David Goodis

Assistant Commissioner
Office of the Information and Privacy Commissioner of Ontario

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

AMCTO MUNICIPAL ACCESS AND PRIVACY FORUM

October 12, 2017

Our Office

- Information and Privacy Commissioner (IPC) provides independent review of government decisions and practices on access and privacy
- Commissioner appointed by, reports to the Legislative Assembly, to ensure impartiality

IPC's Legislation

- *Freedom of Information and Protection of Privacy Act* (*FIPPA*)
  - over 300 provincial institutions such as ministries, provincial agencies, boards, commissions, community colleges and universities
- *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)
  - over 1,200 organizations such as municipalities, police, school boards, conservation authorities, transit commissions
- *Personal Health Information Protection Act* (*PHIPA*)
  - individuals and organizations involved in delivery of health care services, including hospitals, pharmacies, laboratories, doctors, dentists and nurses

IPC Breach Reporting

- no mandatory breach reporting to IPC under *FIPPA/MFIPPA*
- mandatory breach reporting to IPC for health information as of October 1, 2017
  - s. 12(3) of *PHIPA* and related regulations
- we receive reports under all three statutes
  - 102 public sector self-reported (2016)
  - 233 health sector self-reported (2016)
  - more learned from complainants, media

Responding to a Privacy Breach

1. Implement and identify

- implement privacy breach management policy
- determine if actual breach
- identify PI breached
- notify senior management and all other relevant staff
    - we recommend contacting IPC and providing details of the breach

Responding to a Privacy Breach

2. Contain

- containment measures to prevent further harm:
  - prevent further copies of records
  - ensure records retrieved/disposed of
  - determine whether breach would allow unauthorized access to other PI, and take necessary steps
    - e.g. change passwords, identification numbers, shut down the system

Responding to a Privacy Breach

3. Notify

- notice to individuals (PHIPA requires) at first opportunity
- form, timing of notice (direct or indirect?)
- notice should contain:
  - nature and extent of breach
  - nature and extent of PI (financial, recommend credit monitoring)
  - containment steps taken
  - any further actions organization will take
  - contact information for person within organization who can provide additional information or assistance
  - be transparent!

Cont'd

Responding to a Privacy Breach

4. Investigate and remediate

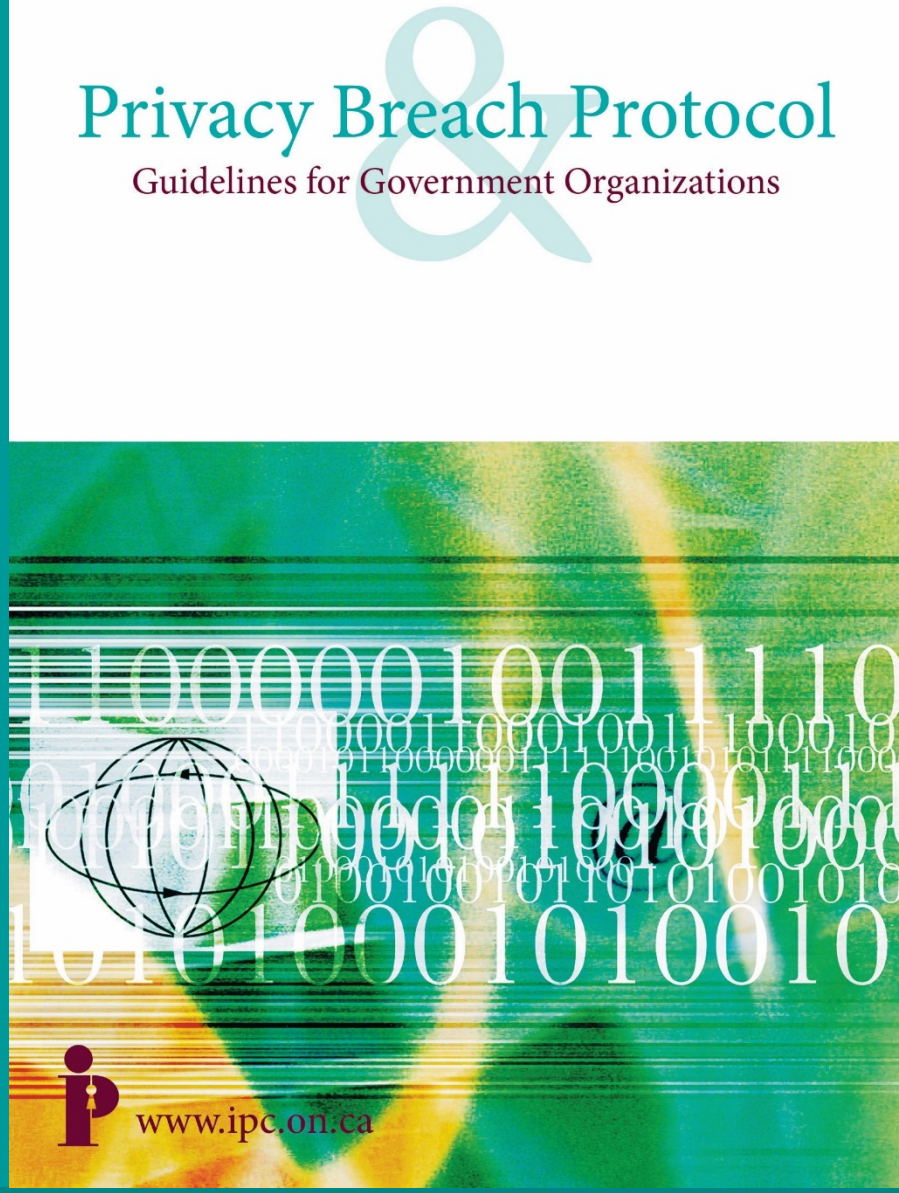
- conduct internal investigation to:
  - review containment measures taken
  - determine if breach effectively contained
  - ensure individuals notified
  - review adequacy of policies and procedures
  - recommendations to prevent future breaches
  - ensure staff properly trained
- document investigation, recommendations
- implement recommendations

What Happens when the IPC Investigates a Breach

- Depending on circumstances, IPC may:
  - ensure adequate containment, notification
  - interview appropriate individuals
  - obtain and review the organization's position on the breach
  - ask for status report of any actions taken by the organization
  - review and provide input and advice on current policies and procedures and any other relevant documents and recommend changes
  - issue a report or order at the conclusion of the review

Privacy Breach Protocol Guide

- implementing a privacy breach protocol, as a best practice, helps identify privacy risks, potential and actual breaches
- guidance on what organizations should do when faced with a breach



What to do When Faced with a Privacy Breach

- *PHIPA* sets out the rules that health information custodians must follow when collecting, using, disclosing, retaining and disposing of personal health information
- guidance to health information custodians when faced with a privacy breach

What to do When Faced With a Privacy Breach:

Guidelines for the Health Sector

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

Health Sector Privacy Breach Reporting

- health information custodians are required to report privacy breaches to the IPC in seven categories described in the regulations
- each category is discussed, examples provided

Reporting a Privacy Breach to the Commissioner

GUIDELINES FOR THE HEALTH SECTOR

To strengthen the privacy protection of personal health information, the Ontario government has amended the *Personal Health Information Protection Act* (the act). Under section 12(3) of the act and its related regulation, custodians must notify the Information and Privacy Commissioner of Ontario (the Commissioner) about certain privacy breaches. This law takes effect **October 1, 2017**.

As a custodian, you must report breaches to the Commissioner in seven categories described in the regulation and summarized below. The categories are not mutually exclusive; more than one can apply to a single privacy breach. If at least one of the situations applies, you must report it. The following is a summary—for the complete wording of the regulation, see the appendix at the end of this document.

It is important to remember that even if you do not need to notify the Commissioner, you have a separate duty to notify individuals whose privacy has been breached under section 12(2) of the act.

SITUATIONS WHERE YOU MUST NOTIFY THE COMMISSIONER OF A PRIVACY BREACH

1. Use or disclosure without authority

This category covers situations where the person committing the breach knew or ought to have known that their actions are not permitted either by the act or the responsible custodian. An example would be where a

HOW TO 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