- Administrative Safeguards
- Technical Safeguards
- Physical Safeguards

No single safeguard is enough on its own. Protecting patient information and clinic systems requires a combination of administrative, technical, and physical safeguards. When applied together, these safeguards reduce the likelihood of cyber attacks, limit the impact of security incidents, support continuity of patient care; and help clinics meet their privacy obligations under PHIPA. This chapter focuses on practical, high-priority safeguards that Community Clinics can realistically implement. Each section also includes a Self assessment checklist to help clinics confirm whether key requirements are in place.

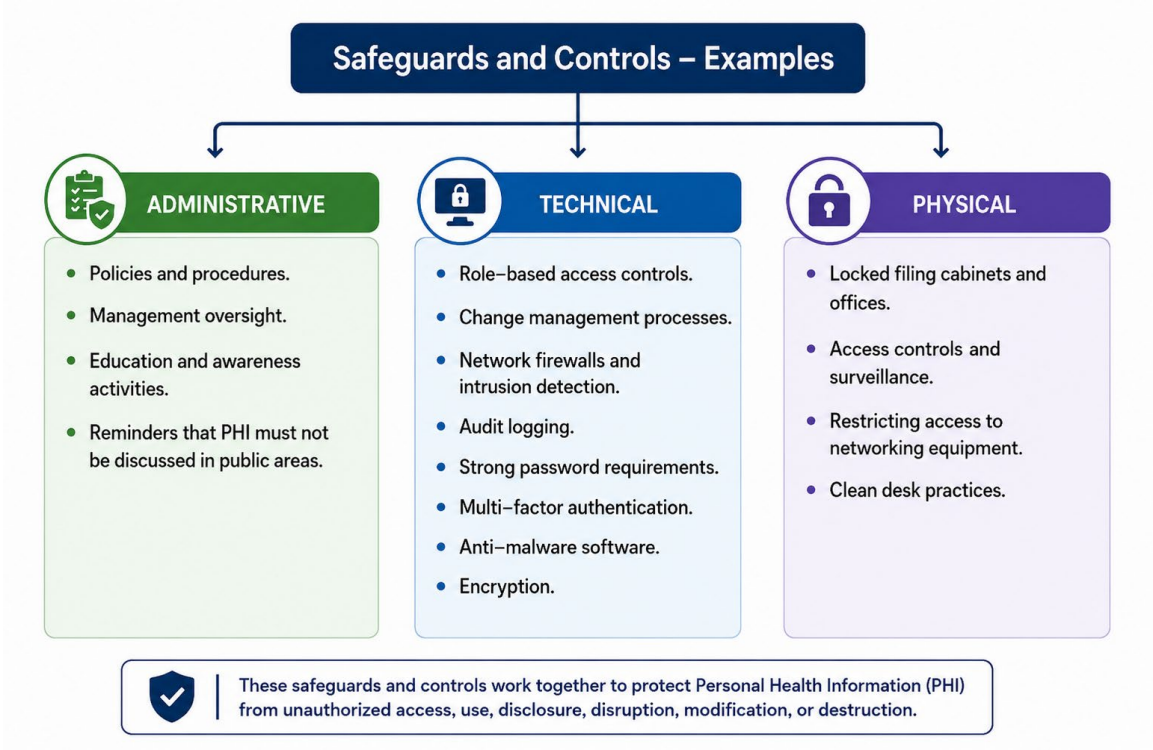

Figure 2.2: Safeguards and Controls. Image generated using OpenAI (ChatGPT), 2026.

2.2.1 Administrative Safeguards

(i) Policies and Procedures

Policies and procedures are the foundation of privacy and cybersecurity in a Community Clinic. These foundational documents explain how PHI is collected, used, accessed, disclosed, stored, retained, and securely disposed of during day-to-day operations. In busy clinic environment where staff often multitask and roles may overlap; written policies and procedures help provide standards for everyone to follow facilitating consistency in process. These administrative documents do not need to be long or complex to be effective. Simple, practical, clinic-specific policies covering topics such as privacy and confidentiality, email use, device security, access management, and incident reporting are often enough. Without clear policies and procedures, staff may rely on habit, memory, or informal guidance which increases the risk of privacy and cybersecurity breaches, inconsistent handling of PHI, delayed incident response, and operational confusion. Well documented and regularly updated policies and procedures also demonstrate due diligence under PHIPA by showing that the Community Clinic has taken reasonable steps to protect PHI and adapt to changes in technology, staffing, vendor relationships, and evolving regulatory expectations.

Self Assessment Checklist: Policies and Procedures

- ☐ Do we have written privacy and cybersecurity policies?
- ☐ Do our policies and procedures cover how PHI is accessed, shared, stored, and disposed of in day-to-day workflows?
- ☐ Do our policies provide guidance on incident reporting and incident management?
- ☐ Are policies reviewed and updated at least annually or when major changes occur?
- ☐ Do staff know where to find these policies and how to apply them in practice?

(ii) Assign Responsibilities and Management Oversight

Every Community Clinic should clearly identify who is responsible for privacy and cybersecurity, even when IT services are outsourced. Vendors may manage systems, but accountability for protecting PHI remains with the Community Clinic.

Management oversight means privacy and cybersecurity are treated as ongoing operational responsibilities, not just technical issues left to vendors. This includes reviewing user access, monitoring incidents or near-misses, assessing vendor performance, identifying risks and documenting decisions and follow-up actions. Effective oversight does not require technical expertise or constant monitoring; it simply means leadership knows who is responsible, what safeguards are in place, and when action is needed. Without clear oversight, clinics may miss security gaps, vendor failures or delayed incident reporting.

Self Assessment Checklist: Management Oversight

- ☐ Is a privacy and/or cybersecurity lead formally identified?
- ☐ Does leadership receive periodic updates on privacy and security issues?
- ☐ Are incidents and near-misses reviewed and documented?
- ☐ Are vendor responsibilities actively monitored rather than assumed?
- ☐ Are decisions and actions documented when risks are identified?

Figure 2.2.1 (ii) below illustrates that privacy and cybersecurity in a Community Clinic is a shared responsibility and is not the responsibility of one person, department or vendor alone. Instead, it requires shared responsibility, clear role assignment and ongoing management oversight across the organization.

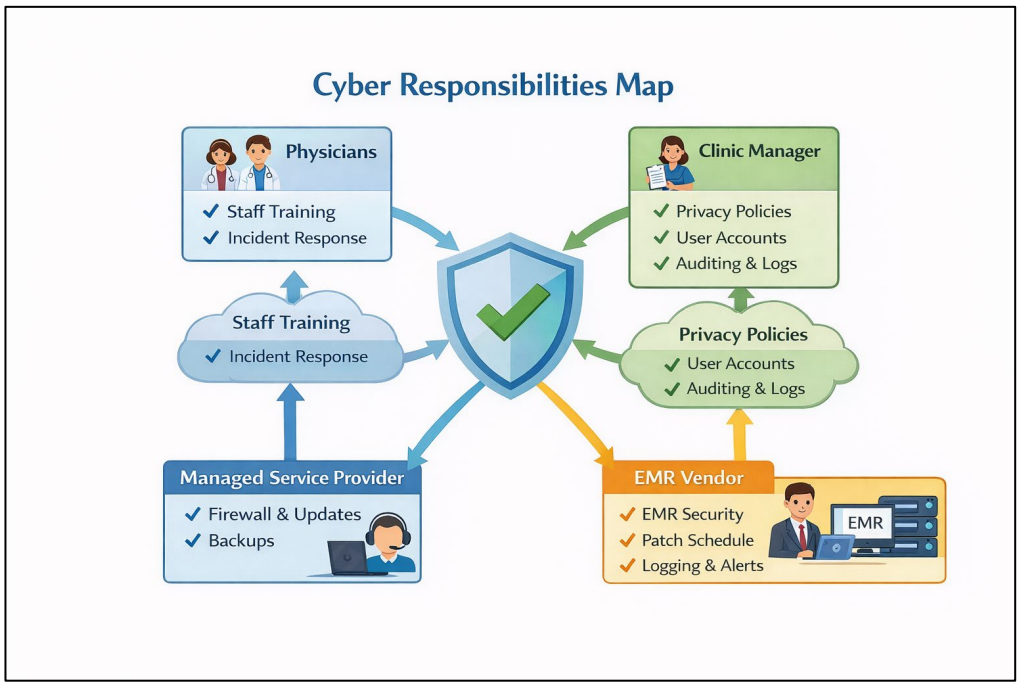

Figure 2.2.1 (ii): Cyber Responsibilities Map. Image generated using OpenAI (ChatGPT), 2026.

(iii) Education and Awareness

Staff training and awareness is one of the strongest defences against cyber attacks.

Training and awareness ensure that clinic staff understand common cyber risks, especially phishing and email-based attacks, and know how to respond safely during day-to-day work. In Community Clinics, email is a critical communication tool used for referrals, results, vendor messages, and scheduling. Because attackers deliberately design phishing messages to look familiar and urgent, technical controls alone are not sufficient. Staff who are appropriately trained to recognize and act on suspicious cyber activity are a crucial second line of defence.

Effective training does not need to be long or technical to be useful. Short, regular reminders, such as brief huddles, checklists posted near workstations, or quick refresher discussions are often the most effective. Clinics can also reinforce simple habits, such as checking sender addresses, hovering over links before clicking, verifying unusual requests; and reporting suspicious emails promptly. Short, regular reminders are often more effective than one-time or annual training. [1] [2]

Self Assessment Checklist: Training and Awareness

- ☐ Do staff receive regular training on phishing and email-based threats?
- ☐ Are short, practical reminders (e.g., five-minute huddles or posters) used instead of relying on one-time or annual training?
- ☐ Are real or relevant phishing examples discussed with staff?
- ☐ Are staff taught to check sender addresses and hover over links before clicking?
- ☐ Is there a simple, clear process for reporting suspicious emails (e.g., forwarding to a shared inbox)?
- ☐ Are staff encouraged to verify unusual payment or information requests by phone using known numbers?
- ☐ Are refresher sessions conducted periodically (e.g., quarterly)?

2.2.2 Technical Controls

(i) Strong Password Requirements

Stolen or misused passwords are one of the one of the most common ways cyber attacks begin. If an attacker gains access to a staff email or EMR account, they can impersonate clinic staff, access PHI, or launch further attacks. Strengthening identity and access controls through unique user accounts, strong passwords, and multi-factor authentication significantly reduces these risks and supports accurate audit logging and accountability, which are important for both security and privacy investigations. [3] [4] [5]

---

[1] **Ontario Health (OH)**, *Critical Cyber Security Controls*, including Secure Email and Strong Authentication, which emphasize layered protections supported by staff awareness.

[2] **Canadian Centre for Cyber Security (CCCS)**, *Email Security Best Practices*, which note that email is a common starting point for phishing and malware and recommend combining filtering, authentication, and user awareness.

[3] **Ontario Health (OH)**, *Critical Cyber Security Controls for Health Organizations* – Strong Authentication Control

[4] **National Institute of Standards and Technology (NIST)**, *Digital Identity Guidelines (SP 800-63)*, which recommend strong, unique authenticators and multi-factor authentication where risk is higher.

[5] **ISO/IEC 27001**, Information Security Management Systems – controls for unique user identification and access restrictions.

Self Assessment Checklist: Strong Password Requirements

- ☐ Does every staff member have a unique username and password?
- ☐ Is the minimum password length and complexity according to NIST guidance, favouring longer passphrases of 15 characters in place?
- ☐ Is password reuse discouraged?
- ☐ Is that same password use for work and home discouraged?
- ☐ Are unique accounts and passwords in place (no sharing of credentials between staff)?
- ☐ Are accounts disabled immediately when staff leave?

(ii) Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is a security control that requires users to verify their identity using more than just a password. MFA adds an extra layer of security by requiring users to verify their identity by sending a temporary code to a phone, email or generated by an authentication app. Even if a password is guessed, reused, or stolen through phishing, MFA can prevent an attacker from unauthorized access. MFA should be enabled for emails, EMRs, remote access, VPNs and administrative accounts. MFA is most effective when combined with unique user accounts and role-based access.[6] [7] [8]

Self Assessment Checklist: Multi Factor Authentication

- ☐ Is MFA enabled for all staff accounts, starting with physicians and managers?
- ☐ Is MFA required for high-risk systems such as email, EMR, VPN, and remote access?
- ☐ Does each staff member use a unique account (no shared logins)?
- ☐ Are strong passwords or long passphrases (15+ characters) required alongside MFA?
- ☐ Is access limited based on job role (role-based access)?
- ☐ Are access reviews performed at least quarterly to confirm who still needs access?
- ☐ Are separate, privileged accounts used for system administration?
- ☐ Are user accounts disabled promptly when staff leave the clinic?

(iii) Encryption

Encryption protects PHI by making data unreadable to unauthorized users if a device is lost, stolen, or accessed improperly. Encryption should be enabled on laptops, desktops, portable storage devices (such as USB drives), backup media, and cloud storage that contain or can

---

[6] **Ontario Health (OH)**, *Critical Cyber Security Controls for Health Care Organizations* – Strong Authentication and Cyber Threat Monitoring and Management controls.

[7] **National Institute of Standards and Technology (NIST)**, *Digital Identity Guidelines (SP 800-63)*, which recommend multi-factor authentication and strong authenticators to reduce credential-theft risk.

[8] **NIST Cybersecurity Framework (CSF) 2.0**, which emphasizes access control under the Protect (PR.AC) function and asset and identity awareness under the Identify (ID.AM) function.

access PHI. Encryption works automatically in the background and does not affect day-to-day clinical workflows. [9] [10] [11]

Self Assessment Checklist: Encryption

- ☐ Are all clinic laptops and desktops that store or access PHI encrypted?
- ☐ Is encryption enabled on USB drives and other removable storage devices?
- ☐ Is PHI restricted to approved systems (EMR, secure file servers, or encrypted cloud storage)?
- ☐ Are devices securely wiped or destroyed before disposal, reuse, or return to vendors?
- ☐ Is remote work enabled through clinic-approved solutions that prevent saving PHI on personal devices?

(iv) Audit Logging

Audit logging is the process of recording who accessed PHI, when access occurred and what actions were taken within clinical systems. Audit logs of solutions that process PHI are required and should align with requirements set out in section 10.1 of the *Personal Health Information Protection Act* (PHIPA). In Community Clinics, audit logs are generated automatically by systems and provide an objective record of user activity. Audit logs help a clinic detect inappropriate access, bulk exports and activity outside normal workflows. Audit logs are most effective when combined with unique user accounts and role-based access, as this allows activity to be traced back to individual users rather than shared accounts.[12] [13] [14] [15]

---

[9] **ISO/IEC 27001**, Information Security Management Systems – controls for data classification, encryption, and secure media handling.

[10] **Canadian Centre for Cyber Security (CCCS)**, *Baseline Cyber Security Controls*, which stress protection of mobile devices and removable media.

[11] **Ontario Health (OH)**, *Critical Cyber Security Controls*, including incident response expectations where encryption reduces breach impact.

[12] **Canadian Centre for Cyber Security (CCCS)**, *Baseline Cyber Security Controls for Small and Medium Organizations*, which recommend collecting, retaining, and analyzing logs to detect malicious activity.

[13] **Personal Health Information Protection Act (PHIPA)**, section 10.1, which outlines audit log requirements for electronic systems containing PHI.

[14] **NIST Cybersecurity Framework (CSF)**, Identify (ID) and Detect (DE) functions, emphasizing understanding users and monitoring for unusual access.

[15] **Ontario Health (OH)**, *Critical Cyber Security Controls*, including SIEM, Incident Response, Cyber Threat Monitoring, and Strong Authentication.

Self Assessment Checklist: Audit Logging

- ☐ Is audit logging enabled for all users in the EMR and other systems that store or access PHI?
- ☐ Does the EMR comply with PHIPA section 10.1 audit log requirements for systems containing PHI?
- ☐ Is the audit log exportable?
- ☐ Have we identified all systems that store or process PHI been identified (e.g., EMR, shared drives, imaging systems, cloud inboxes)?
- ☐ Does every staff member use a unique account (no shared logins)?
- ☐ Are logs enabled for system logins, record views, bulk exports, and printing?
- ☐ Is a designated role responsible for reviewing audit logs on a regular schedule (e.g., monthly)?
- ☐ Are criteria documented for when audit log findings trigger an alert, investigation, or incident review?

(v) Endpoint Protection

Endpoint protection refers to the security controls used to protect clinic workstations, laptops (including corporate issued mobile devices and tablets), and servers from malware, ransomware, and other malicious activity. In Community Clinics, endpoints are the devices staff use every day to access email, EMR, imaging systems, and shared files. Because these devices sit directly in clinical workflows, they are one of the most common entry points for cyber attacks. Modern endpoint protection tools work quietly in the background to detect and block common threats before they take hold. Automatic updates, restricted administrator privileges, and removal of outdated software further reduce risk. [16] [17]

Self Assessment Checklist: Endpoint Protection

- ☐ Do all clinic workstations, laptops, and servers have endpoint protection installed?
- ☐ Is endpoint protection managed centrally by the MSP or the clinic's IT function?
- ☐ Has the clinic standardized on a single, supported endpoint protection product?
- ☐ Are automatic updates enabled for endpoint protection tools and operating systems?
- ☐ Are local administrator privileges restricted to IT staff or MSP accounts only?
- ☐ Is obsolete or unsupported software and unused browser plugins removed promptly?

---

[16] **Ontario Health (OH)**, *Critical Cyber Security Controls*, including Endpoint Detection and Response (EDR) and Vulnerability Management.

[17] **Canadian Centre for Cyber Security (CCCS)**, *Baseline Cyber Security Controls for Small and Medium Organizations*, which recommend modern endpoint protection, automatic updates, and restricted administrative privileges.

(vi) Network Security

Network security focuses on how devices connect to each other and to the internet within the clinic. A Community Clinic's systems and network should be separated from any guest Wi-Fi, visitor devices and internet-connected devices that external users may access. Network segmentation ensures that even if someone gains access to a guest or shared network, they cannot easily reach clinical systems that store or access PHI. Basic network security protection includes using strong wireless encryption (such as WPA2 or WPA3), changing default router passwords, disabling unused networks, and clearly separating networks by trust level. [18] [19]

Self Assessment Checklist: Network Security

- ☐ Is there a separate guest Wi-Fi network with internet access only and no connection to clinic systems?
- ☐ Is the clinic Wi-Fi configured with a unique network name and a strong password shared only with staff?
- ☐ Is strong wireless encryption enabled (WPA2-Enterprise or WPA3 where available)?
- ☐ Have default router and network device administrator passwords been changed?
- ☐ Is access to network management restricted to authorized IT or MSP staff only?
- ☐ Are unused wireless networks and services disabled?
- ☐ Are networks separated by level of trust (e.g., clinical, guest, IoT devices)?

(vii) Backups and Recovery

Backups and recovery safeguards ensure that Community Clinics can restore systems and patient data quickly after ransomware, system failure, or any other system outages. For Community Clinics, "good enough" recovery means maintaining regular, tested backups, keeping systems patched, and using strong access controls such as Multi-Factor Authentication (MFA). At least one backup copy should be offline or immutable, meaning it cannot be altered or encrypted by ransomware. Backups should also be tested regularly so clinics know recovery will work when needed. Clinics must know *how* to restore data, and *which systems* must come back first to safely resume patient care.

---

[18] **Canadian Centre for Cyber Security (CCCS)**, *Baseline Cyber Security Controls for Small and Medium Organizations*, which emphasize network segmentation, secure configurations, and restricted access as foundational safeguards.

[19] **NIST Cybersecurity Framework (CSF)**, Protect (PR) function, which highlights secure network design and separation to limit unauthorized access and reduce cyber risk.

These controls work together to shrink the window of opportunity for attackers and provide a safe path to recovery without paying ransom. [20] [21] [22] [23]

Self Assessment Checklist: Backups and Recovery

- ☐ Is at least one backup copy that is offline or immutable maintained?
- ☐ Are backup schedules, storage locations, and retention documented in writing (e.g., by the MSP)?
- ☐ Are backups taken frequently for critical systems (e.g., daily for EMR data)?
- ☐ Are backup restorations tested at least quarterly and results documented?
- ☐ Are operating systems and major applications patched and updated regularly?
- ☐ Is MFA enabled for remote access, email, and administrative accounts?
- ☐ Is there an inventory of systems that must be restored first to resume safe patient care?
- ☐ Is responsibility for starting restoration during an incident clearly assigned?

(viii) Vendor and Cloud Oversight

Community Clinics often rely heavily on external providers and may assume that vendors are fully responsible for security. However, outsourcing services does not transfer accountability for ensuring appropriate safeguarding of PHI. Community Clinics should understand where PHI is stored, whether it is encrypted, how incidents are reported and who is responsible for responding. Having clear agreements, basic oversight, and shared understanding of responsibilities helps clinics manage these risks and demonstrate reasonable due diligence in protecting patient information. [24] [25] [26] [27]

---

[20] **Canadian Centre for Cyber Security (CCCS)**, *Ransomware Playbook* and *Baseline Cyber Security Controls*, which emphasize maintaining offline, tested backups and planning for recovery.

[21] **Ontario Health (OH)**, *Critical Cyber Security Controls*, including Backups, Disaster Recovery, Incident Response, Endpoint Detection and Response (EDR), Cyber Threat Monitoring, and Strong Authentication.

[22] **NIST Special Publication 800-40**, *Guide to Enterprise Patch Management Planning*, which frames patching as essential preventive maintenance to reduce exploitable vulnerabilities.

[23] **NIST Cybersecurity Framework (CSF)**, Recover (RC) function, which highlights recovery planning, testing, and improvement following incidents.

[24] **Canadian Centre for Cyber Security (CCCS)**, *Baseline Cyber Security Controls*, which expect leadership to assign responsibility, maintain asset awareness, and ensure policies and procedures are in place even when IT services are outsourced.

[25] **ISO/IEC 27001**, Information Security Management Systems, which include supplier security controls requiring organizations to define security requirements for vendors and monitor supplier performance.

[26] **Ontario Health (OH)**, *Critical Cyber Security Controls*, including Incident Response and Cyber Threat Monitoring and Management.

[27] **NIST Cybersecurity Framework (CSF) 2.0**, Govern (GV) function, which emphasizes clear roles, responsibilities, and oversight across internal and external partners.

Self Assessment Checklist: Vendor and Cloud Oversight

- ☐ Is a privacy or security lead identified to coordinate with vendors and track incidents?
- ☐ Is a basic due-diligence checklist used before adopting new cloud or third-party services?
- ☐ Does the vendor or MSP follow a recognized security framework or standard (e.g., ISO 27001, SOC 2, or equivalent)?
- ☐ Has the vendor provided evidence of security controls, such as an attestation report (e.g., SOC 2), certification, or security summary upon request?
- ☐ Does due diligence confirm where PHI is stored and whether it is encrypted at rest and in transit?
- ☐ Does the vendor maintain audit logs and provide access to logs or reports when needed?
- ☐ Are data retention and secure destruction practices defined for vendors?
- ☐ Can the vendor securely return or destroy PHI when the service ends?
- ☐ Do contracts with MSPs, EMR vendors, and cloud providers clearly reference PHI protection?
- ☐ Are vendor responsibilities documented (e.g., patching, backups, anti-virus, logging, monitoring)?
- ☐ Are breach notification responsibilities and timelines defined in vendor agreements?
- ☐ Is there a documented incident response process, and does the vendor clearly define how and when the clinic will be notified of an incident?
- ☐ Is there a documented process for patient breach notification and the IPC?
- ☐ Are regular reviews held with MSPs to discuss alerts, incidents, and planned improvements?

2.2.3 Physical Safeguards

Physical security is a critical part of protecting Personal Health Information (PHI) and clinic systems. While cyber attacks are often thought of as remote or digital events, many incidents begin with unauthorized physical access to clinic devices and infrastructure.

In a Community Clinic environment, devices such as routers, switches, servers, workstations, laptops, and backup media are all potential access points to sensitive information. If an attacker or unauthorized individual gains physical access to these systems, they may be able to bypass technical controls, install malware, extract data, or disrupt operations.

Physical safeguards do not need to be complex or expensive. In most cases, they involve basic controls, awareness, and consistent day-to-day practices. At minimum, Community Clinics should ensure the following high-priority physical safeguards and controls.

Key physical safeguards include the following:

Restricting access to critical equipment

Networking equipment such as routers, switches, and server hardware should be located in locked rooms, cabinets, or secured areas, with access limited to authorized personnel only (e.g., MSP or designated staff). These systems should not be placed in open or publicly accessible areas such as reception, hallways, or shared workspaces.

Controlling access to workstations and clinical areas

Devices used to access EMRs, email, or shared drives should not be left unattended in publicly accessible areas. Staff should lock workstations when stepping away, even briefly, especially in high-traffic areas.

Protecting sensitive information in physical form

Notes containing passwords, system access details, or PHI should never be written on sticky notes, whiteboards, notebooks, or easily visible locations. Printed documents containing PHI should be securely stored, not left unattended on desks or shared spaces.

Securing portable devices and storage media

Laptops, tablets, USB drives, and external hard drives should be locked away when not in use and never left in vehicles, waiting rooms, or unsecured areas. These devices are easily lost or stolen and may contain or provide access to sensitive information.

Managing physical access to the clinic environment

Clinics should take reasonable steps to prevent unauthorized individuals from accessing restricted areas. This includes awareness of behaviors such as tailgating, where individuals follow authorized staff into secure areas without proper access. Additionally, surveillance technologies can identify suspicious activities and deter unauthorized intrusion.

Visitor awareness and supervision

Visitors, vendors, and service providers (including cleaning staff or maintenance personnel) may have physical access to clinic spaces. Clinics should ensure that access is limited, supervised where appropriate, and aligned with confidentiality expectations.

Protecting equipment from environmental risks

IT equipment should be protected from physical hazards such as water damage, overheating, fire, or power instability, which can lead to system outages and data loss.

Physical safeguards work best when combined with administrative and technical controls. Together, they help reduce the likelihood of unauthorized access, prevent avoidable incidents, and support continuity of care in the event of a disruption.

Self Assessment Checklist: Physical Security

- ☐ Is IT hardware reasonably protected from theft, tampering, and environmental damage (fire, water, overheating, power issues).
- ☐ Are employees trained on recognizing tailgating (unauthorized access to an area by walking close behind someone who is authorized, often by catching doors before they close)?
- ☐ Are employees informed on "clean desk" practices (not leaving out sensitive documents or notes)?
- ☐ Do employees know to never physically write passwords in places easy to see (e.g., sticky notes, white boards)?
- ☐ Are portable storage devices (e.g. USB drives, external hard drives) locked away?
- ☐ Is physical access to server rooms, networking equipment (e.g., routers, switches), and offices with sensitive data impeded by appropriate locks, enforced badge access, and/or biometrics?
- ☐ Is access to clinic workspaces and systems controlled to prevent unauthorized entry (e.g., locked doors, monitored areas)?
- ☐ Are laptops and mobile devices secured when unattended and not left in public or unsecured areas?
- ☐ Are visitors and third parties appropriately supervised or restricted when accessing clinic areas?

Chapter 3 – Privacy Legislation

Privacy is a fundamental right. It is the right or ability of an individual to control or influence the ways in which information about them is collected, used, and disclosed.

PHIPA (the *Act*) governs PHI within the healthcare sector and sets out what is required by health information custodians (HICs) to protect PHI. The *Act* balances the privacy rights of individuals with the legitimate need of HICs to collect, use and disclose PHI for the delivery of effective and timely health care. PHIPA is technology-neutral but requires reasonable safeguards.

PHIPA provides the following: (1) individuals a right of access to PHI about themselves and (2) to request a correction or amendment to their PHI, (3) requires a mechanism be in place for independent review and resolution of complaints related to PHI and (4) provides remedies for non-compliance.

Who is Subject to PHIPA?

Persons or organizations subject to PHIPA are health information custodians (HIC) as defined in section 3 of the *Act* and include for example, a health care practitioner or a person who operates a group practice of health care practitioners. A HIC has custody and control of patient/client information and must have in place **Information Practices** that comply with the requirements of the *Act* and its regulations.

Note: In Ontario, the Information and Privacy Commissioner of Ontario (IPC) oversees compliance with PHIPA to ensure those subject to the *Act* abide by the privacy principles and requirements set out in law. See the "About Us" page for the Information and Privacy Commissioner of Ontario for more information.

Consent

Consent to collect, use or disclose PHI must be express or implied. Express consent is required when using or disclosing PHI outside the purpose for which it was originally collected, when not permitted by PHIPA.

PHIPA does permit various uses and disclosures of PHI provided specified requirement are satisfied including conducting research; planning, evaluating, and managing the health system; maintaining a registry of PHI to improve the provision or quality of health care; and protecting and promoting public health.

Individuals have a right under PHIPA to provide express instructions to limit or restrict how their PHI may be used or disclosed for health care purposes. However, information withheld

by express instructions such as a consent directive (lockbox) or confidential status are still subject to disclosure when required or permitted by law.

Examples that do not require consent to use or disclose PHI are provided below. Disclosure should be limited to the minimum to achieve the intended purpose.

- Reporting a child in need of protection to a Children's Aid Society
- Information to diagnose, investigate, prevent, treat, or contain communicable diseases to Public Health
- Reporting sexual abuse, misconduct to a regulated health professions college
- Births and Deaths to the Registrar General
- Name, address, and condition of any person who has a condition that may make it unsafe for them to drive to the Registrar of Motor Vehicles
- Other reporting requirements including the disclosure of PHI to eliminate or reduce a significant risk of serious bodily harm to the patient or others

Responding to Privacy Incidents and Breaches

Figure 3 below provides a simple step-by-step roadmap for responding to privacy incidents and breaches, aligned with guidance from the **Information and Privacy Commissioner of Ontario** (IPC) and the **National Institute of Standards and Technology (NIST)**. Having a clear and practical incident response process helps clinics act quickly, protect patients, maintain continuity of care, and demonstrate due diligence.

Even with appropriate security measures in place to protect PHI there may be an incident that results in a breach of patient/client information. A privacy incident is a suspected privacy breach or a situation that could result in a privacy breach. A privacy breach occurs when PHI is stolen, lost, accessed, collected, retained, used, disclosed, or disposed of in ways that do not comply with PHIPA. When a privacy breach occurs, you should take immediate steps to respond to the breach.

Example of Privacy Breaches:

- Looking up a patient no longer in your Circle of Care
- Looking up records of a co-worker, neighbour, family, friend or high-profile patient out of curiosity
- Records for Patient A are provided to Patient B
- Sharing private work-related information with those not privy
- Posting patient information to social media without consent
- Overriding a consent directive (lockbox) without appropriate authorization
- Taking a photo or recording without consent
- Lost or stolen health records

Note: Shared systems such as Ontario Health's ConnectingOntario only permit access for the provision of care or assisting in the provision of care. No further uses such as quality management, risk management or research are permitted. It is important that a Privacy Lead in your clinic review the terms of use and/or contract to shared systems before allowing access to ensure your clinic policy aligns with who gets permissions to the system and allows for appropriate use of data contained within a shared system.

You must have a privacy breach response protocol in place. Privacy law requires the following steps outlined below to occur when a privacy breach is identified. Additionally, you must maintain a privacy breach log (document and track privacy breaches) and report annual privacy breach statistics to the IPC.

The IPC outlines the following breach response steps:

Contain (actions taken to limit exposure) – identify the scope of the breach and take steps to ensure no information has been retained by unauthorized parties to limit further exposure of PHI and/or alleviate consequences for both the individual(s) whose information was involved and the clinic. Put measures in place to mitigate additional risk during the investigation period e.g., revoke access.

Investigate – conduct an investigation to understand fully what happened, why it happened and how to prevent it from happening again; the identify the root cause(s) and consider the contributing factors to help determine how to prevent recurrence.

Notify affected individual(s) as soon as feasible – can be direct (verbal, written) or indirect e.g., notice (only in certain circumstances); notification must include privacy breach details, type of PHI at issue, steps taken to address the privacy breach, how to make a complaint to the IPC, and your office contact information. The investigation need not be fully concluded to report a privacy breach to impacted parties.

Remediate (action taken to prevent recurrence) – reduce the risk of a similar future privacy breaches by solutioning based on the root cause(s). Some examples include simplifying processes, updating policies and training material, or staff responsible for the breach taking privacy training again.

Report to the IPC when required – https://www.ipc.on.ca/en/health-organizations/report-a-privacy-breach

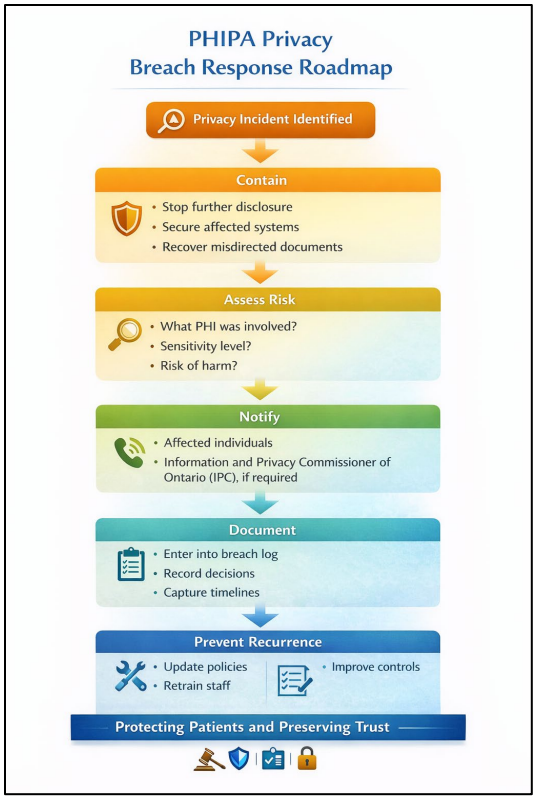

Figure 3: PHIPA Privacy Breach Response Roadmap. Image generated using OpenAI (ChatGPT), 2026.

3.1 Incident Identification

A privacy incident is any situation where PHI may have been exposed or mishandled. This includes suspected breaches, near misses, or unusual activity that requires investigation. A privacy breach occurs when PHI is collected, used, disclosed, retained, or disposed of in a way that does not comply with PHIPA. This includes theft, loss, and unauthorized access, collection, use, disclosure, copy, modification or disposal. Common examples include misdirected faxes or emails, lost or stolen devices, unauthorized access or snooping, suspicious system activity, ransomware or malware alerts or vendor notifications involving clinical data.

Self Assessment Checklist: Incident Identification

- ☐ Is a privacy incident and breach policy in place?
- ☐ Do staff know what is a privacy incident or near miss privacy breach?
- ☐ Is there a clear, blame-free way for staff to report concerns?
- ☐ Is a privacy or administrative lead identified to receive privacy incident reports?
- ☐ Are privacy incidents reported promptly, even when details are incomplete?
- ☐ Is documentation started as soon as an incident is suspected?

3.2 Contain the Incident

Once a privacy incident is identified, the clinic's first obligation is conduct a preliminary assessment to identify the scope of the breach including who and how many people are impacted and what (including which systems) have been compromised in order to appropriately contain the incident and determine next steps.

Containment will help prevent further inappropriate access, collection or disclosure of information mitigating additional risk or exposure. Containment actions may include securing affected systems, disabling user access, recovering misdirected documents, shutting down compromised accounts, or contacting vendors or IT support.

Under PHIPA, clinics are expected to act as soon as feasible, even while facts are still being gathered.

Self Assessment Checklist: Containment

- ☐ Are immediate steps taken to stop further access, collection, use or disclosure?
- ☐ Can user accounts or system access be disabled quickly if needed?
- ☐ Are misdirected documents recovered or restricted promptly?
- ☐ Are MSPs or vendors contacted without delay when systems are involved?
- ☐ Are containment actions documented?

3.3 Investigate

After initial containment, conduct a fulsome investigation to understand the full scope of the breach. Whether conducted internally or with the assistance of external experts, the investigation should aim to determine what happened, why it happened and how to prevent it from happening again. To prevent recurrence, identify the root cause(s) which will inform the remediation strategy.

Self Assessment Checklist:

- ☐ Has the type of PHI involved been identified?
- ☐ Is the number of affected individuals known or estimated?
- ☐ Have the events that led to the breach been identified and analyzed?
- ☐ Have you determined whether the breach was an isolated incident or a systemic issue?
- ☐ Was the source of the breach and its root cause(s) identified?
- ☐ Have you examined organizational privacy measures, such as existing policies and procedures and training?
- ☐ Have steps been taken to assess and evaluate the adequacy of privacy and security measures, including a review of the organization's information management practices in relation to the circumstances of the breach?

- ☐ Was IPC guidance used to support the assessment?

3.4 Notify When Required

If the incident involves PHI and is deemed a privacy breach, PHIPA requires notification to affected individual(s) and, in certain circumstances, to the Information and Privacy Commissioner of Ontario (IPC). Notification must occur at the first reasonable opportunity when required and must include specific information. Not all incidents are reportable, but clinics must be able to show that notification obligations were considered and documented using IPC's seven reportable breach categories. **Report to the IPC when required –** https://www.ipc.on.ca/en/health-organizations/report-a-privacy-breach

Self Assessment Checklist: Notification

- ☐ Was it determined whether individual notification is required?
- ☐ Was it assessed whether IPC notification is required?
- ☐ Do patient/client notifications include required details (what happened, PHI involved, steps taken, contact info)?
- ☐ Are notification decisions documented, including reasons not to notify?
- ☐ Print the list of situations where you must notify IPC of a privacy breach on the "Report a privacy breach" page and attach it to your binder for quick reference.

3.5 Document the Incident

Documentation is a core administrative safeguard under PHIPA. Every privacy incident should be recorded in a Privacy Incident Log. An incident log creates an official record of what happened, what actions were taken, systems involved (if any), actions/decisions made and follow-up measures, and why decisions were made. Proper documentation demonstrates that the clinic took reasonable steps and allows for review, learning, and regulatory accountability.

Self Assessment Checklist: Documentation

- ☐ Was the incident entered into the Privacy Incident Log?
- ☐ Are timelines, systems involved (if any), and actions clearly recorded?
- ☐ Are decisions and rationales documented?
- ☐ Is the log stored securely and accessible only to authorized reviewers?

3.6 Remediation

Responding to a privacy incident does not end with patient/client notification and IPC notification (where required). PHIPA expects clinics to take reasonable steps to prevent similar incidents in the future. This completes the incident response process. This may

involve updating policies, retraining staff, improving controls, changing workflows that contributed to the incident. Change made are based on the analysis of the events that led to the privacy incident/breach, and the root cause(s).

Self Assessment Checklist: Remediation

- ☐ Were root cause(s) identified?
- ☐ Were relevant policies or procedures updated where needed?
- ☐ Was staff retraining completed where appropriate?
- ☐ Were technical or administrative controls improved?
- ☐ Were improvements communicated to staff?

Chapter 4 – Practical Privacy and Cybersecurity Tips

Most privacy and cybersecurity incidents in Community Clinics do not result from sophisticated attacks or intentional misuse. They typically arise from everyday operational pressures — for example, sending a fax or email too quickly, selecting the wrong recipient, storing information in the incorrect location, or relying on informal workarounds that gradually become routine.

The chapter provides some practical privacy and cybersecurity tips to support your practice and facilitate compliance in your practice with the PHIPA legislation. The following represent minimum expected behaviours in Community Clinics.

4.1 Keep Patient Information Where It Belongs

Personal Health Information (PHI) should live in **approved clinical systems**, not in email inboxes, downloads folders, or personal devices. In practice, privacy risk increases every time information is copied, saved locally, or shared outside the EMR or approved secure platforms. Clinics can reduce risk by minimizing where PHI exists.

Practical tips

- ☐ Work directly in the EMR whenever possible
- ☐ Avoid saving PHI to desktops, shared drives, or download folders
- ☐ Use secure portals instead of attaching PHI to emails
- ☐ Clean up local files and downloads regularly

4.2 Be Careful in Public and Semi-Public Spaces

Privacy risks are not limited to digital systems. Hallways, waiting rooms, printers, and shared spaces are frequent sources of unintentional disclosure.

Practical tips

- ☐ Avoid discussing patient information in hallways, waiting rooms, elevators, or reception areas
- ☐ Position monitors away from public view or use privacy screens where space is tight
- ☐ Retrieve printed documents immediately
- ☐ Lock filing cabinets, offices and rooms when not in use

4.3 Slow Down During High-Risk Moments

Many privacy breaches occur during moments of urgency such as faxing results, emailing referrals, or rushing to finish tasks at the end of the day. These moments require extra attention, not speed. Building in small pauses at key points can prevent serious incidents.

Practical tips

- ☐ Double-check recipients and address every time before sending emails or faxes
- ☐ Pause before clicking "send" on emails containing patient information
- ☐ Use a two-person check for highly sensitive information (e.g., mental health, communicable disease status)
- ☐ Encourage staff to stop and ask when something feels unusual

4.4 Use Email Carefully

Email is convenient but risky. Many privacy breaches involve misdirected emails, auto-complete errors, or compromised inboxes. Clinics should clearly define what is appropriate for email—and what is not.

Practical tips

- ☐ Use regular email only for low-sensitivity content
- ☐ Never send detailed clinical notes by regular email
- ☐ Double-check recipients before sending
- ☐ Never log into EMR from links in emails
- ☐ Report suspicious emails immediately

4.5 Protect Devices Like Prescription Pads

Laptops, tablets, USB drives, and phones are powerful tools—but also common sources of privacy incidents when lost or stolen.

Practical tips

- ☐ Use only encrypted clinic-approved devices for PHI
- ☐ Never leave devices unattended in cars or public places
- ☐ Lock screens when stepping away, even briefly
- ☐ Avoid using personal devices for clinic work unless formally approved
- ☐ Report lost or stolen devices immediately

4.6 Use Shared Systems Only for Care Purposes

Shared systems such as ConnectingOntario or regional EMRs permit access only for providing or assisting with patient care. Additional uses such as quality improvement, Curiosity, learning, or convenience are not valid reasons for access.

Practical tips

- ☐ Access patient records only when involved in the patient's care

- ☐ Do not "check up" on friends, family, or public figures
- ☐ Remember that all access is logged and reviewable
- ☐ Ask if unsure whether access is permitted

4.7 Report Early, Even If You're Not Sure

A strong privacy culture encourages early staff reporting of concerns and near misses to the Privacy Lead, where actions can be reviewed for compliance with PHIPA. Reporting is about preventing harm, not assigning blame.

Practical tips

- ☐ Report suspected incidents or near misses immediately
- ☐ Use the clinic's incident reporting process instead of "fixing it quietly"
- ☐ Encourage colleagues to raise concerns

4.8 Make Privacy and Security Visible

Privacy and Cybersecurity works best when they are part of daily routines, not hidden in long policies.

Practical tips

- ☐ Post phishing red-flag reminders near workstations
- ☐ Keep breach reporting instructions easy to find
- ☐ Include brief privacy reminders in team huddles
- ☐ Review anonymized incidents periodically to reinforce learning

4.9 Privacy Management Program and Accountability

While the practical tips above focus on everyday actions, sustained privacy and cybersecurity protection requires a structured program. At a minimum, every Community Clinic should establish and maintain a Privacy Management Program that brings together administrative, technical, and physical safeguards with clear governance and accountability. A privacy management program is combination of the policies, processes, and actions that you can use to protect Personal Health Information or PHI, comply with requirements under PHIPA, and build trust with patients. The checklist below provides a practical starting point.

Checklist: Privacy Governance and Accountability Action Items

- ☐ Foster a culture that embodies foundational privacy principles.
- ☐ Assign clear roles and responsibilities.
- ☐ Inventory your information – know what is in your custody and control.
- ☐ Establish good record–keeping practices.

- ☐ Use a systematic approach to assessing new or changes to information management systems, programs or technologies that can identify and mitigate privacy risks.
- ☐ Choose Third Party Service Providers carefully – consider privacy and security when working with third–party service providers, such as electronic medical record providers, and build these into your contractual agreements.
- ☐ Ensure your staff have the proper privacy knowledge and skills on an ongoing basis and make sure to regularly update your training materials.
- ☐ Have staff sign privacy and confidentiality agreements and re–attest to them on an annual basis. Attestation should include that they understand and commit to following the privacy policy and legislation.
- ☐ Ensure staff understand the consequences of not following privacy expectations/ policies, ranging from learning opportunities and retraining to possible disciplinary action and legal consequences.
- ☐ Ensure data recovery plans are in place and prepare how you will resume operations in the event of significant business interruptions.
- ☐ Ensure appropriate retention and destruction policies are in place. Ensuring secure disposal of health records: Out of sight is not out of mind! | Information and Privacy Commissioner of Ontario

Appendix: Definitions

Access Controls

Technical and administrative measures are used to ensure that only authorized individuals can access systems, applications, or information, such as unique user accounts, role–based permissions, and authentication requirements.

Administrative Safeguards

Non–technical measures used to protect Personal Health Information (PHI), including policies, procedures, training, governance, contracts, and management oversight.

Asset Inventory (Asset Management)

A documented list of devices, systems, software, and cloud services that store, process, or access PHI, including ownership, location, and purpose.

Audit Logging (Audit Logs)

System–generated records that capture user activity, such as logins, record access, exports, and configuration changes, to support accountability and oversight.

Backups

Copies of data created to allow restoration of systems and information, following data loss, system failure, or cyberattack.

Business Email Compromise (BEC)

A cyberattack in which an attacker gains access to or impersonates a trusted email account to commit fraud, steal information, or manipulate communications.

Call Tree

A predefined list of internal and external contacts, with escalation order, used to coordinate response during a cyber or privacy event.

Circle of Care

Not a defined term under PHIPA. It is an informal term used to describe HICs and their authorized agents who are permitted to rely on a patient's implied consent when collecting, using, disclosing, or handling PHI for the purposes of provision of or assisting in the provision of health care.

Cloud Service

A technology service delivered over the internet that stores, processes, or transmits data, including email platforms, file–sharing tools, and hosted electronic medical records.

Confidentiality Agreement

A written agreement requiring staff or third parties to protect PHI and comply with applicable privacy and security obligations.

Credential Theft

The unauthorized acquisition of usernames, passwords, or authentication credentials often through phishing, malware, or password reuse.

Cyber Incident

Any event that compromises, or has the potential to compromise, the confidentiality, integrity, or availability of information systems or data.

Data Exfiltration

The unauthorized copying or transfer of data from a system to an external location, often without detection.

Double Extortion

A ransomware tactic in which attackers both encrypt systems and steal data, threatening to publish PHI and/or other sensitive data if the ransom is not paid.

Endpoint

Any device that connects to the clinic's network and processes information, including desktops, laptops, tablets, and servers.

Endpoint Detection and Response (EDR)

Security software that monitors endpoints for suspicious activity and supports detection, investigation, and response to cyber threats.

Encryption

A security technique that converts data into an unreadable format unless accessed with an authorized cryptographic key, protecting data at rest and in transit.

Express Consent

Explicit permission given by an individual, verbally or in writing, to collect, use, or disclose PHI for a specific purpose.

Guest Network (Guest Wi–Fi)

A segregated network that provides internet access to visitors while preventing access to internal clinic systems and devices.

Health Information Custodian (HIC)

A person or organization defined under PHIPA that has custody or control of PHI and is responsible for compliance with the Act.

Identifying Information

Includes information that identifies an individual or information that can reasonably foreseeably be used, either alone or with other information, to identify an individual. The definition of PHI also includes other identifying information that is contained in a record that contains personal health information.

Immutable (Immutable Backup / Immutable Storage)

A characteristic of data or backups that prevents them from being altered, deleted, or overwritten for a defined retention period, even by administrators or ransomware. Immutable storage provides protection against data tampering and encryption attacks by ensuring backup integrity.

Incident Response (IR)

The structured process used to identify, contain, remediate, and recover from cyber or privacy events affecting systems or information.

Incident Response Binder

A physical and/or digital collection of documents used to support response to cyber or privacy events, such as contact lists, contracts, checklists, and response guidance.

Information and Privacy Commissioner of Ontario (IPC)

Ontario's independent oversight body responsible for administering and enforcing Ontario privacy laws, including the PHIPA. The IPC provides guidance for HICs, investigates privacy complaints, and receives certain mandatory privacy breach reports.

Information Practices

Statements that describe how a Health Information Custodian is accountable to the public and inform individuals how PHI is protected, the purposes and conditions under which information may be shared, how PHI can be accessed or corrected, and how a complaint can be made. Information Practices should be posted as public notice.

Least Privilege

The principle that users are granted only the minimum system access required to perform their job duties.

Managed Service Provider (MSP)

A third–party organization that manages information technology services such as networks, backups, patching, and security tools on behalf of a clinic.

Malicious Software (Malware)

Software designed to harm systems, steal information, disrupt operations, or allow unauthorized access. Common examples include ransomware, spyware, and viruses.

Multi–Factor Authentication (MFA)

An authentication method that requires two or more verification factors, such as a password and a one–time code, to confirm a user's identity.

Offline Backup

A backup copy that is physically or logically disconnected from live systems, reducing the risk of encryption or deletion during an attack.

Patching

The process of applying updates or fixes to software, devices, or systems to correct known problems, improve performance, or address security vulnerabilities.

Personal Health Information (PHI)

Any identifying information about a patient in oral or recorded form, if the information:

- relates to the physical or mental health of the patient, including medical history and the patient's family medical history;
- relates to the provision of health care to the patient, including identification of a person as a provider of health care to the patient;

- relates to payment or eligibility for health care;
- is the patient's health card number; or
- identifies a substitute decision maker.

Phishing

A social–engineering attack that uses deceptive messages to trick individuals into revealing credentials, opening malicious files, or clicking harmful links.

Privacy Lead

The individual responsible for coordinating privacy governance, training, and compliance activities within the clinic.

Role–Based Access

A way of limiting access based on what a person needs to do their job, so staff can only see or use the information and systems necessary for their role.

Role–Based Access Control (RBAC)

A technical access control that enforces role-based access by assigning permissions based on job roles rather than to individuals directly.

Ransomware

A type of malicious software that encrypts systems or data and demands payment to restore access.

Safeguards and Controls – Examples

Administrative:

- Policies and procedures.
- Management oversight.
- Confidentiality agreements.
- Contracts, including Memorandums of Understanding and Letters of Understanding.
- Non–Disclosure Agreements.
- Education and awareness activities.
- Reminders that PHI must not be discussed in public areas.

Technical:

- Role–based access controls.
- Change management processes.
- Network firewalls and intrusion detection.
- Audit logging.
- Strong password requirements.
- Multi–factor authentication.
- Anti–malware software.
- Encryption.

Physical:

- Locked filing cabinets and offices.
- Secure records destruction.
- Physical security personnel.
- Access controls and surveillance.

Threat Actor

An individual or group that intentionally attempts to exploit systems, users, or data for malicious purposes.

Unique User Account

An individual login assigned to a specific person, enabling accountability and accurate audit logging.

References

The following resources provide the foundational frameworks, legal requirements, and best practices upon which this reference document is built.

Ontario Privacy Legislation and Guidance

Information and Privacy Commissioner of Ontario (IPC): *Health privacy breaches and related resources*. Provides definitions of breaches, reporting requirements, and links to official forms.

IPC Ontario: *Report a health privacy breach*. Detailed guidance on the seven reportable breach categories and the mandatory online reporting form.

IPC Ontario: *Privacy Breach Protocol: Responding to a Privacy Breach*. Recommended steps for health custodians to contain, evaluate, and prevent recurrence.

IPC Ontario: *A Privacy Management Handbook for Small Health Care Organizations (May 2025)*. Practical tips for operationalizing privacy programs.

IPC Ontario: *Privacy and Access in Public Sector Contracting with Third Party Service Providers (June 2024)*. Best practices for ensuring accountability with vendors.

IPC Ontario: *Ensuring secure disposal of health records: Out of sight is not out of mind! (May 2025)*. Standards for the physical destruction of PHI.

IPC Ontario: *Privacy Breaches: Guidelines for Public Sector Organizations (July 2025)*. General reporting and investigation frameworks.

Canadian and Provincial Cyber Security Standards

Ontario Health Cyber Security Centre. *Cyber security guidance for Ontario healthcare organizations.* Information on provincial toolkits and incident support for Community Clinics.

Ontario Health Cyber Security Centre: *Cyber Security Centre and Provincial Cyber Security Operating Model*. Outlines how Ontario coordinates cybersecurity governance, roles, and incident response.

Canadian Centre for Cyber Security (CCCS): *Report a Cyber Incident*. Incident reporting and management platform for Canadians.

CCCS: *Baseline Cyber Security Controls for Small and Medium Organizations*. Foundational technical requirements for Canadian businesses.

CCCS: *Ransomware Playbook (ITSM.00.099)*. Comprehensive planning for the prevention and recovery of ransomware attacks.

International Frameworks

National Institute of Standards and Technology (NIST): *NIST Cybersecurity Framework (CSF) 2.0*. Global standard for Identify, Protect, Detect, Respond, and Recover functions.

NIST: SP 800–61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management. Detailed process for structured incident analysis and containment.

NIST: *SP 800–40 Rev.4, Guide to Enterprise Patch Management Planning*. Standards for preventive maintenance and vulnerability mitigation.

NIST: *SP 800–63B–4, Digital Identity Guidelines*. Guidance on multi–factor authentication (MFA) and secure credential management.

International Organization for Standardization (ISO): *ISO/IEC 27001:2022 Information Security Management Systems*. Global standard for information security governance and controls.

Other References

OpenAI (2026): *AI–generated images created using ChatGPT (DALL·E).* https://openai.com

Cybersecurity Action Item Checklist:

- ☐ Create an asset inventory.
- ☐ Enable MFA for all accounts.
- ☐ Install Endpoint protection (Anti–virus) on all assets where applicable.
- ☐ Enable automatic patching for all software or hardware.
- ☐ Enable encryption of laptops and mobile devices.
- ☐ Force encryption for USB keys.
- ☐ Confirm backups occur daily.
- ☐ Confirm offline backups are available at least once a week.
- ☐ Make sure users don't have elevated privileges (admin rights).
- ☐ Configure a password policy of 15+ characters.
- ☐ Separate guest network from EMR network.
- ☐ Segregate IoT devices from EMR network.
- ☐ Configure Wi–Fi with WPA2 or WPA3 encryption.
- ☐ Change default username and/or password on all devices.
- ☐ Verify all service providers are ISO 27001 and/or SOC 2 or 3 compliant.
- ☐ Provide staff with Awareness training.
- ☐ Create an Incident Response plan.
- ☐ Create a Privacy Breach process.