

# *PHIPA* Update from the IPC

Brian Beamish

Information and Commissioner Of Ontario



Information and Privacy  
Commissioner of Ontario

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

PHIPA Connections  
Summit 2018

Toronto, Canada

December 4, 2018



# Impact of Breach Notification

# Mandatory *PHIPA* Breach Reporting

- As of October 1, 2017, health information custodians must notify IPC of certain privacy breaches
  - use or disclosure without authorization
  - stolen information
  - further use or disclosure
  - breaches occurring as part of a pattern
  - breaches related to a disciplinary action against a college or non-college member
  - significant breaches
- Custodians began collecting breach statistics in January 2018 for reporting in March 2019

## Reporting a Privacy Breach to the Commissioner

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.

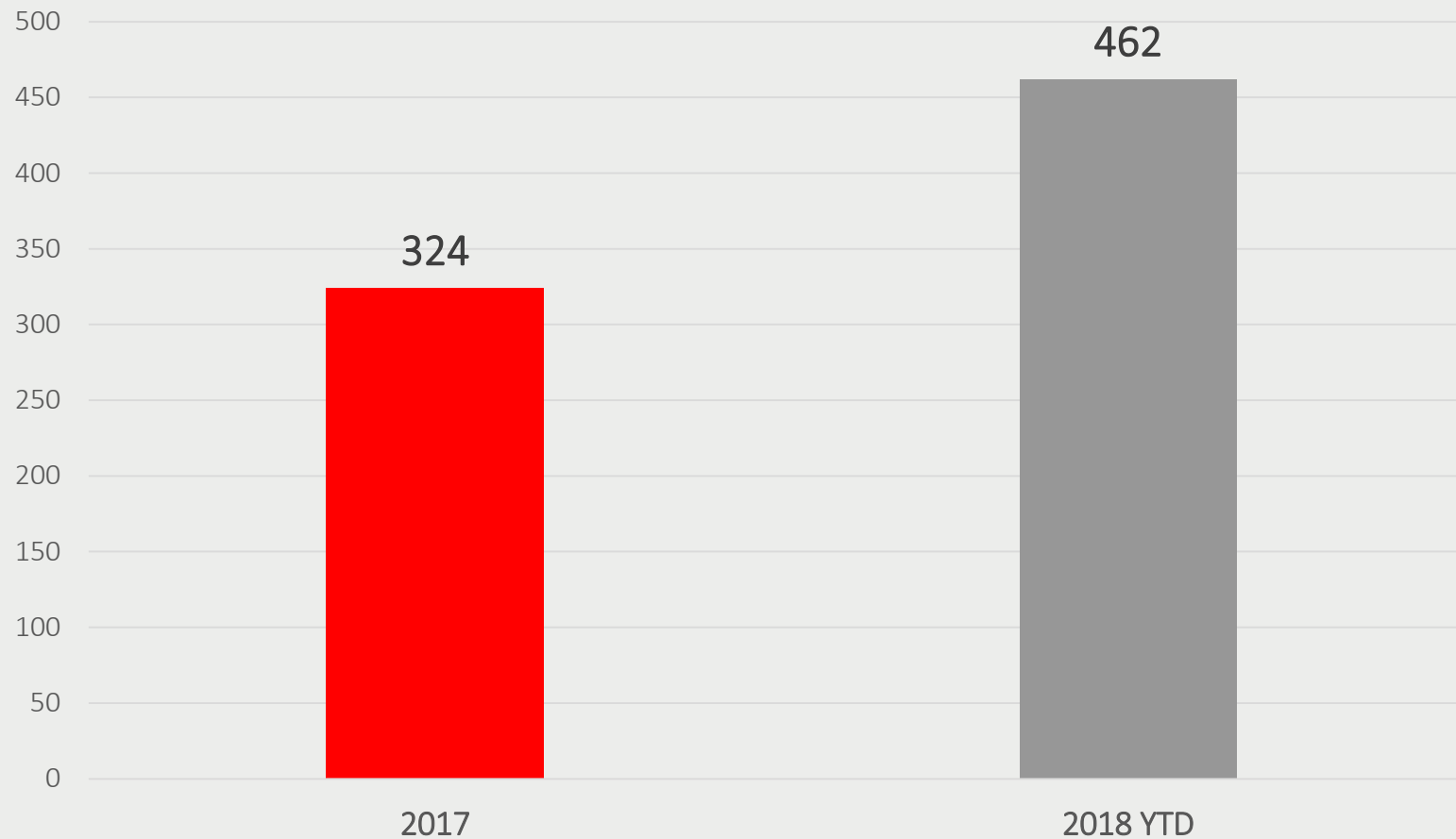
It is important to remember that even if you do not need to notify the Commissioner, you have a separate duty to notify individuals whose privacy has been breached under section 12(2) of the act.

### SITUATIONS WHERE YOU MUST NOTIFY THE COMMISSIONER OF A PRIVACY BREACH

#### 1. Use or disclosure without authority

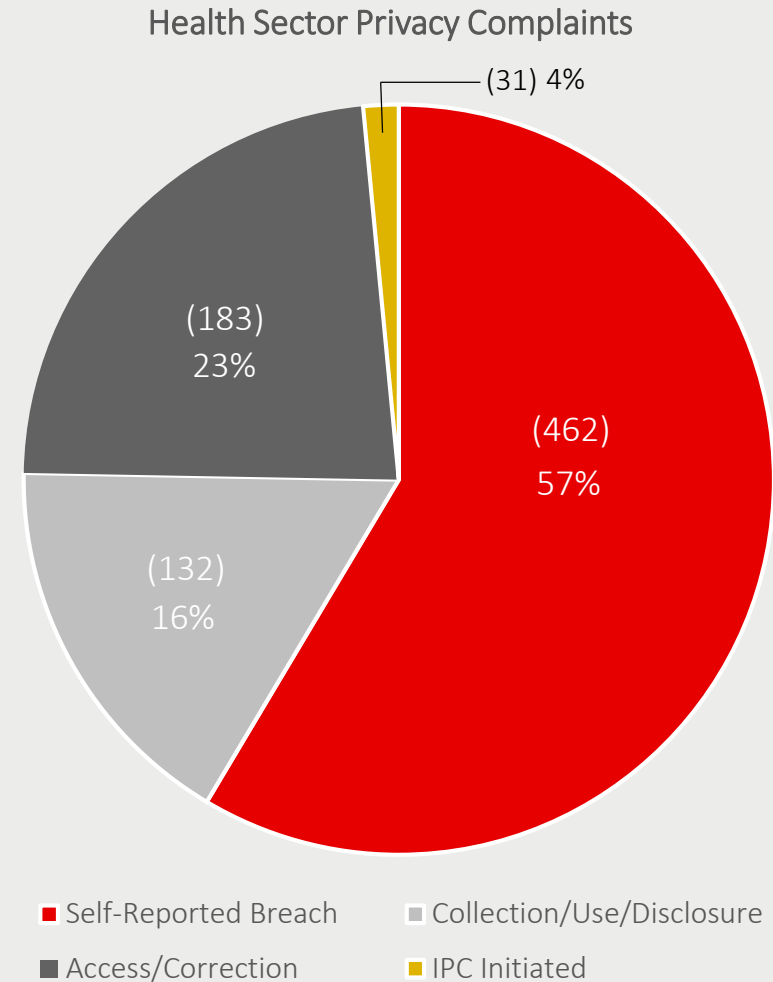
This category covers situations where the person committing the breach knew or ought to have known that their actions are not permitted either by the act or the responsible custodian. An example would be where a

# Self-Reported Breaches Before and After Mandatory Breach Reporting



# Health Sector Privacy Complaints 2018 (YTD)

- Of the 462 self-reported breaches in 2018:
  - 107 were snooping incidents
  - 12 were ransomware/cyberattack
- Remaining 343 were related to:
  - lost or stolen PHI
  - misdirected information
  - records not properly secured
  - other collection, use and disclosure issues

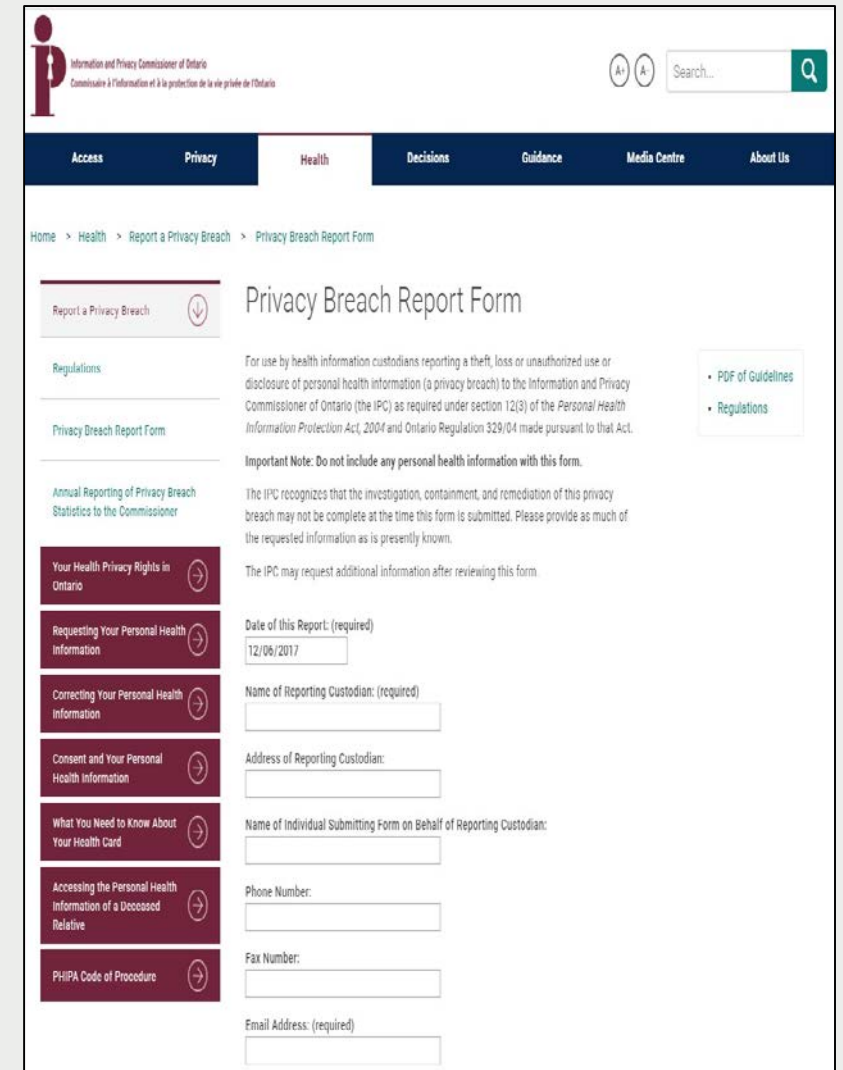


# IPC Privacy Breach Online Report Form

Although you can report breaches by mail or fax, we recommend that you use our online report form.

You will be asked to provide:

- a description of the breach
- steps taken to contain the breach
- steps taken to notify affected individuals
- steps taken to investigate and remediate the breach



The screenshot shows the online report form for a privacy breach. The page is titled "Privacy Breach Report Form" and is part of the Information and Privacy Commissioner of Ontario's website. The form is designed for health information custodians to report a theft, loss, or unauthorized use or disclosure of personal health information. It includes a navigation menu with options like "Access", "Privacy", "Health", "Decisions", "Guidance", "Media Centre", and "About Us". The main content area features a "Report a Privacy Breach" button, a "Regulations" link, and a "Privacy Breach Report Form" link. A sidebar on the left contains several links related to health privacy rights and information. The main form area contains an "Important Note" and a "Date of this Report" field. Below this are fields for "Name of Reporting Custodian", "Address of Reporting Custodian", "Name of Individual Submitting Form on Behalf of Reporting Custodian", "Phone Number", "Fax Number", and "Email Address".

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

Search...

Access Privacy Health Decisions Guidance Media Centre About Us

Home > Health > Report a Privacy Breach > Privacy Breach Report Form

Report a Privacy Breach

Regulations

Privacy Breach Report Form

Annual Reporting of Privacy Breach Statistics to the Commissioner

Your Health Privacy Rights in Ontario

Requesting Your Personal Health Information

Correcting Your Personal Health Information

Consent and Your Personal Health Information

What You Need to Know About Your Health Card

Accessing the Personal Health Information of a Deceased Relative

PHIPA Code of Procedure

Privacy Breach Report Form

For use by health information custodians reporting a theft, loss or unauthorized use or disclosure of personal health information (a privacy breach) to the Information and Privacy Commissioner of Ontario (the IPC) as required under section 12(3) of the Personal Health Information Protection Act, 2004 and Ontario Regulation 329/04 made pursuant to that Act.

• PDF of Guidelines  
• Regulations

**Important Note: Do not include any personal health information with this form.**

The IPC recognizes that the investigation, containment, and remediation of this privacy breach may not be complete at the time this form is submitted. Please provide as much of the requested information as is presently known.

The IPC may request additional information after reviewing this form.

Date of this Report: (required)  
12/06/2017

Name of Reporting Custodian: (required)  
[Text Input Field]

Address of Reporting Custodian:  
[Text Input Field]

Name of Individual Submitting Form on Behalf of Reporting Custodian:  
[Text Input Field]

Phone Number:  
[Text Input Field]

Fax Number:  
[Text Input Field]

Email Address: (required)  
[Text Input Field]

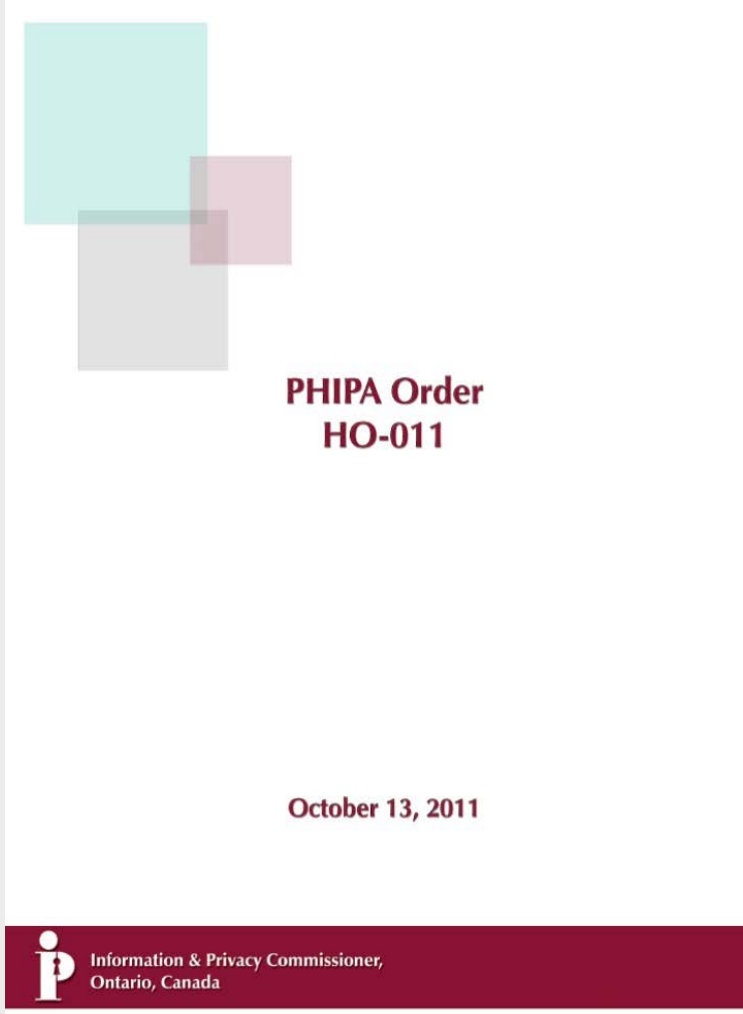


Examples: report or not?

# Significant Breaches


Is it a significant breach?  
Consider the circumstances:

- How sensitive is the information?
- How many records are involved?
- How many individuals are affected?
- Is more than one health information custodian or agent involved?

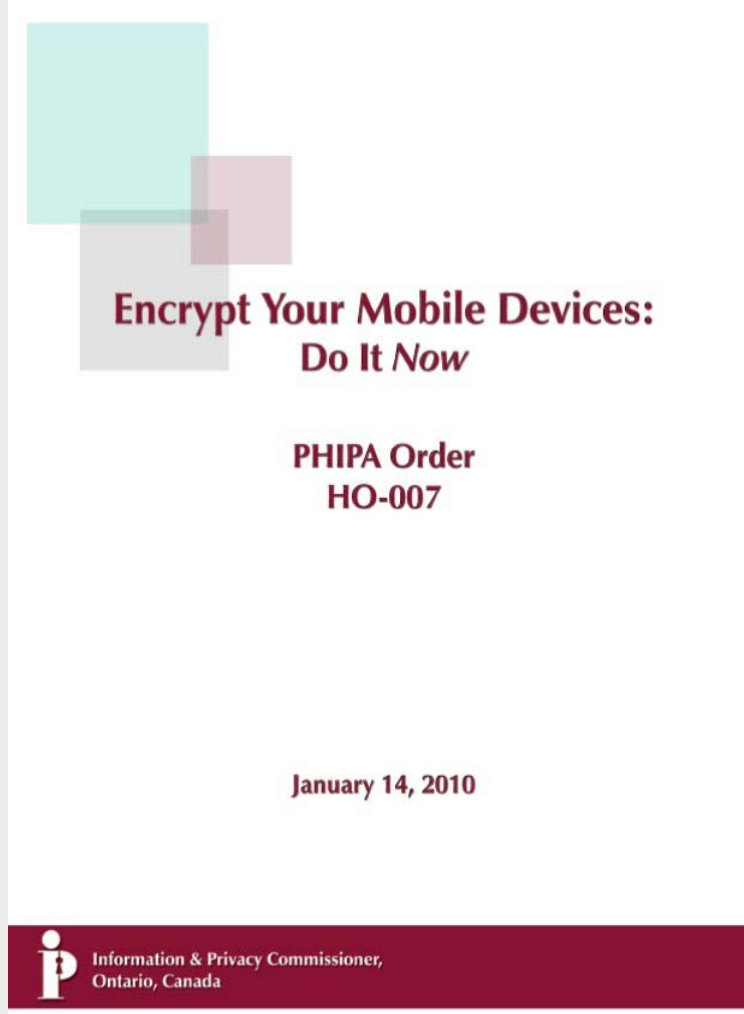


PHIPA Order  
HO-011

October 13, 2011

 Information & Privacy Commissioner,  
Ontario, Canada


The cover features a decorative graphic of three overlapping squares in teal, grey, and pink in the upper left corner. The text is centered on the page.



**Encrypt Your Mobile Devices:  
Do It Now**

PHIPA Order  
HO-007

January 14, 2010

 Information & Privacy Commissioner,  
Ontario, Canada

The cover features a decorative graphic of three overlapping squares in teal, grey, and pink in the upper left corner. The text is centered on the page.



# When You May Not Need to Report a Breach

- You may not need to report a breach if:
  - it is not intentional
  - it is a one-off incident
  - it is not part of a pattern
- Not every breach is significant
  - nurse clicks on the wrong patient file
  - records clerk opens the wrong file folder
  - doctor walks into the wrong patient room

# Mandatory Breach Reports We've Received

## – the Major and the Minor

- Agent of a local health integration network experienced a ransomware attack where the health and financial information of patients was accessed
  - information included telephone numbers, addresses, dates of birth, health card numbers, medical histories and credit card information
- Audit of a hospital's electronic medical record system revealed that a nursing student accessed the credentials of a staff physician
  - student used physician's credentials to modify patient records for fraudulent purposes such as writing prescriptions
  - student was charged with forgery
- One clinic misdirected a fax to another clinic by mistake
- Prescription was handed to the wrong person with a similar name who handed it back and it was given to the proper person

# A Tale of Two Pharmacies

## 1. Now You See It, Now You Don't

- pharmacist placed a prescription on the countertop with the label facing the public for a very brief time

## 2. Reuse, Recycle, Reveal

- pharmacist was reusing prescription containers and putting new labels over old ones
- new labels could be peeled off exposing personal information on the old label





Unauthorized Access

# Meaning of Unauthorized Access

- When you view, handle or otherwise deal with PHI without consent and for purposes not permitted by *PHIPA*, for example:
  - when not providing or assisting in the provision of health care to the individual; and
  - when not necessary for the purposes of exercising employment, contractual or other responsibilities
- The act of viewing PHI on its own, without any further action, is an unauthorized access

# Consequences of Unauthorized Access

- Review or investigation by privacy oversight bodies
- Prosecution for offences
- Statutory or common law actions
- Discipline by employers
- Discipline by regulatory bodies

# Prosecutions

To date, six individuals have been prosecuted:

- **2011** – a nurse at North Bay Health Centre
- **2016** – two radiation therapists at a Toronto Hospital
- **2016** – a registration clerk at a regional hospital
- **2017** – a social worker at a family health team
- **2017** – an administrative support clerk at a Toronto hospital

# Guidance Document: Detecting and Deterring Unauthorized Access

Impact of unauthorized access

Reduce risk through:

- policies and procedures
- training and awareness
- privacy notices and warning flags
- confidentiality and end-user agreements
- access management
- logging, auditing and monitoring
- privacy breach management
- discipline



## Detecting and Deterring Unauthorized Access to Personal Health Information



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





# Logging, auditing and monitoring

- Manual or semi-manual auditing may have a deterrent effect, but are resource intensive and may not enhance ability to detect and prevent unauthorized access
- Discipline, fines and prosecutions may have a deterrent effect, but are resource intensive and do not enhance ability to detect and prevent unauthorized access
- Big data analytics and artificial intelligence are being used to more effectively deter, detect and prevent unauthorized access

# Innovative Procurement of Audit Solution

- The IPC was approached by Mackenzie Health in 2015 to participate in the steering committee to provide the perspective from a regulatory point of view
- Mackenzie Health partnered with the Mackenzie Innovation Institute (Mi2) on an innovation-based procurement approach.
- In collaboration with Mi2, Michael Garron Hospital, Markham Stouffville Hospital, and vendor KI Design, Mackenzie Health addressed the challenge of auditing transactions through the Privacy Auditing Innovation Procurement (PAIP) project
- IPC provided comments throughout the project, particularly on the project objectives and assessment criteria
- IPC provided real life examples of unauthorized access for testing

# Results of Pilot

- Solution used big data analytics and artificial intelligence to determine what accesses could be explained
- A small portion of unexplained accesses were flagged for further investigation
- During the six month pilot, many privacy breaches were detected
- The number of breaches decreased significantly as the solution was fine tuned and missing information from various information systems (e.g., scheduling) was added
- The number of breaches is expected to decrease further with staff awareness and increased ability for solution to explain accesses

# Health Information Custodians must provide breach statistics starting in 2019.

## They must track incidents where PHI is:

- stolen
- lost
- used without authority
- disclosed without authority

This includes breaches that did not meet the criteria for mandatory reporting to the IPC.

## 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.

WELCOME TO  
BIENVENUE AU



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

Online Statistics Submission  
Website

Site Web de présentation des  
statistiques annuelles

Login/ Nom d'utilisateur:

Password/Mot de passe:

LOGIN

Forgot your password? [Please Click Here](#).

Vous avez oublié votre mot de passe ? S'il vous plaît [Cliquez ici](#).



# Privacy Breach Reporting

- The more effective the auditing and monitoring, the more privacy breaches that will be detected
- Those using innovative audit solutions will likely have more breaches to report, but over time the number of breaches is expected to decline
- IPC will **NOT** be identifying any health care organizations in our first annual report of privacy breaches



# Latest *PHIPA* Guidance

# *Responding to a Health Privacy Breach*

1. notify staff and other custodians
2. identify the scope of the breach and take steps to contain it
3. notify individuals affected by the breach, the IPC, and/or the regulatory colleges
4. investigate and remediate

This publication replaces the guidance document, *What to do When Faced With a Privacy Breach: Guidelines for the Health Sector*

Responding to a Health  
Privacy Breach: Guidelines for  
the Health Sector



## Clarifying Access Requests

Individuals who request access to information under the *Personal Health Information Protection Act, 2004* (the *Act*) do not always know the type of records a health information custodian has about them, or how those records are organized. For this reason, clarification is often required.

The purpose of this issue of *PHIPA* Practice Direction is to remind health information custodians of the legislative requirements regarding the clarification of requests; and to emphasize that clarification will make things easier for everyone concerned—the health information custodian; requesters, complainants and the Information and Privacy Commissioner/ Ontario (IPC).

It is vital that health information custodians have a clear understanding of the nature and scope of requests in order to process them efficiently and to satisfy the requester's right of access.

### REQUIREMENT FOR REQUESTERS

The *Act* specifies that a person seeking access to his or her own personal health information must provide sufficient detail to enable the health information custodian to identify and locate the record with reasonable efforts.

It is vital that health information custodians have a clear understanding of the nature and scope of requests in order to process them efficiently and to satisfy the requester's right of access.

## Clarifying Access Requests

- remind health information custodians of the legislative requirements regarding the clarification of requests
- emphasize that clarification will make things easier for everyone concerned

Health information custodians should have a clear understanding of the nature and scope of requests to process them efficiently and to satisfy a requester's right of access

## PUBLICLY RELEASED DECISIONS UNDER THE *PERSONAL HEALTH INFORMATION PROTECTION ACT, 2004*

This practice direction should be read in conjunction with the *Code of Procedure for Matters under the Personal Health Information Protection Act*.

# Publicly Released Decisions

- when a *PHIPA* Decision will be made available to the public
- which parties will be identified by name in that decision

### APPLICATION

This practice direction describes when a Decision of the Office of the Information and Privacy Commissioner of Ontario (the IPC) made pursuant to the *Personal Health Information Protection Act* (the Act) will be made available to the public.

When a Decision of the IPC pursuant to the Act is made available to the public, this practice direction describes which Parties will be identified by name in that public Decision.

### SETTLED, WITHDRAWN OR ABANDONED COMPLAINTS

Where a file is closed because a Complaint is settled, withdrawn or abandoned, the IPC will not issue a public Decision.

### INTAKE STAGE

Decisions of the IPC at the Intake Stage will not be made available to the public except as described in the following paragraph.

Where an Analyst conducts a Review of a Deemed Refusal, Failure to Provide Access or Expedited Access Complaint, Decisions made in, or at the conclusion of, that Review will be made available to the public. Such Decisions will not name the Complainant or the person whose personal health information is at issue. This public Decision will name the Respondent(s) (unless doing so would identify the Complainant or the

# IPC Webinar



<https://youtu.be/KjitJ74wn4A>





# Decisions and Orders of Note

# Right of Correction

## PHIPA Decision 67

- A complainant submitted a 62-part request to correct her health records, to the Toronto Central Local Health Integration Network (TCLHIN)
- TCLHIN agreed to make two of the requested corrections but denied the remainder citing that the complainant did not demonstrate that the records were incomplete or inaccurate
- Complainant appealed the decision to our office
- The IPC decided that the TCLHIN was not required to make the corrections
- Most of the corrections were about differences of opinion and the complainant did not prove that the information was inaccurate or incomplete
- Some of the information consists of good faith professional opinions

# An Insurance Company

## PHIPA Decision 56

- Insurance company was collecting OHIP numbers through its application process for purchasing supplementary health insurance plans
- This collection of OHIP numbers contravened *PHIPA*
- However, collecting and using OHIP numbers when emergency travel claims were filed was found to be permissible
- Insurance company discontinued its practice of collecting OHIP numbers and deleted OHIP numbers from its administrative system

# Applying *PHIPA* and *FIPPA* to Records of Complaints

- **Order PO-3861**
- Addresses the applicability of both *PHIPA* and *FIPPA* to a patient's request for records about his complaints against physicians at a hospital
- Appellant was entitled under *PHIPA* to only his personal health information in the records
- Hospital claimed many records were excluded from *FIPPA* on the basis that they relate to hospital privileges
- IPC rejected this claim for most of the records
- They were created in order to respond to the appellant's complaints, not for the hospital to determine whether to take disciplinary or other workplace action against the physicians
- Order will assist in sorting out whether *FIPPA* or *PHIPA* applies to records



What's Coming



# What We are Working On

- **Genetic information** – factors to consider before increasing its availability through shared electronic systems
- **Abandoned records** – reducing the risk through succession planning prior to planned or unforeseen changes in practice
- **Consumer health apps** – what to consider before asking patients to use apps to manage their health care and access their personal health information
- **Updating *PHIPA* documents** – we are updating our *PHIPA* documents to reflect IPC decisions, legislative amendments, and evolving best practices

# Our Open Door Policy

- Any public institution or agency considering programs which may impact privacy can approach IPC for advice
- Most privacy challenges can be addressed through collaboration
- Privacy protections can be developed and can be implemented
- It is best to address privacy concerns from the outset
- Success depends on involvement of other agencies and stakeholders

# 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](http://www.ipc.on.ca)

E-mail: [info@ipc.on.ca](mailto:info@ipc.on.ca)

Media: [media@ipc.on.ca](mailto:media@ipc.on.ca) / 416-326-3965