



Managing PHIPA Breaches

Essential Steps for Healthcare Providers
Long Term Care IT Compliance Series- Part 2

BROCKIT

Quick Recap – What is PHIPA?

Protects personal health information (PHI).

Requires Breach Notifications.

Delineates Responsibilities.

Applies to LTC Homes.

- PHIPA: Personal Health Information Protection Act, 2004.
- Governs how personal health information (PHI) must be collected, used, disclosed, and protected.
- Explains responsibilities
- Applies to Health Information Custodians (HICs) like LTC homes.

Reference:

"Every health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure."

– **PHIPA Section 12(1)**



Key Test:

If the information **identifies** an individual **and** relates to their health or healthcare services — it is PHI under PHIPA.

Definition under PHIPA, Section 4(1):

“Personal health information” means identifying information about an individual in oral or recorded form if the information:

- Relates to the physical or mental health of the individual (including family health history)
- Relates to the provision of health care to the individual
- Relates to payments or eligibility for health care
- Relates to organ or tissue donation by the individual
- Relates to the individual’s health number (OHIP number)
- Identifies an individual’s substitute decision-maker

Specifically, it includes:

- Name, address, telephone number (if tied to health records)
- Health card number
- Medical history (diagnoses, treatments, prescriptions)

- Test results (lab, imaging, etc.)
- Mental health information
- Billing information related to health services
- Records of health service provision (who saw the patient, what services were provided)
- Any correspondence containing personal health information (e.g., appointment letters, referrals)

Why Focus on Breaches?



PHIPA REQUIRES
IMMEDIATE AND SPECIFIC
ACTION.



BREACHES = HUGE
FINANCIAL, LEGAL, AND
REPUTATIONAL RISK.



SPEED AND ACCURACY
REDUCE LIABILITY.

- Breaches are not just an IT problem; they are a *legal emergency* under PHIPA.
- Breaches must be responded to immediately to mitigate harm and fulfill legal obligations.
- Delay or improper response increases liability.

Reference:

"A health information custodian shall notify the individual at the first reasonable opportunity if personal health information about the individual is stolen, lost or accessed by unauthorized persons."

– **PHIPA Section 12(2)**

What is a Breach Under PHIPA?



Unauthorized collection, use, or disclosure of PHI



Access without a legitimate need ("snooping")



Lost/stolen devices containing PHI



Ransomware attack affecting PHI availability or confidentiality



Intent doesn't matter!

PHIPA Section 2 Definitions: 'Use' and 'Disclosure'.

Unauthorized collection, use, or disclosure of PHI

Access without a legitimate need ("snooping")

Lost/stolen devices containing PHI > Laptops, phones, tablets, etc.

Ransomware attack affecting PHI availability or confidentiality

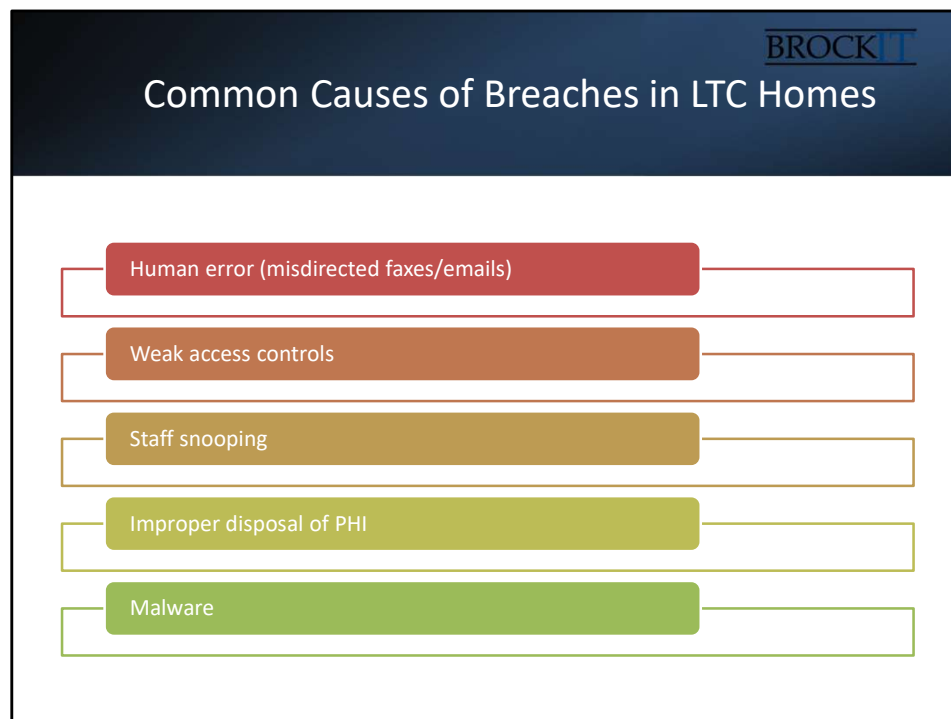
- Breach = Unauthorized collection, use, or disclosure of PHI.
- This includes snooping, ransomware attacks, and data loss events.

Reference:

"Use" means to view, handle or otherwise deal with the information, with or without modifying it.

"Disclosure" means to make the information available or to release it to another custodian or to another person.

– **PHIPA Section 2 – Definitions**



Unauthorized Access ("Snooping")

- A nurse accesses the health record of a resident who is a friend, family member, or celebrity without a legitimate work-related reason.
- IT system shows audit logs of multiple "curiosity accesses" without patient care involvement.

Breach: Unauthorized use of PHI (PHIPA Section 10, Section 12).

2. Lost or Stolen Devices

- A laptop containing unencrypted resident health records is stolen from a staff member's car.
- A USB stick with backup patient files is misplaced inside the LTC facility.

Breach: Loss of PHI. Even if loss is unintentional, notification obligations are triggered.

3. Misdirected Communication

- Staff faxes a resident's care plan to the wrong pharmacy.
- An email containing appointment dates and diagnoses is accidentally sent to the wrong family member.

Breach: Unauthorized disclosure of PHI.

Even if retrieved afterward, this still requires documentation and possibly notification.

4. Cyberattacks (Ransomware, Hacking)

- Malware encrypts an LTC home's server containing resident records. Attackers demand ransom to restore access.
- An external attacker compromises staff accounts and exfiltrates resident data.

Breach: Unauthorized access or use of PHI.

Must assess if PHI was accessed or stolen and report accordingly.

5. Unauthorized Disclosure to Unauthorized Individuals

- Staff member verbally discusses a resident's diagnosis in the cafeteria within earshot of other visitors.
- Printed discharge summary left unattended at a nursing station or common area.

Breach: Improper disclosure of PHI.

Even casual disclosures can breach PHIPA.

6. Improper Disposal of Records

- Shredding bins are improperly emptied, and paper charts are found intact in general garbage.
- Old computers with stored PHI are sold without proper data wiping.

Breach: Failure to safeguard PHI at end-of-life of records/devices.

7. Access by Contractors Without Privacy Training

- A third-party IT vendor accesses PHI during a server upgrade without having signed privacy agreements.
- Cleaning staff access paper records left on desks.

Breach: Agents acting on behalf of a custodian must be trained and bound by privacy obligations (PHIPA Section 17).

PHIPA Section 29(1) + LTC Act O. Reg. 79/10 s.229(4).

- Human error, weak IT controls, curiosity ("snooping"), and malware are the most common sources.
- "Curiosity breaches" are specifically outlawed.

Reference:

"No health information custodian shall collect, use or disclose personal health information about an individual unless the individual consents..."

– **PHIPA Section 29(1)**

Also:

Staff must only access information necessary for their duties (Principle of Least Privilege).

– **Long-Term Care Homes Act, 2007**, O. Reg. 79/10, s. 229 (4)



1. Contain the Breach

- **Stop unauthorized access** immediately.
- **Retrieve or secure** any exposed information (paper records, stolen devices, leaked emails).
- **Disable accounts** or system access if malicious activity is suspected.
Reference: PHIPA Section 12(1) – Reasonable steps to protect PHI.

2. Notify Appropriate Internal Authorities

- Alert the **Privacy Officer** or **designated breach response lead** immediately.
- Notify **senior leadership** (Administrator, Director of Care) depending on the severity.
Reference: PHIPA Section 15(1) – Requirement to designate Privacy Contact Person.

3. Preserve Evidence

- **Save audit logs**, emails, access logs, device tracking info.
- **Isolate compromised devices** but do **NOT** turn them off (to preserve forensic evidence).
- **Document everything** immediately: who discovered the breach, when, and how.
Reference: IPC Guidance on Security Incident Management.

4. Assess the Scope and Impact

- What information was involved? (Type, volume, sensitivity)
- Whose information was involved? (Residents, families, staff?)
- How long was it exposed?
- Who accessed it (internal staff vs. external party)?

Reference: IPC Breach Reporting Protocol – Step 1: Containment and Assessment.

5. Notify Affected Individuals (if required)

- Must notify at the **first reasonable opportunity**.
- Notification must include what happened, what information was involved, and advice to minimize harm.

Reference: PHIPA Section 12(2) – Mandatory notification.

6. Determine If IPC Notification is Required

Notify the **Information and Privacy Commissioner of Ontario (IPC)** if:

- Breach is part of a pattern.
- Staff disciplinary action occurs.
- Significant number of individuals affected.
- Significant sensitivity of information.

Reference: O. Reg. 329/04 Section 6.3.

7. Mitigate Future Risks

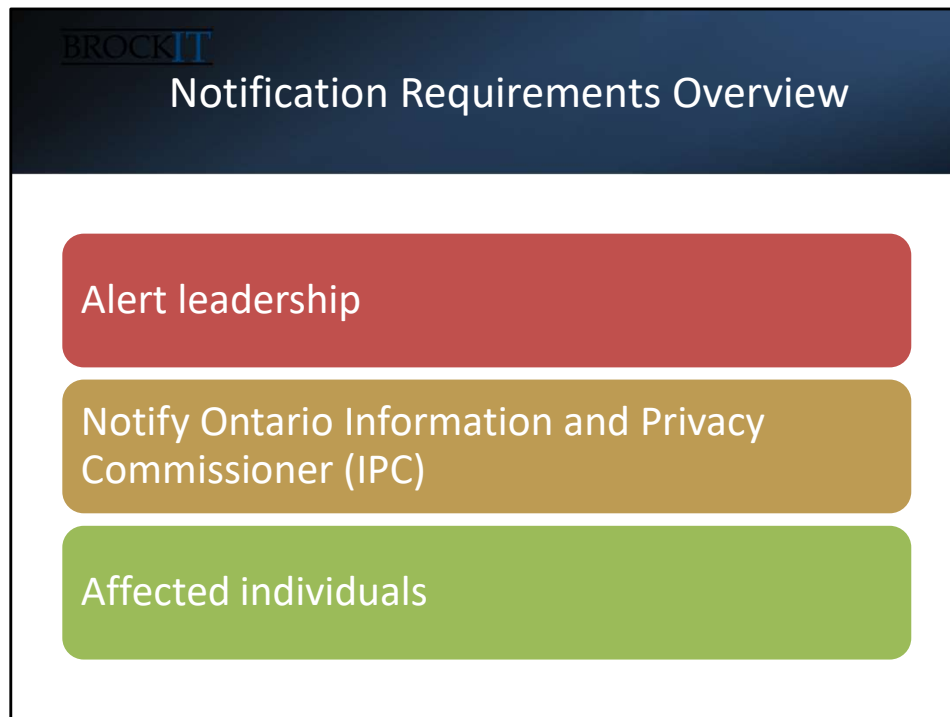
- Short-term: Force password resets, increase monitoring.
- Long-term: Update policies, add encryption, retrain staff as needed.

Reference: IPC Guidance – Preventative Measures after Breach.

Reference:

"A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information is protected..."

– **PHIPA Section 12(1)**



Affected Individuals

Mandatory for any theft, loss, or unauthorized use or disclosure of their PHI
Even minor breaches must notify individuals

Information and Privacy Commissioner (IPC)

Mandatory for **serious breaches** (see conditions next slide)
Must submit a formal Breach Report to IPC

Regulatory Colleges

Required if the breach involves **professional misconduct** by a regulated health professional (e.g., nurse, physician)
Must notify the applicable College (e.g., College of Nurses of Ontario)

Institutional Leadership

Always internally escalate to your Administrator, Privacy Officer, Director of Care
Organizational procedures determine method and urgency

Ontario Ministry of Health / Other Third Parties

Sometimes required (e.g., systemic breaches, public health emergencies)
Depends on nature of breach

PHIPA Section 12(2).

Organization leadership must always be alerted

Ontario's Information and Privacy Commissioner (IPC) must be notified in certain cases (slide to follow)

Affected individuals must be notified **at the first reasonable opportunity**

Reference:

"Notice to the individual must be given at the first reasonable opportunity."

– **PHIPA Section 12(2)**

It is important to remember that even if you do not need to notify the IPC, you have a separate duty to notify individuals whose privacy has been breached under subsection 12(2) or clause 55.5(7)(a) of PHIPA.²

Under subsection 12(3) and clause 55.5(7)(b) of the *Personal Health Information Protection Act* (PHIPA) and its related regulation, custodians must notify the Information and Privacy Commissioner of Ontario (IPC) at the first reasonable opportunity about certain privacy breaches.¹

<https://www.ipc.on.ca/en/health-organizations/report-a-privacy-breach>

When Must You Notify the IPC?

Part of a pattern

Disciplinary action taken

Large number of individuals affected

Breach is significant (sensitivity, volume or consequences)

Not every breach needs to be reported to the IPC — but serious ones do.

You must notify the IPC immediately if:

- The breach is part of a pattern of similar breaches.
- The custodian has disciplinary action against a staff member relating to the breach.
- The breach affects a significant number of individuals.
- The breach involves sensitive health information (e.g., mental health, HIV status).
- Any other situation where the custodian would reasonably believe that it is significant.

Reference:

O. Reg. 329/04 Section 6.3 — Reportable breach conditions.

"A custodian shall notify the Commissioner if the custodian has reasonable grounds to believe that the personal health information was used or disclosed without authority by a person who knew or ought to have known that they were doing so."

Review link here: <https://www.ipc.on.ca/en/health-organizations/report-a-privacy->

breach

How to Notify Individuals

Clear, simple language (Written by lawyer)

Include:

- What happened
- What information was involved
- Steps taken to address it
- Advice for them to protect themselves (e.g., monitoring, password changes)
- Contact info for follow-up

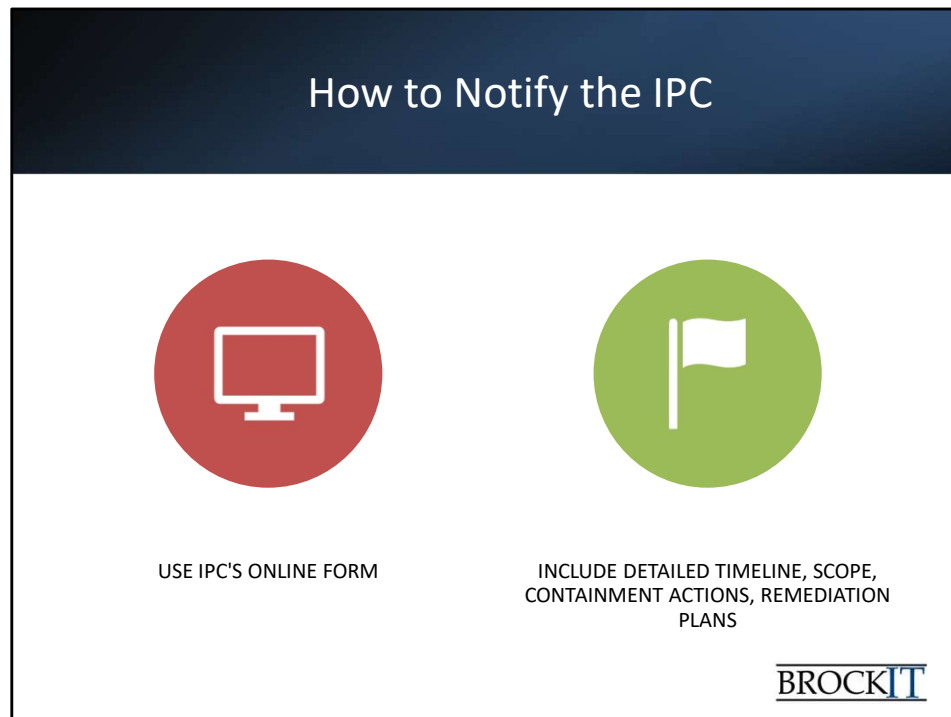
BROCKIT

- In **writing whenever possible**. (Letters, secure emails.)
- In exceptional cases (e.g., urgency, contact info missing), phone or verbal notice acceptable — but document verbal notification.
- Language must be **clear, compassionate, and accessible** (Grade 6–8 reading level recommended).
- Don't hide the facts; build trust by being upfront.
- LET YOUR LAWYER WRITE IT

Reference:

"The notice shall include sufficient information to permit the individual to understand the significance of the theft, loss or unauthorized use or disclosure."

– **PHIPA Section 12(2)**



- IPC provides a secure online Breach Report Form.
- Written notifications must include full details: nature, scope, containment, and corrective actions.
- Report must be comprehensive, factual, and explain corrective actions taken.

Reference:

IPC Breach Reporting Form and guidance:

<https://www.ipc.on.ca/privacy/health-privacy/health-privacy-breach-reporting/>

To Colleges:

- Usually formal written notice (letter or secure email) describing the facts and any professional discipline initiated.

Internal Leadership:

- Email and in-person briefings (depending on severity).

Legal and Documentation Requirements



DOCUMENT EVERY
BREACH



MAINTAIN BREACH LOG
(MANDATORY)



ANNUAL BREACH
REPORTING TO IPC
(MARCH 1ST)

O. Reg. 329/04 s.6.4.

A centralized record (digital or paper) that documents **every single breach**, no matter how small. Even if a breach seems minor and does not require IPC notification, you still must log it internally.

Every breach should have the following logged with it;

- Date of incident
- Description of incident
- Date discovered
- PHI Involved
- Notification steps taken
- Containment and prevention steps

How to maintain Breach log

Use a secure system: Sharepoint list, privacy breach tracking software, etc.

Keep logs confidential: Privacy officer, DOC, administrator or other key leadership only

Update logs immediately: Don't wait until investigation is over, log the event, update the log as new information becomes available.

Use consistent format: Standardise fields like dates, breach types, notifications,

actions, etc. This is where specific software is handy.

Cross-reference with reports: Ensure your individual breach reports (to IPC, Colleges, affected individuals) match the breach log entries

Annual reporting: <https://www.ipc.on.ca/sites/default/files/legacy/2017/11/annual-breach-statistics-rptg.pdf>

Section 6.4(1):

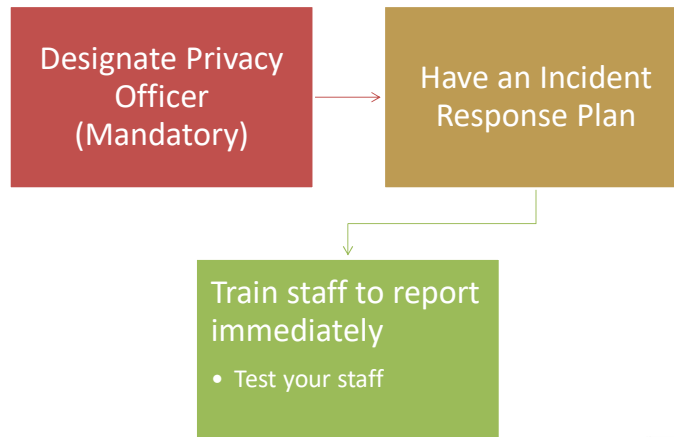
"A health information custodian shall make and maintain a record of every incident involving the theft, loss or unauthorized use or disclosure of personal health information in the custodian's custody or control."

Section 6.4(2):

"The record shall include the following information:

- (a) The date or estimated date of the theft, loss or unauthorized use or disclosure.
- (b) A description of the circumstances of the incident.
- (c) The date on which the incident was discovered.
- (d) A description of the personal health information involved.
- (e) The steps taken to notify the individual and the Information and Privacy Commissioner, if applicable.
- (f) The steps taken to contain the breach and to prevent future occurrences."

Tips for Managing a Breach Effectively



- Having a formal Incident Response Plan (IRP) is critical.
- **PHIPA requires designation of a Contact Person for privacy compliance.**
- Train your staff on privacy and security
- Test your staff
 - Create simulated events to test your staff's reaction such as creating a simulated patient file and leaving it in the printer for staff to find and report.

Reference:

"A health information custodian shall designate a contact person to be responsible for ensuring the custodian complies with this Act."

– **PHIPA Section 15(1)**



- Audit user activity (logs) immediately
- Backup verification (ensure clean backups)
- Device encryption (prevents reportable breach if device is lost!)
- Review access control and authentication settings

Reference:

"Custodians must implement practices and procedures to protect personal health information against unauthorized access."

– O. Reg. 329/04, Section 10(1)

1. Audit User Activity Immediately

Goal: Identify if and how personal health information (PHI) was accessed improperly.

Actions:

• **Review system audit logs** for unusual access patterns:

- Access outside normal hours.
- Large volumes of record accesses (e.g., mass opening of charts).
- Access to records without legitimate clinical need (e.g., wrong floor, wrong patient).

• **Pull email server logs** if the breach involved misdirected messages or phishing.

- **Use application audit features** if using Electronic Medical Record (EMR) systems (e.g., PointClickCare, Med e-Care).

Why It Matters:

Helps confirm whether PHI was actually accessed or just exposed, which affects reporting obligations to individuals and the IPC.

Reference: O. Reg. 329/04 Section 10(1) – Reasonable measures to protect PHI.

2. Backup Verification (Ensure Clean Backups Exist)

Goal: Protect organizational ability to recover PHI and operations in the event of ransomware or data loss.

Actions:

- **Immediately verify the integrity of your most recent backups.**
- **Check backup encryption** status and whether backups are isolated from production systems.
- **Test restore a sample backup** (not just confirming backup completion — actually restoring a file/database) to confirm it is usable.
- **Review backup logs** for any suspicious activity (e.g., tampering, failed backup jobs).

Why It Matters:

A working, recent backup can prevent PHI data loss and reduce the severity of a breach incident dramatically.

Reference: HIPAA obligations to protect and recover PHI if compromised (Section 12(1)).

3. Device Encryption Status Review

Goal: Determine if loss or theft of a device constitutes a *reportable* breach.

Actions:

- **Check encryption settings** on any lost/stolen device (laptops, USB drives, mobile devices):
 - For Windows: Verify BitLocker encryption enabled.
 - For Mac: Verify FileVault enabled.
 - For mobile: Verify full device encryption settings active (MDM enforced if possible).
- **Document encryption status** formally (screenshots, system logs).
- **If the device was encrypted** and no passwords were compromised, **PHIPA considers this a low-risk incident** — notification to individuals may not be necessary.

Why It Matters:

Encryption can exempt an organization from mandatory breach reporting under IPC guidance because the PHI would be protected from unauthorized access.

Reference: IPC Ransomware and Device Theft Guidance.

4. Review Access Control and Authentication Settings

Goal: Strengthen the security of systems post-breach and reduce likelihood of future breaches.

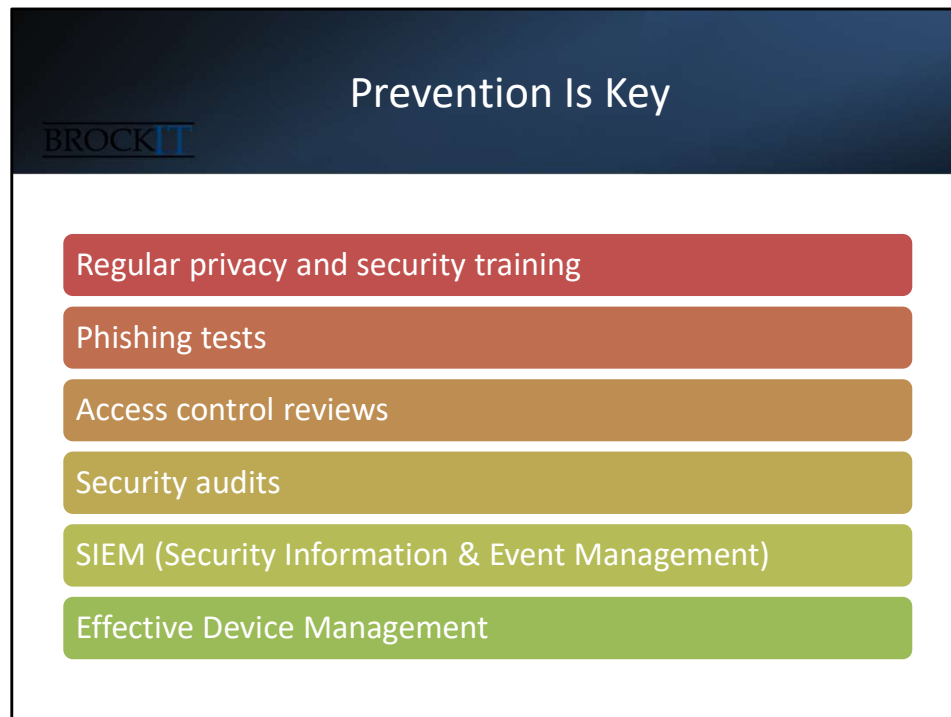
Actions:

- **Force immediate password resets** for affected or suspicious accounts.
- **Enable Multi-Factor Authentication (MFA)** for systems handling PHI if not already active.
- **Review permissions and group memberships** in Active Directory or EMR systems:
 - Ensure "least privilege" principle (users only have the access necessary for their roles).
 - Remove any **orphaned accounts** (former employees, temporary contractors).
- **Lock down open shares** or folders containing PHI (e.g., network folders accessible to too many users).

Why It Matters:

Many breaches escalate because access controls were too loose. Locking down access reduces the attack surface and protects against further unauthorized use.

Reference: O. Reg. 329/04 Section 10(1) – Custodians must implement secure practices and procedures.



- Prevention reduces breach risks drastically.
- Training, technical controls, and governance are your best defense.
- Follow industry standards (CIS Controls)

Reference:

"Health information custodians must ensure agents are appropriately trained on information practices and policies."

– **PHIPA Section 17(2)**

1. Regular Privacy and Security Training


✓ **Goal:** Ensure all staff understand their obligations under PHIPA and recognize threats that could lead to breaches.

Actions:


- Conduct **mandatory annual privacy training** covering PHIPA obligations, breach reporting, and safe handling of PHI.
- Provide **cybersecurity training** on topics like password management, recognizing phishing, secure device use, and protecting resident data.
- Offer **role-specific training** for high-risk staff (e.g., nursing staff, admissions clerks, IT

admins).

[Your Company Name] offers tailored **Privacy and Cybersecurity Training** programs designed specifically for healthcare and long-term care facilities, ensuring staff stay compliant and vigilant.

 *Reference:* PHIPA Section 17(2) – Agents must be appropriately trained.

2. Phishing Tests (Simulated Phishing Campaigns)

 **Goal:** Identify and remediate staff susceptibility to phishing attacks before a real-world incident occurs.


Actions:

- Regularly send **simulated phishing emails** to staff to test their awareness.
- Track who clicks, who reports suspicious emails, and who ignores them.
- Use results to **target additional training** to vulnerable users.
- Gamify results (e.g., award certificates for strong performers) to foster a positive security culture.

Brock IT provides **managed phishing testing services** — customized campaigns, staff performance reporting, and remediation training — helping reduce your organization's real-world risk of phishing-related breaches.

 *Reference:* IPC Breach Prevention Guidance – Cybersecurity Best Practices.

3. Access Control Reviews


 **Goal:** Ensure staff access only the information necessary for their role ("Principle of Least Privilege").

Actions:


- Regularly **audit Active Directory groups**, EMR user permissions, and folder access rights.
- Remove access immediately for terminated staff, contractors, and inactive accounts.
- Conduct **quarterly or bi-annual reviews** of access levels for all users.
- Limit administrative privileges strictly to those who require it.

Best Practice:

Tie access reviews to staffing events like promotions, department changes, and terminations to maintain control dynamically.

 *Reference:* O. Reg. 329/04 Section 10(1) – Reasonable safeguards for access control.

4. Security Audits

 **Goal:** Identify vulnerabilities in systems, networks, and physical security before they are exploited.

Actions:

- Conduct **annual security risk assessments** of IT systems and devices handling PHI.
- Perform **penetration testing** (internal and external) if feasible.
- Review firewall configurations, VPN security, wireless network protections, and email security settings.
- Audit physical security (locked storage areas, device theft protections).

•**Security Information and Event Management (SIEM) products** collect, correlate, and analyze log data from multiple sources (servers, endpoints, firewalls, cloud services).

•**SIEM benefits for healthcare organizations:**


- Detect suspicious activity early (e.g., unauthorized access to resident PHI).
- Correlate user actions with device activities.
- Identify patterns of breaches across systems before they escalate.
- Provide **critical evidence for breach investigations** and **audit reporting**.

•Examples of SIEM platforms: **Huntress SIEM, Microsoft Sentinel, Arctic Wolf**, etc.


Best Practice:

Integrate SIEM with Electronic Medical Records (EMRs), Active Directory, and endpoint management tools to monitor PHI access events in real time.

Involve external assessors periodically to ensure impartial evaluations.

 *Reference:* IPC Health Sector Guidance – Risk Assessments and Security Reviews.

5. Effective Device Management


 **Goal:** Protect endpoint devices (laptops, phones, tablets) from loss, theft, and compromise.

Actions:

- Require **full-disk encryption** on all portable devices (BitLocker, FileVault).
- Use **Mobile Device Management (MDM)** solutions to enforce security policies remotely (e.g., wipe data if a device is lost).
- Maintain an **accurate asset inventory** of all devices storing or accessing PHI.
- Enable **automatic security patching** to minimize vulnerabilities.

Best Practice:

Set up **geo-fencing** and **remote wipe capabilities** for devices used outside facility networks.

 *Reference:* PHIPA Section 12(1) – Reasonable measures to protect PHI.

Final Thoughts & Q&A

- Quick action + Clear process = Better outcomes
- Protect your residents and your organization.
- Open for Questions

Contact

William Thomson
613 499 9960 Ext 115
William@Brock-IT.ca



Open for questions!