Guidelines for Responding to a Privacy Breach

This section will:
- explain what constitutes a privacy breach
- identify whistle-blower protections in PIPA
- identify the four steps that physicians need to take following a suspected or confirmed breach
- explain the role of Information and Privacy Commissioner with regard to breaches

PIPA requires physicians to protect personal information that is under the practice's custody and control. Part of that responsibility involves managing privacy breaches, including taking steps to prevent them from occurring, developing a privacy breach response plan and promptly responding when a breach occurs. A privacy breach occurs when there is unauthorized collection, use, disclosure, retention, or disposal of personal information. Those activities are "unauthorized" if they occur in contravention of PIPA.

The following scenarios are common examples of how a privacy breach can occur:
- Personal information is stolen or misplaced.
- A patient's medical record or an electronic portable device containing personal health information (e.g., laptop, handheld electronic device, USB storage device) is lost or stolen.
- A letter containing a patient's diagnosis is inadvertently sent by mail, fax or electronically to an incorrect address or to the wrong person.
- A medical record is saved in a web folder that is publicly accessible online.
- A physician sells a computer previously used by the practice to a business without first deleting the personal information saved on the computer and securely wiping the hard drive.
- A physician uses their electronic access to look up the personal health information of a friend or relative who is not currently receiving treatment from that physician.

The fact that a privacy breach has occurred does not necessarily mean the practice has contravened PIPA, as certain types of privacy breaches may be unavoidable (e.g., ransomware or phishing scams carried out by sophisticated hackers). The requirement to have "reasonable" security measures does not impose a standard of perfection but requires a very high level or rigour given the sensitivity of personal health information. The practice should be objectively diligent and prudent in all circumstances and implement measures that include:
- strong, up-to-date, industry-standard encryption for electronic information
- unique passwords
- controls to restrict access
- secure data back-ups
- physical measures such as locked cabinets

For more information, see Step 7 – Employ Safeguards.

Suspected or real privacy breaches can come to a practice's attention through compliance monitoring mechanisms such as audit trails that flag unusual access, a complaint by an employee, patient, or member of the public, or through the OIPC as a result of a formal complaint.

Anyone who reports a privacy breach in good faith and on the basis of reasonable belief is protected under PIPA's whistle-blower provisions. These provisions protect an individual from being dismissed, suspended, demoted, disciplined, harassed or otherwise disadvantaged for having reported the breach, and the individual's identity may be kept confidential by the OIPC.

The OIPC has prepared guidance materials to assist in detecting, responding to, and preventing privacy breaches. The guidance materials include:
- Privacy Breach Checklist to evaluate the impact of a privacy breach and determine if notification is necessary.
- Online Privacy Breach Report Form if an organization decides to self-report a privacy breach to the OIPC.

For more information, see Privacy Breaches: Tools and Resources.

Once a privacy breach is identified, the practice must immediately respond to the breach by taking four key steps.

Step 1: Contain the Breach

Take immediate steps to contain the breach and mitigate the risk of harm by:

- contacting the designated privacy officer
- immediately containing the breach, which could involve stopping the unauthorized practice, suspending user accounts, revoking computer access codes, shutting down the system that was breached, recovering the records, or correcting weaknesses in physical security
- notifying law enforcement if the breach involves theft or criminal activity
- making sure evidence that could be used to investigate or correct the breach is not compromised

Step 2: Evaluate the Risks Associated with the Breach

As soon as possible after discovering a breach, determine the extent of the breach and potential harms that could occur as a result, by considering:

- What kinds of personal information were involved and how sensitive is that information?
- What format was the information in (paper, electronic) and how was it protected (encrypted, anonymized, password protected)?
- Was it lost, stolen or mistakenly disclosed?
- Could the personal information be misused, and if so, how?
- What was the cause of the breach?
- Was it an isolated event or is there a risk of ongoing or further exposure?
- Who and how many individuals were affected by the breach?
- What harm to the affected individual(s) could result from the breach?
- Is there a relationship between the unauthorized recipients and the data subject? (A close relationship between the victim and the recipient could increase the likelihood of harm).
- What harm could result to the practice as a result of the breach?
- Are there risks to the public (such as health and/or safety) as a result of the breach?
- Has the information been recovered?

Step 3: Implement Notification Procedures

Consider whether the following individuals or groups need to be notified:

- individuals (whether patients or staff) whose personal information was involved in the breach
- the OIPC
- law enforcement authorities
- professional regulatory bodies (such as the College of Physicians and Surgeons)
- mutual defence organizations (such as the Canadian Medical Protective Association)
- other groups based on legal, professional, or contractual obligations

In determining whether to notify consider:

- Do any legal obligations (contractual, legislated, etc.) require notification?
- How sensitive was the personal information?
- How many people were affected by the breach?
- Was the information was fully recovered without further disclosure?
- Could the personal information be used to commit fraud or identity theft?
- Is there is a reasonable risk of physical harm, psychological harm (including humiliation or damage to reputation), or financial harm (including loss of business or employment opportunities)?
- Is there is a risk of harm to the public or to patient relations?

Individuals who are affected by a privacy breach should be **notified immediately** if it is necessary to avoid or mitigate harms that they could experience as a result of the breach. The determination of whether or not to report the breach to the OIPC should generally be made within **two days** of the breach. While PIPA does not currently include

an explicit requirement for organizations to report breaches to the OIPC, doing so will assist the practice to demonstrate that it has taken reasonable steps to respond to the privacy breach and in the resolution of any complaint made to the OIPC.

The notification should include:

- the date and description of the privacy breach
- a description of the personal information that was involved in the privacy breach
- a description of potential risks of harm that could occur as a result of the breach
- steps taken to mitigate the harm
- steps planned to prevent privacy breaches in the future
- what affected individuals can do to further protect themselves and mitigate the risk of harm
- if appropriate in the circumstances, an offer for complimentary credit monitoring
- contact information for the practice's privacy officer who can answer questions
- a statement of the right to complain to, and whether or not the practice has notified, the College Of Physicians And Surgeons or the OIPC

Step 4: Prevent Future Privacy Breaches

Once immediate steps are taken to mitigate the risks, the practice, including the staff, should investigate the cause of the breach. Long-term safeguards should be developed to prevent further breaches. This may require updating privacy and security policies, performing a security audit of the practice's physical and technical safeguards, re-training employees on their privacy obligations, and undertaking a final audit to verify that the security arrangements have been implemented and function as planned. This process should generally take place **within two months** of the breach.