# Regulators' Expectations for Responding to Privacy Breaches

**David Goodis**

**Assistant Commissioner**
**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

**Infonex**

**Legal Issues in Privacy: Cybersecurity**

**November 19, 2019**

# Who is the Information and Privacy Commissioner of Ontario?

- **Brian Beamish** appointed by Ontario Legislature (2015)
- 5 year term
- reports to Legislature, not government or minister
- ensures independence as government “watchdog”

# Privacy law in Ontario and Canada

| Federal public sector | Ontario public sector | Ontario health sector | Private sector |
|---|---|---|---|
| Government of Canada<br>federal ministries, agencies, crown corporations<br><br>*Privacy Act* | Government of Ontario<br>provincial ministries, agencies, hospitals, universities, cities, police, schools<br><br>*Freedom of Information and Protection of Privacy Act* (*FIPPA*)<br>*Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) | Health care individuals, organizations ("health information custodians") hospitals, pharmacies, labs, doctors, dentists, nurses<br><br>*Personal Health Information Protection Act* (*PHIPA*) | Private sector businesses<br><br>*Personal Information Protection and Electronic Documents Act* (*PIPEDA*) |
| OPC oversight | IPC/O oversight | IPC/O oversight | OPC oversight |

# Does law require us to notify Commissioner of a privacy breach?

- Ontario public (*FIPPA/MFIPPA*)
  - no but best practice to notify if significant breach
- Ontario health (*PHIPA*)
  - yes if significant breach as per regs [s. 12(3)]
- Private (*PIPEDA*)
  - yes if RROSH [s. 10.1(1)]
- Canada public (*Privacy Act*)
  - no but policy directive says yes if material breach

# Timing of reporting breach to Commissioner

- generally, Commissioners ask that organizations report a significant breach as soon as reasonably possible
- very late notice to Commissioner may put you in bad light with
  - Commissioners
  - subject individuals
  - courts?
- early notice will give you advantage of Commissioner's advice

# Content of breach report to Commissioner

- generally, Commissioners ask organization to report:
  - circumstances of the breach (how did info become lost, stolen, used without authority?)
  - did you report breach to individuals? If so, how?
  - what is the exact nature of the information, how many people?

# Does law require us to notify affected individuals of a privacy breach?

- Ontario public (*FIPPA/MFIPPA*)
  - no, but best practice if real risk of significant harm
    - ❖ RROSH based on number of individuals, sensitivity, potential for abuse
- Ontario health (*PHIPA*)
  - yes for all breaches [s. 12(2)]
- Private (*PIPEDA*)
  - yes if RROSH [s. 10.1(3)]
- Canada public (*Privacy Act*)
  - no but policy directive says yes if material breach

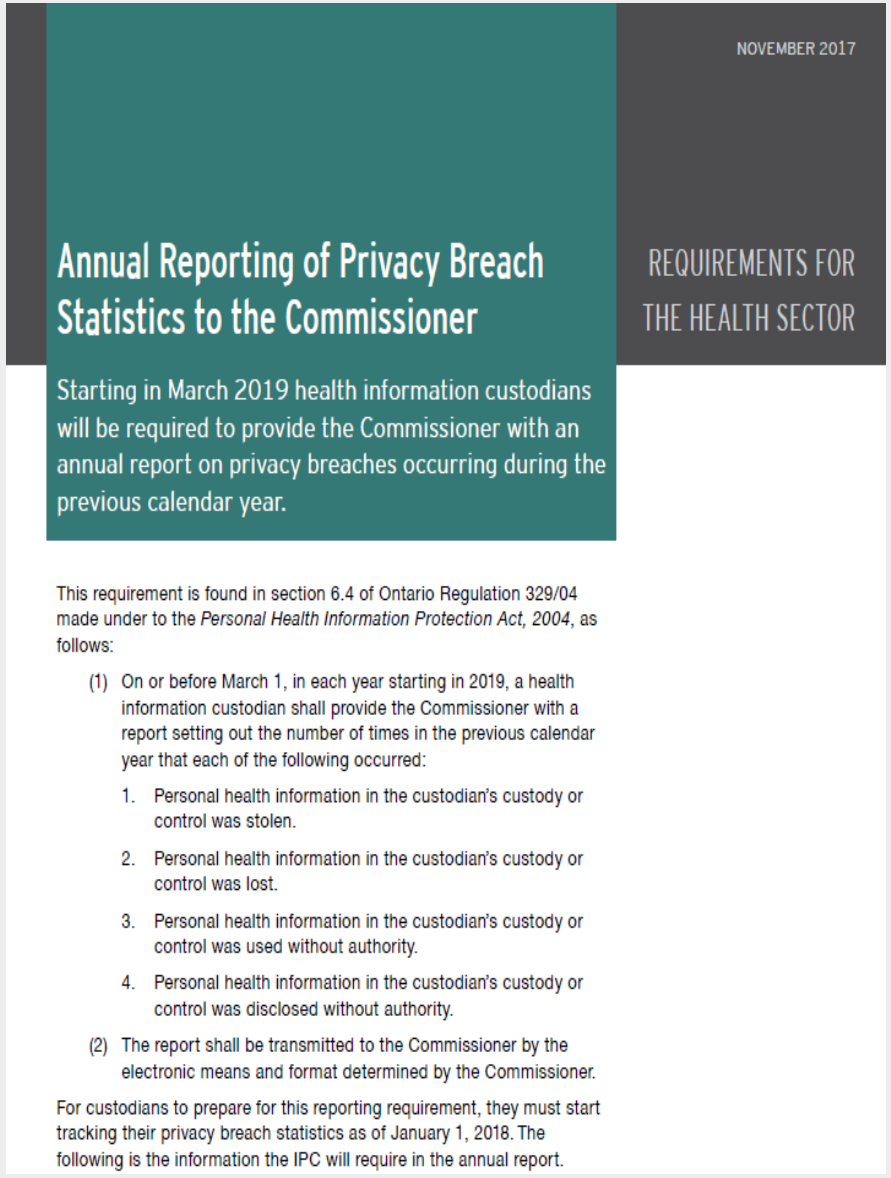
# *PHIPA* reporting to IPC obligations

- Ontario Regulation 329/04 [s. 6.3] – HIC must notify IPC where:
  1. Use or disclosure without authority
  2. Stolen information
  3. Further use or disclosure without authority after a breach
  4. Pattern of similar breaches
  5. Disciplinary action against a college member
  6. Disciplinary action against a non-college member
  7. Significant breach

# PHIPA reporting obligations

- annual breach reporting to IPC
  - HIC must provide statistical report of breaches in previous calendar year
  - must include all cases where PHI:
    - stolen
    - lost
    - used or disclosed without authority
- first reports due March 1, 2019

# IPC health sector breach reporting guidance



NOVEMBER 2017

## Annual Reporting of Privacy Breach Statistics to the Commissioner

REQUIREMENTS FOR THE HEALTH SECTOR

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.

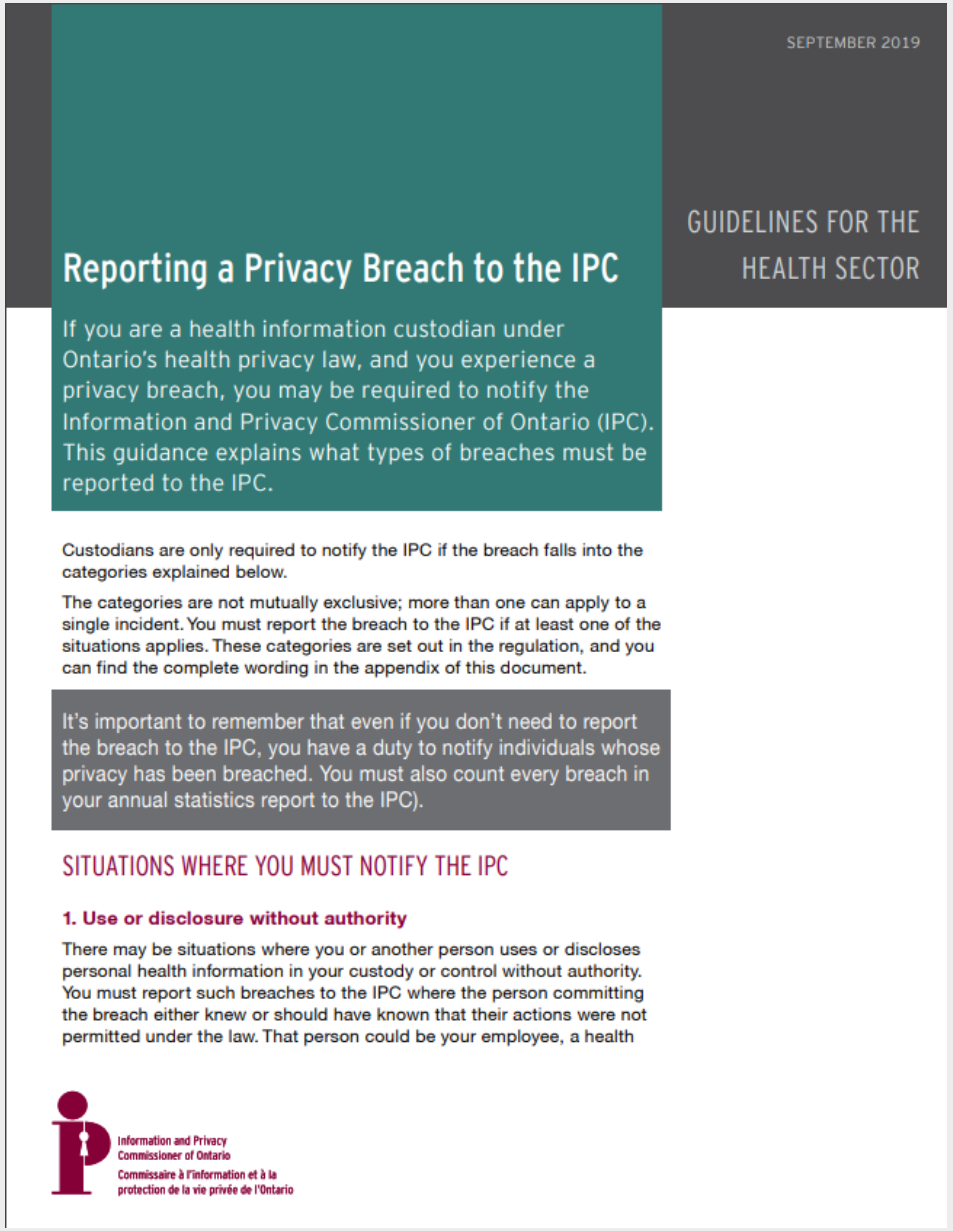
This requirement is found in section 6.4 of Ontario Regulation 329/04 made under to the *Personal Health Information Protection Act, 2004*, as follows:

(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.



SEPTEMBER 2019

## Reporting a Privacy Breach to the IPC

GUIDELINES FOR THE HEALTH SECTOR

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).

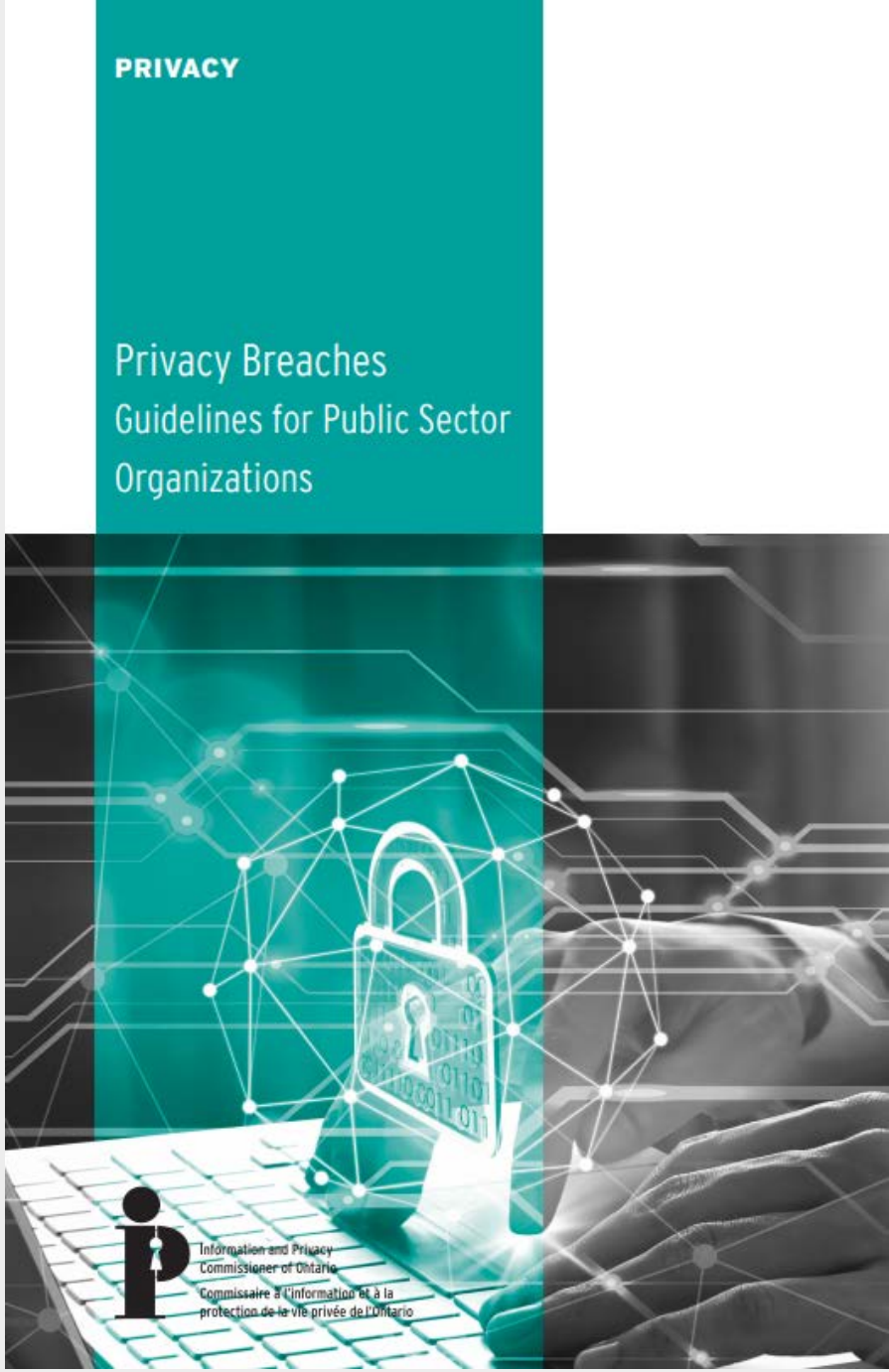
### SITUATIONS WHERE YOU MUST NOTIFY THE IPC

**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

# IPC guidelines for public sector on responding to privacy breaches



# PHIPA reported privacy breaches

- 11,278 reported to IPC in 2018

| | Stolen Personal Health Information | % | Lost Personal Health Information | % | Used Without Authority | % | Disclosed Without Authority | % | Total | % |
|---|---|---|---|---|---|---|---|---|---|---|
| One individual | 9 | 11.54 | 256 | 74.64 | 431 | 71.36 | 9,504 | 92.69 | 10,200 | 90.44 |
| 2 to 10 individuals | 29 | 37.18 | 55 | 16.03 | 110 | 18.21 | 617 | 6.02 | 811 | 7.19 |
| 11 to 50 individuals | 14 | 17.95 | 17 | 4.96 | 45 | 7.45 | 106 | 1.03 | 182 | 1.61 |
| 51 to 100 individuals | 5 | 6.41 | 5 | 1.46 | 10 | 1.66 | 10 | 0.10 | 30 | 0.27 |
| Over 100 individuals | 21 | 26.92 | 10 | 2.92 | 8 | 1.32 | 16 | 0.16 | 55 | 0.49 |
| **Total** | **78** | **100.0** | **343** | **100.0** | **604** | **100.0** | **10,253** | **100.0** | **11,278** | **100.0** |

# Responding to a privacy breach

- have breach response plan - steps to take when breach occurs
- plan will depend on organization type, nature/amount of personal information organization holds

# Responding to a privacy breach

- alert relevant people in organization
  - privacy officer, lawyer, anyone who may need to be involved in responding to breach
- contain breach
  - identify nature/scope
  - what personal information is involved?
  - take corrective action, including:
    - ensure unauthorized people don't retain PI
    - prevent any additional unauthorized access
    - suspend access to PI by people who accessed it without authorization

# Responding to a privacy breach

- investigate the breach
  - identify, analyze events that led to breach, determine cause
  - if breach due to a systemic issue, review program-wide procedures
  - review breach response plans, privacy policies, staff training

# What happens when IPC investigates a breach?

- Commissioner may
  - assess if breach contained
  - determine if affected individuals notified [plus advise on method of notice]
  - advise on steps to mitigate
  - interview individuals involved
  - review, advise on organization's policies and procedures
  - issue a report after investigation
- investigation forward looking – how to prevent future breaches?

# Cooperation between regulators

- privacy regulators in Canada and internationally may act cooperatively to address multi-jurisdictional issues:
  - Casino Rama cyber attack (2016)
    - ❖IPC/O involved with Ontario Lottery and Gaming Corporation (*FIPPA* public institution)
    - ❖Privacy Commissioner of Canada involved with Casino Rama (private sector company)

# 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