Ontario Chiropractic Association

Privacy Breach Response Guide

Step 1: Immediate Internal Notification

- **Action:** Notify your clinic's **Chief Privacy Officer**, **clinic manager**, or designated privacy lead.
- **Why:** Early notification ensures a coordinated response and preserves evidence.
- **Include:** IT staff, legal counsel, and communications personnel if necessary.

Step 2: Contain the Breach

- **Action:** Take urgent steps to **stop the unauthorized access or disclosure**.
  - Shut down compromised systems
  - Revoke access credentials
  - Retrieve or secure any disclosed PHI
- **Why:** Containment limits further harm and exposure.

Step 3: Assess the Scope and Impact

- **Action:** Conduct a preliminary investigation to determine:
  - What PHI was involved
  - How many individuals were affected
  - Whether the breach was accidental, malicious, or systemic
- **Why:** This informs your legal obligations and next steps.

Step 4: Notify Affected Individuals

- **Action:** Notify patients as soon as reasonably possible if the breach poses a real risk of significant harm.
  - Use clear, plain language
  - Include what happened, what information was involved, and what steps are being taken
- **Why:** PHIPA *requires* notification to individuals when their PHI is compromised.

Step 5: Notify the IPC and Other Authorities

- **Action:** Report the breach to the **Information and Privacy Commissioner of Ontario (IPC)** if:
  - The breach was intentional or repeated
  - It involved a significant volume of PHI
  - It involved sensitive health information
  - It is part of a pattern or systemic issue
- **Also notify:** Regulatory colleges (e.g., CCO) if professional misconduct is suspected.
- **OCA can help**: Contact the OCA's Privacy Officer for support reporting the breach if desired

Step 6: Document Everything

- **Action:** Maintain detailed records of:
  - How the breach was discovered
  - Who was notified and when
  - What containment and remediation steps were taken
- **Why:** Documentation is essential for demonstrating compliance and defending against liability.

Step 7: Remediate and Prevent Future Breaches

- **Action:** Conduct a full investigation and implement corrective measures:
  - Update policies and procedures
  - Provide staff training
  - Strengthen technical safeguards (e.g., encryption, access controls)
- **Why:** PHIPA requires custodians to take reasonable steps to prevent future breaches.