Mandatory Reporting Obligations, Best Practices and Tribunal Processes of the IPC

Brendan Gray, Health Law Counsel

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Cybersecurity in Health Care

November 18, 2020

DISCLAIMER

THIS PRESENTATION IS:

- PROVIDED FOR INFORMATIONAL PURPOSES,
- NOT LEGAL ADVICE, AND
- NOT BINDING ON THE IPC.

Topics

1. Intro to the IPC
2. *PHIPA* Breach Notification and Reporting
3. IPC's *PHIPA* Processes
4. Responding to a Privacy Breach

What is the IPC?

Information and Privacy Commissioner of Ontario (IPC or Commissioner)

- The IPC is an officer of the legislative assembly.
- Until very recently, the IPC only had authority under three acts:
  - *Freedom of Information and Protection of Privacy Act* (*FIPPA*)
  - *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)
  - *Personal Health Information Protection Act, 2004* (*PHIPA* or the *Act*)

Information and Privacy Commissioner of Ontario (cont')

- But now there are more with an oversight role for the IPC, such as:
  - *Child, Youth and Family Services Act, 2017*
  - *Anti-Racism Act, 2017*

PHIPA Breach Notification and Reporting

Breach Notification Summary

- A custodian must notify the individual at the first reasonable opportunity if personal health information (PHI) in its custody or control is stolen, lost or used or disclosed without authority

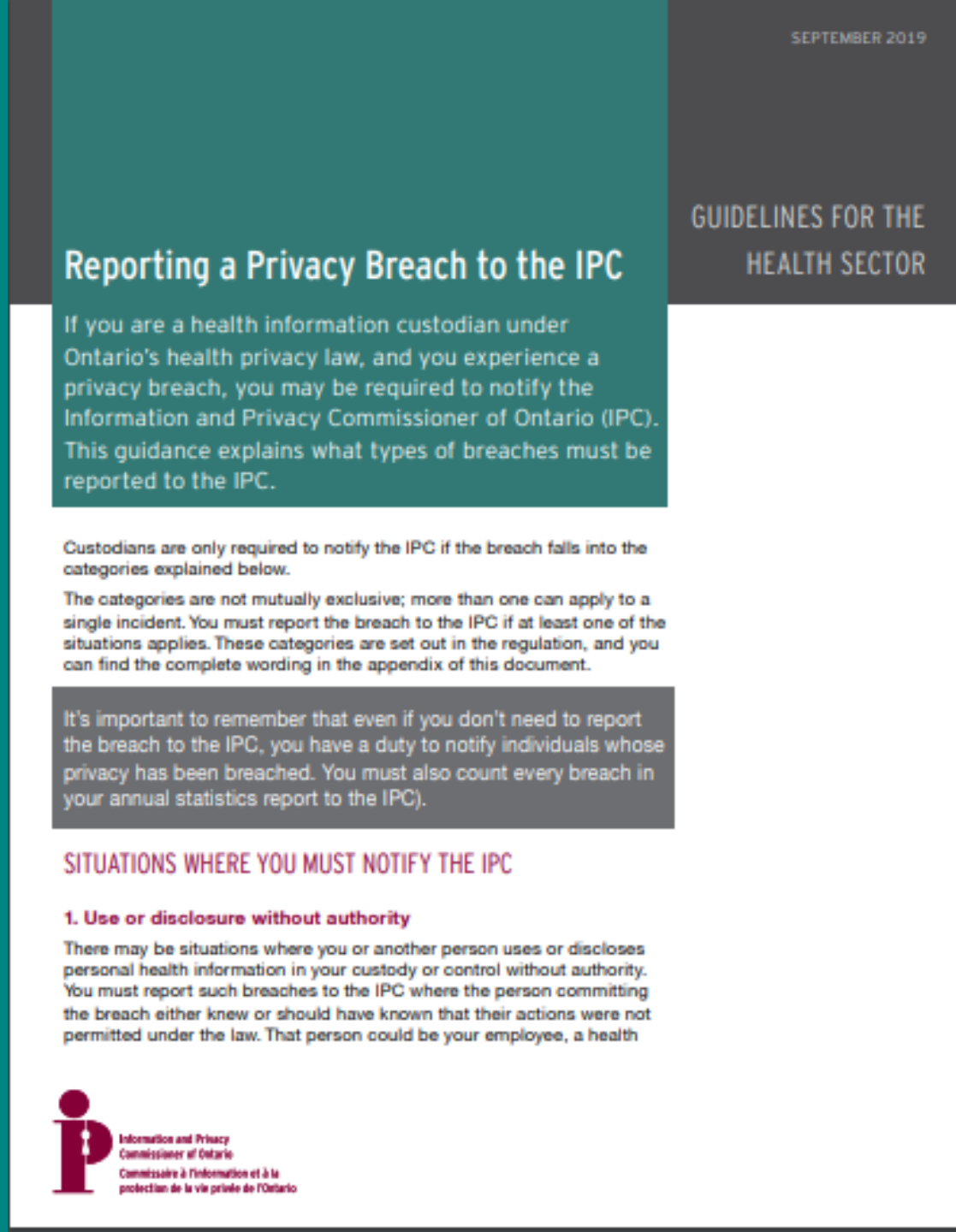
- In the context of the provincial electronic health record (EHR), a custodian must notify the individual at the first reasonable opportunity if it collects PHI without authority

- The Commissioner must also be notified if the circumstances surrounding the theft, loss or unauthorized collection*, use or disclosure meets certain prescribed requirements

*In the context of the EHR

Breach Notification to the Commissioner

- Regulations prescribing when the Commissioner must be notified of thefts, losses and unauthorized uses and disclosures came into force October 1, 2017
- The IPC published a guidance document explaining when a breach must be reported to the Commissioner
- Regulations prescribing when the Commissioner must be notified of unauthorized collections from the EHR came into force October 1, 2020



SEPTEMBER 2019

GUIDELINES FOR THE HEALTH SECTOR

Reporting a Privacy Breach to the IPC

If you are a health information custodian under Ontario's health privacy law, and you experience a privacy breach, you may be required to notify the Information and Privacy Commissioner of Ontario (IPC). This guidance explains what types of breaches must be reported to the IPC.

Custodians are only required to notify the IPC if the breach falls into the categories explained below.

The categories are not mutually exclusive; more than one can apply to a single incident. You must report the breach to the IPC if at least one of the situations applies. These categories are set out in the regulation, and you can find the complete wording in the appendix of this document.

It's important to remember that even if you don't need to report the breach to the IPC, you have a duty to notify individuals whose privacy has been breached. You must also count every breach in your annual statistics report to the IPC).

SITUATIONS WHERE YOU MUST NOTIFY THE IPC

1. Use or disclosure without authority

There may be situations where you or another person uses or discloses personal health information in your custody or control without authority. You must report such breaches to the IPC where the person committing the breach either knew or should have known that their actions were not permitted under the law. That person could be your employee, a health

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Notification to the Commissioner of Thefts, Losses and Unauthorized Uses and Disclosures

- A health information custodian must notify the Commissioner if:

1. The use or disclosure without authority was made by a person who knew or ought to have known their actions were not permitted
2. PHI is stolen
3. There is a further use or disclosure without authority after the breach
4. There is a pattern of similar breaches
5. Disciplinary action/restricted privileges is imposed on college member
6. Disciplinary action is imposed on a non-college member
7. The breach is significant having regard to factors such as the sensitivity and volume of PHI and the number of individuals and custodians affected

Notification to the IPC under Part V.1 of *PHIPA*

Part V.1 of *PHIPA* (and related regulations) are now in force (as of October 1, 2020). This Part applies to the provincial electronic health record. In that context, there are additional notification and reporting obligations for custodians

- The IPC must be notified of an unauthorized collection from the EHR in the same circumstances as if the collection were an unauthorized use of disclosure outside of the EHR
- The IPC must be notified of all consent overrides for the purpose of eliminating or reducing a signification risk of serious bodily harm to a person other than the individual to whom the information relates or a group of persons

Duty to Notify Individuals

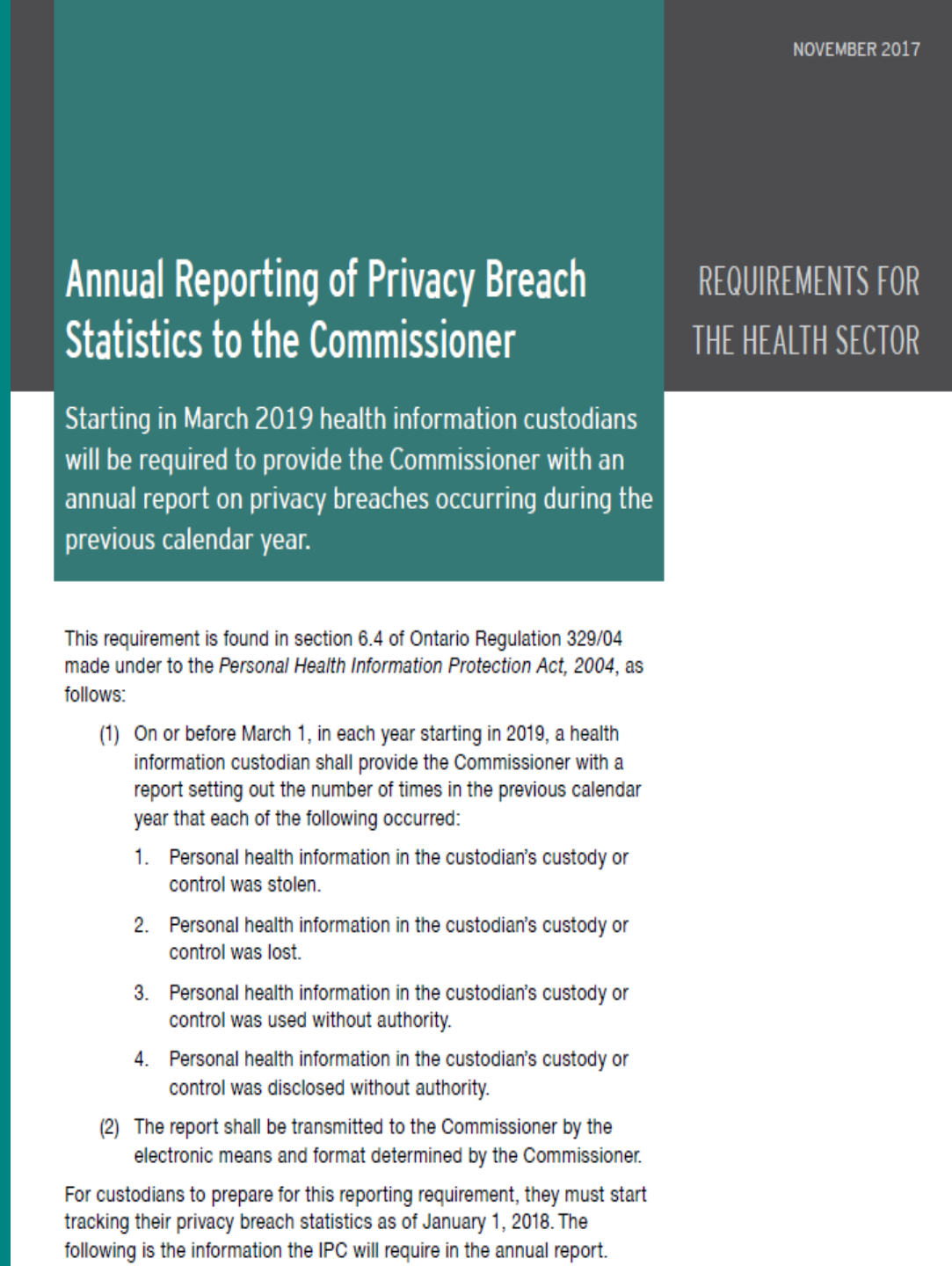
- It is important to remember that, even if you do not need to notify the IPC, you have a separate duty to notify individuals of breaches under sections 12(2) and 55.5(7)(a) of *PHIPA*

- Individuals must also be notified of all consent overrides (collections and uses contrary to a consent directive) in the EHR (section 55.7(7)(a))

Annual Reports to the Commissioner

- Health information custodians must provide the IPC with annual privacy breach statistics.
- They must track incidents where personal health information was:
    - stolen
    - lost
    - used without authority
    - disclosed without authority *
    - collected without authority (in the context of the provincial EHR)
- This annual report must also include breaches that do not meet the criteria for immediate mandatory reporting to the IPC.

* In the context of the provincial EHR, only the custodian collecting, and not the custodian disclosing, must include the breach.



NOVEMBER 2017

REQUIREMENTS FOR THE HEALTH SECTOR

Annual Reporting of Privacy Breach Statistics to the Commissioner

Starting in March 2019 health information custodians will be required to provide the Commissioner with an annual report on privacy breaches occurring during the previous calendar year.

This requirement is found in section 6.4 of Ontario Regulation 329/04 made under to the *Personal Health Information Protection Act, 2004*, as follows:

(1) On or before March 1, in each year starting in 2019, a health information custodian shall provide the Commissioner with a report setting out the number of times in the previous calendar year that each of the following occurred:

1. Personal health information in the custodian's custody or control was stolen.
2. Personal health information in the custodian's custody or control was lost.
3. Personal health information in the custodian's custody or control was used without authority.
4. Personal health information in the custodian's custody or control was disclosed without authority.

(2) The report shall be transmitted to the Commissioner by the electronic means and format determined by the Commissioner.

For custodians to prepare for this reporting requirement, they must start tracking their privacy breach statistics as of January 1, 2018. The following is the information the IPC will require in the annual report.

IPC's *PHIPA* Processes

PHIPA Processes

- Internal review of IPC's *PHIPA* processes led to changes
  - Most significant: an increase in the number of public decisions, to provide guidance and increase transparency
  - IPC issues "*PHIPA* Decisions" which include:
    - Orders
    - Decisions not to conduct a review
    - Decisions following a review, with no orders
    - Interim decisions

PHIPA Processes (Cont')

- Over 100 Decisions issued since August 2015
  - More staff involved in *PHIPA* Decisions
    - *PHIPA* Orders previously written primarily by Commissioner or Assistant Commissioner
    - IPC Adjudicators and Investigators to write more decisions (also analysts in some circumstances)

HEALTH

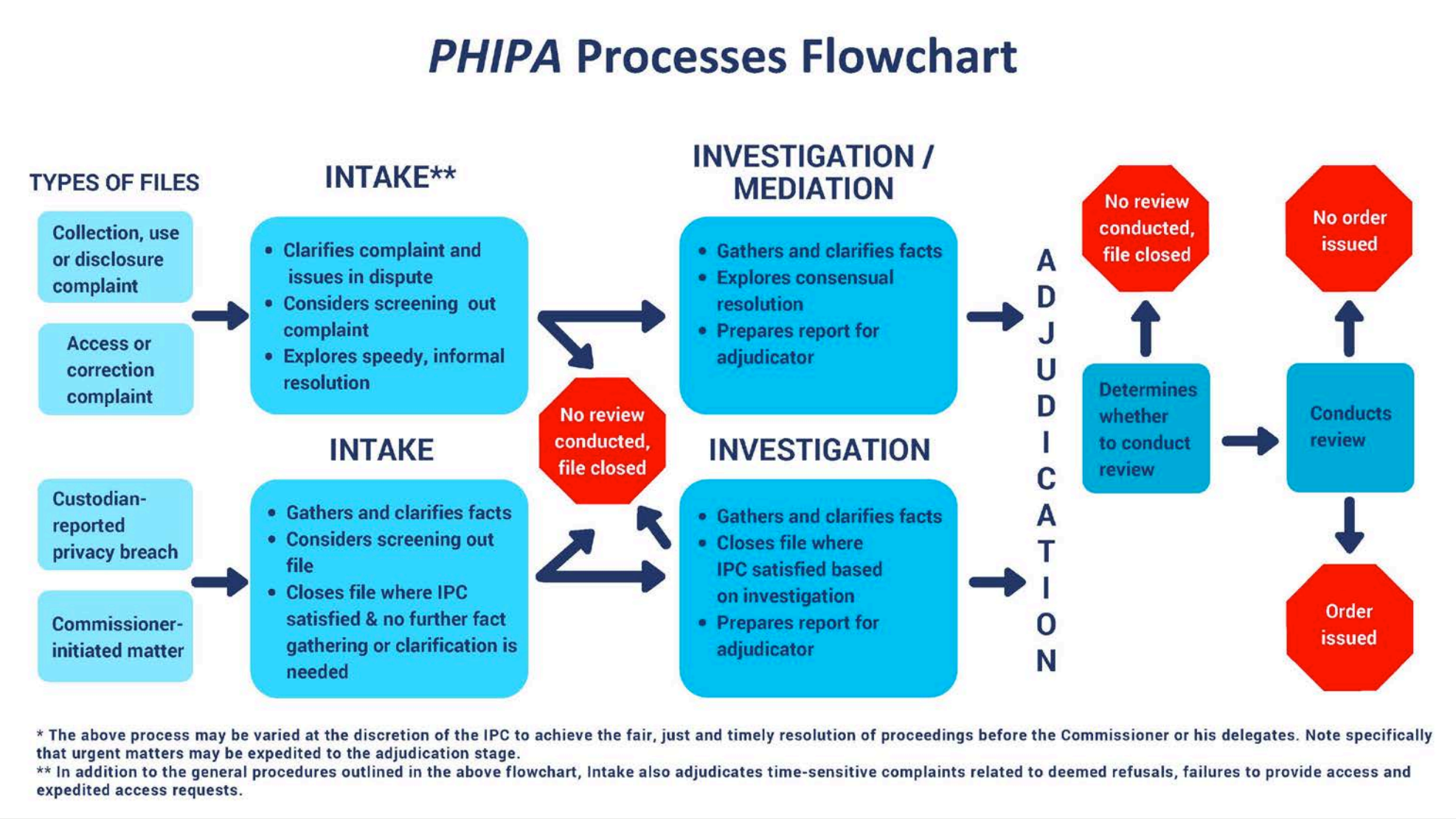
AUGUST 2019

Code of Procedure

for Matters under the *Personal Health Information Protection Act, 2004*

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Stages of *PHIPA* Files



Responding to a Privacy Breach

Responding to a Privacy Breach

Step 1: Immediately implement privacy breach protocol, including

- Notify all relevant staff of the breach
- Develop and execute a plan designed to contain the breach and notify those affected
- Report the matter to the IPC (if applicable)

Responding to a Privacy Breach

Step 2: Stop and contain the breach, including

- Identify the scope of the breach and take the necessary steps to contain it, including:
  - Retrieve and secure any personal health information that has been disclosed
  - Ensure that no copies of the personal health information have been made or retained by an individual who was not authorized to receive the information
  - Determine whether the privacy breach would allow unauthorized access to any other personal health information and take the necessary steps, such as changing passwords, identification numbers and/or temporarily shutting your system down

Responding to a Privacy Breach

Step 3: Notify those affected by the breach, including

- Notify those individuals whose privacy was breached at the first reasonable opportunity
- When notifying individuals affected by a breach:
    - Provide details of the breach, including the extent of the breach and what personal health information was involved
    - Advise of the steps you are taking to address the breach and that they are entitled to make a complaint to the IPC (and include the IPC's contact information). If you have reported the breach to the IPC, advise them of this fact
    - Provide contact information for someone within your organization who can provide additional information and assistance

Responding to a Privacy Breach

Step 4: Investigation and remediation, including

- Conduct an internal investigation, including:
  - Ensuring that the immediate requirements of containment and notification have been met
  - Reviewing the circumstances surrounding the breach
  - Reviewing the adequacy of your existing policies and procedures in protecting personal health information
  - Ensuring all staff are appropriately educated and trained

QUESTIONS?

CONTACT US

Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

TDD/TTY: 416-325-7539

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965