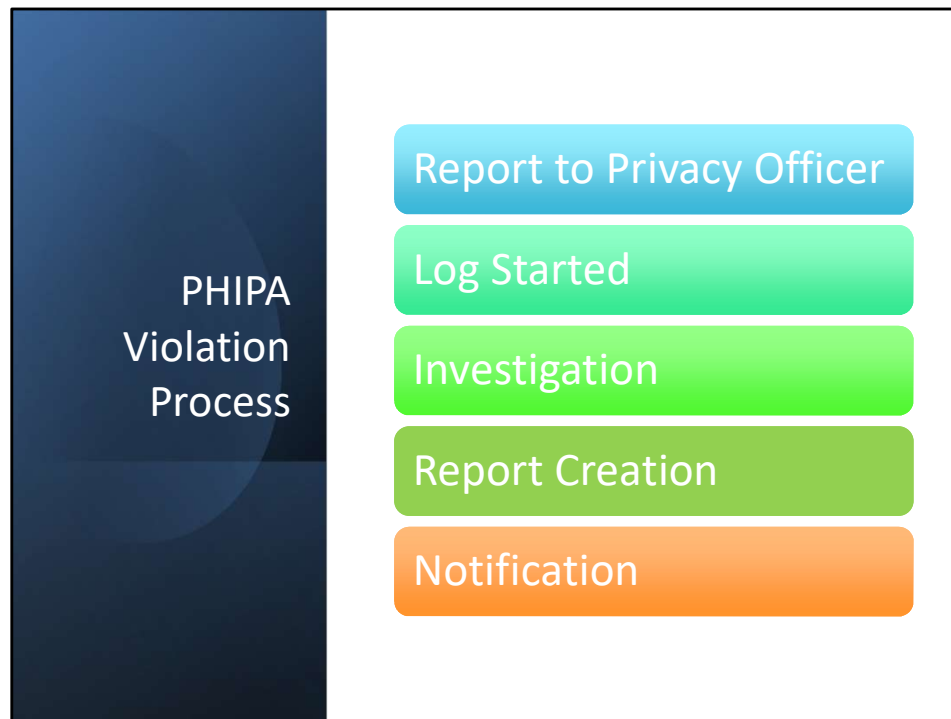




PHIPA Breach Tabletop
Exercise

Training Scenarios for
Long-Term Care Staff



1. Report to Privacy Officer
 1. Staff should report the discovered potential breach to the privacy officer whether they believe it's a breach or not
2. Log Started
 1. The breach should be recorded in the official breach log and updated as the investigation progresses
3. Investigation
 1. Who – Who accessed the file and for which patient
 2. What – What data was accessed. Example, Medication lists? Diagnosis? Doctors visits? Etc.
 3. When – When was it accessed and how many times?
 4. Where – Where was it accessed from?
 5. How – How did they access it? If this patient is not assigned to this staff member then how did they get access to the data?
 6. Why – Why did this staff member access the file? What reason did they give?
4. Report Creation
 1. Reports must be created.
 1. For internal use: Identify what went wrong, how to prevent it going forward and what discipline must be implemented

2. For External use: This is provided to the IPC or 3rd parties

1. Notification

1. Notification to 3rd parties should be written by legal following the guidelines;
 - 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.

Scenario 1: Curiosity Access by Staff Member

Summary:

- A Nurse accesses the chart of a former resident who was a local celebrity. The Nurse had no care duties related to the resident.

PHI Involved:

- Mental health notes.
- Medications.
- Diagnosis history.

Potential Consequences:

- Staff discipline.
- IPC and College notification.
- Family Notification
- Potential reputational damage.

Discussion:

- How would your organization detect this access?
 - Regular Audits
- What logs would you review?
 - EMR Access Logs
- What notifications are required under PHIPA?
 - Family, IPC, and College of nurses
 - Recommended you reach out to your lawyer to discuss how to notify the families
- How do you avoid 'curiosity access'?
 - Least Permissions
 - Acceptable use policies
 - Acceptable use training (Organization and regulatory body)

Scenario 2: Stolen Laptop from Employee Vehicle

Summary:

- A care coordinator's unencrypted laptop is stolen from their vehicle. It contained resident data including spreadsheets.

PHI Involved:

- Names,
- Health numbers,
- Medical histories,

Potential Consequences:

- Reportable breach.
- High-risk to resident data.
- Notification to IPC and individuals.
- Family trust implications.

Discussion Prompts:

- How do you verify encryption status?
 - With an asset management tool
- What is your stolen device protocol?
 - You need to have a device protocol that will outline what needs to happen when you are notified that a device has been lost or stolen.
- Who must be notified?
 - The police, the IPC, the governing body of the employee who's device was stolen may need to be notified, the parties or the families of the parties involved
 - Recommended that you notify legal counsel prior to notifying the anyone.
- Would this device meet asset management standards?
- Possible changes to process and requirements for devices that are transported offsite

Scenario 3: Improper Disposal of Paper Records

Summary:

- A box of historical resident charts is found in the outdoor recycling bin, awaiting public pickup.

PHI Involved:

- Historical medical notes .
- Family contacts.
- Health numbers.

Potential Consequences:

- Improper disposal.
- Possible IPC notification and the parties involved
- Breach of retention/destruction policy.

Discussion Prompts:

- What is your records disposal process?
 - Do you have a well-defined records disposal process.
- How are staff trained on secure disposal?
 - Staff need to be trained on how to handle and dispose of PHI on a regular basis
- Who audits shredding or recycling procedures?
 - This should be well defined and a part of your regular audits.

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!