

Mandatory Reporting and Breach Notification

Changes to PHIPA and
what you need to know





Sarah Yun

Associate

Overview of amendment to O. Reg. 329/04 and
What you need to know



Brian Beamish

Information and Privacy Commissioner of Ontario

What to do when faced with a privacy breach and
What to expect from the IPC





ROGERS 40%

12:00

Sunday, October 1

1 CALENDAR now

Mandatory Reporting is a Reality
Today at 12:00 AM
All of Ontario

1 CALENDAR now

Visit CanLII for O. Reg. 329/04
Today at 12:00 AM

1 CALENDAR now

Register to see Brian Beamish (Dec 5)
Today at 12:00 AM
Old Mill Inn

The changing privacy landscape



3 billion people affected



145 million people affected



57 million people affected



19,000 Canadians affected



Celebrity privacy compromised



14,450 people affected

The changing privacy landscape



1 >

Digital Acceleration

More and more sensitive and confidential information is moving online



2 >

New Risk Landscape

The risk exposure of electronic health records is evolving and increasing



3 >

Evolving Legislative Direction

Additional legislative measures are required to align with the changing nature of privacy



**Ontario Legislature
introduces changes to
PHIPA**

The legal framework

ACT

Ontario PHIPA SEARCH contact us | français Topics +

Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A

- PART I
INTERPRETATION AND APPLICATION
- PART II**
PRACTICES TO PROTECT PERSONAL HEALTH INFORMATION
- PART III
CONSENT CONCERNING PERSONAL HEALTH INFORMATION
- PART IV
COLLECTION, USE AND DISCLOSURE OF PERSONAL HEALTH INFORMATION
- PART V
ACCESS TO RECORDS OF PERSONAL HEALTH INFORMATION AND CORRECTION
- PART V.1
ELECTRONIC HEALTH RECORD
- PART VI
ADMINISTRATION AND ENFORCEMENT
- PART VII
GENERAL

SECTION

10.

11.

11.1

12.

13.

14.

15.

16.

17.

17.1

12. Security

SUBSECTION

(1) Security

(2) Notice of theft, loss, etc.
to individual

(3) Notice to Commissioner

(4) Exception

If the theft, loss, or unauthorized use or disclosure meets the prescribed requirements

The seven triggers to notify the IPC

(3) Notice to
Commissioner

 Ontario Regulation
329/04

Prescribed Requirements

SECTION 6.3



Seven scenarios to familiarize yourself with

The seven triggers to notify the IPC

1

2

3

4

5

6

7

A person used or disclosed personal health information without authority



Snooping



Accidents

1. The health information custodian has reasonable grounds to believe that personal health information in the custodian's custody or control was used or disclosed without authority by a person who knew or ought to have known that they were using or disclosing the information without authority.

The seven triggers to notify the IPC

1

2

3

4

5

6

7

Personal health information
was stolen



Paper,
Electronic,
Malware



De-identified,
Encrypted

2. The health information custodian has reasonable grounds to believe that personal health information in the custodian's custody or control was stolen.

The seven triggers to notify the IPC

1

2

3

4

5

6

7

A subsequent breach flows from an initial breach



Accident leading to a breach



Single accident

3. The health information custodian has reasonable grounds to believe that, after an initial loss or unauthorized use or disclosure of personal health information in the custodian's custody or control, the personal health information was or will be further used or disclosed without authority.

The seven triggers to notify the IPC

1

2

3

4

5

6

7

Pattern of similar breaches
(similarity + time)



Malfunctioning
automated
process



Isolated
incident?

4. The loss or unauthorized use or disclosure of personal health information is part of a pattern of similar losses or unauthorized uses or disclosures of personal health information in the custody or control of the health information custodian.

The seven triggers to notify the IPC

1

2

3

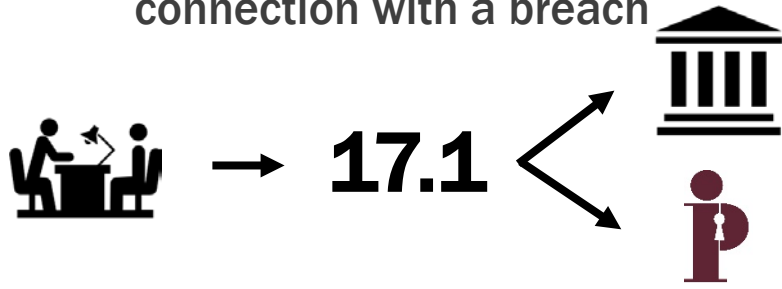
4

5

6

7

Discipline against a College member in connection with a breach



Suspension,
Termination,
Resignation



Unrelated to a
privacy breach

5. The health information custodian is required to give notice to a College of an event described in **section 17.1** of the Act that relates to a loss or unauthorized use or disclosure of personal health information.



Ontario Colleges

“College” means,

- (a) in the case of a member of health profession regulated under the *Regulated Health Professions Act, 1991*, a College of the health profession named in Schedule 1 to that Act, and
- (b) in the case of a member of the Ontario College of Social Workers and Social Service Workers, that College.



The seven triggers to notify the IPC

1

2

3

4

5

6

7

Discipline against an agent in connection with a breach



Suspension,
Termination,
Resignation



Unrelated to a
privacy breach

6. The health information custodian would be required to give notice to a College, if an agent of the health information custodian were a member of the College, of an event described in **section 17.1** of the Act that relates to a loss or unauthorized use or disclosure of personal health information.

The seven triggers to notify the IPC

1

2

3

4

5

6

7

Breach was significant



Sensitive,
High volume,
Widespread



Trivial breach

7. The health information custodian determines that the loss or unauthorized use or disclosure of personal health information is significant after considering all relevant circumstances, including the following:

- i. Whether the personal health information that was lost or used or disclosed without authority is sensitive.
- ii. Whether the loss or unauthorized use or disclosure involved a large volume of personal health information.
- iii. Whether the loss or unauthorized use or disclosure involved many individuals' personal health information.
- iv. Whether more than one health information custodian or agent was responsible for the loss or unauthorized use or disclosure of the personal health information.

What to take away

1

2

3

4

5

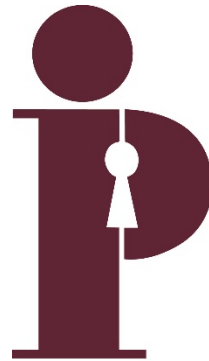
6

7



3 key points to remember:

- 1. Electronic personal health information is here to stay**
- 2. Obligation to notify the Commissioner**
- 3. Know your resources**



Information and Privacy
Commissioner of Ontario

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

Brian Beamish

The Legislative Assembly of Ontario has appointed Brian Beamish to a five-year term as Information and Privacy Commissioner, a role he had been acting in since July 1, 2014. Mr. Beamish joined the IPC as Director of Policy and Compliance in 1999 and served as Assistant Commissioner from 2005.

Up Next

Thank You

Sarah Yun
syun@weirfoulds.com

Mandatory Reporting and Breach Notification: What You Need to Know

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 2017

Toronto, Canada

December 5, 2017

Health Privacy Breach Investigations

- The IPC investigates health privacy complaints under *PHIPA*
- Investigations arise from:
 - complaints from individuals
 - reports from Health Information Custodians (HIC)
 - Commissioner's discretion
- Typical causes:
 - access to health records
 - misdirected information (wrong phone, email or fax)
 - insecure storage or destruction of records
 - loss or theft of devices (laptops, USB sticks, mobile phones)
 - unauthorized access (snooping)

What to Do When Faced With a Privacy Breach

Implement Privacy Breach Protocol

- notify your Chief Privacy Officer and all relevant staff
- identify the breach
- develop a response plan
- **determine if the breach must be reported to the IPC**

Contain and Notify

- contain the breach
- notify all affected individuals

Investigate and Remediate

- review containment measures
- confirm all individuals are notified
- review circumstances of breach
- review your policies and procedures
- develop recommendations to prevent future breaches
- Implement recommendations

Reporting a Breach to the IPC

You must notify the IPC in cases of:

- unauthorized use or disclosure
- stolen information
- further use or disclosure after a breach
- pattern of similar breaches
- disciplinary action against a college or non-college member
- significant breach

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

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

Duty to Notify Individuals

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.

Reporting a Breach to the IPC

The screenshot displays the 'Privacy Breach Report Form' on the Information and Privacy Commissioner of Ontario website. The page includes a navigation menu with 'Access', 'Privacy', 'Health', 'Decisions', 'Guidance', 'Media Centre', and 'About Us'. The 'Health' section is active. The breadcrumb trail is 'Home > Health > Report a Privacy Breach > Privacy Breach Report Form'. The main content area features a sidebar with links to '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', and 'PHIPA Code of Procedure'. The main content area contains the following text: '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.' It also includes an 'important Note: Do not include any personal health information with this form.' and a note that '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.' and 'The IPC may request additional information after reviewing this form.' The form fields include: 'Date of this Report: (required)' with a date picker set to 12/06/2017; 'Name of Reporting Custodian: (required)' with a text input field; 'Address of Reporting Custodian:' with a text input field; 'Name of Individual Submitting Form on Behalf of Reporting Custodian:' with a text input field; 'Phone Number:' with a text input field; 'Fax Number:' with a text input field; and 'Email Address: (required)' with a text input field. There are also links for 'PDF of Guidelines' and 'Regulations'.

Although you can report breaches by mail or fax, we recommend that you use the online breach 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 or remediate

What to Expect

Intake Stage

- file may be closed quickly if the breach is not significant, the information provided is complete, and the IPC is satisfied with steps taken
- analyst may contact HIC to clarify the facts and issues
- goal is to informally resolve any issues raised by the breach

Investigation/Mediation Stage

- IPC investigates whether HIC has adequately responded to breach, and any additional issues raised by the breach
- file may be closed by decision or mediator's report
- where a complainant is involved, IPC attempts to find a consensual resolution
- if not resolved or closed, file is sent to adjudication

Adjudication

- IPC reviews facts of case, may close case without a review, or start a review
- If Notice of Review is issued, parties involved may provide further details and facts
- Adjudicator will issue a decision to resolve all the issues, which may include orders and recommendations
- IPC may follow-up to ensure compliance

Closing a Privacy Breach File

Corrective Action

- Did the HIC satisfactorily deal with the breach?
 - investigated and contained the breach
 - notified the affected parties
 - contacted the IPC

Collaboration

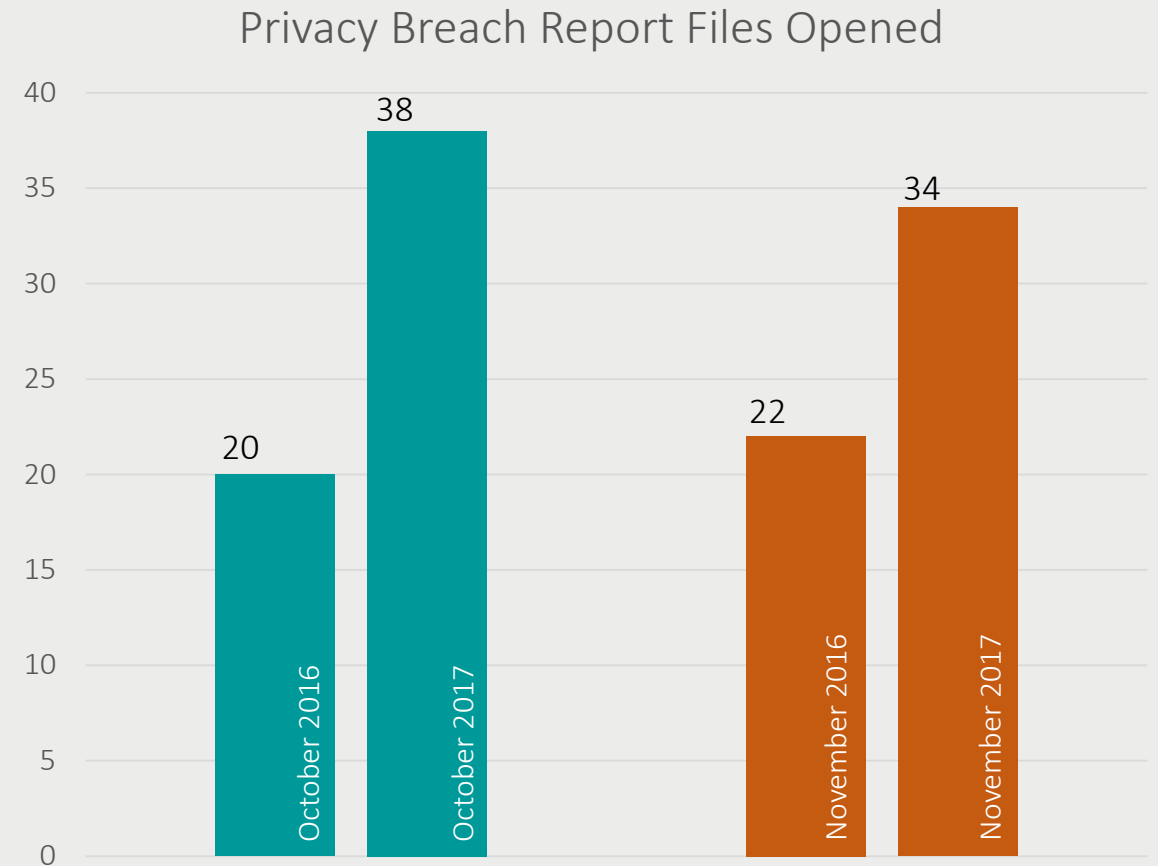
- respond full and quickly to IPC inquiries
- open to resolving concerns of affected parties

Compliance

- requirements of *PHIPA* have been met
- commitment to following recommendations for improvement
- commitment to reporting back to IPC when requested

Health Privacy Breach Statistics

- Out of the 269 reported breaches to date in 2017:
 - 43 were snooping incidents
 - 8 were ransomware/cyberattack
- Remaining 218 were related to:
 - lost or stolen PHI
 - misdirected information
 - records not properly secured
 - general collection, use and disclosure





Examples: Report or not?

Accidental Breaches

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

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

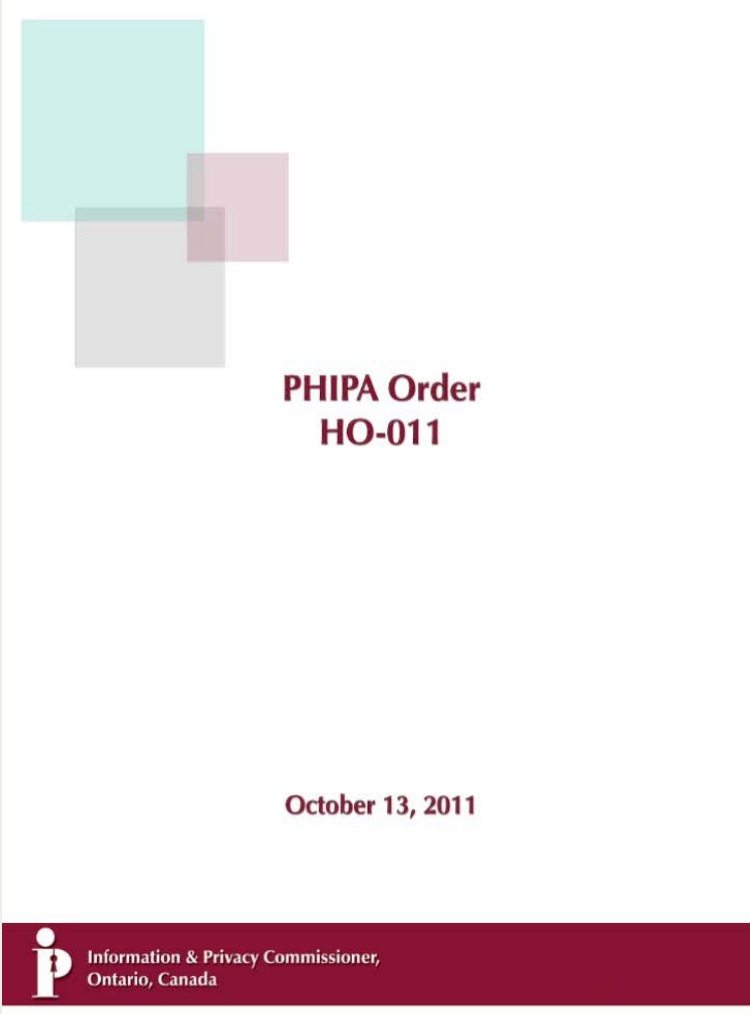
- pharmacist was reusing prescription containers and putting new labels over old ones
- new labels could be peeled off exposing PHI on the old label



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?

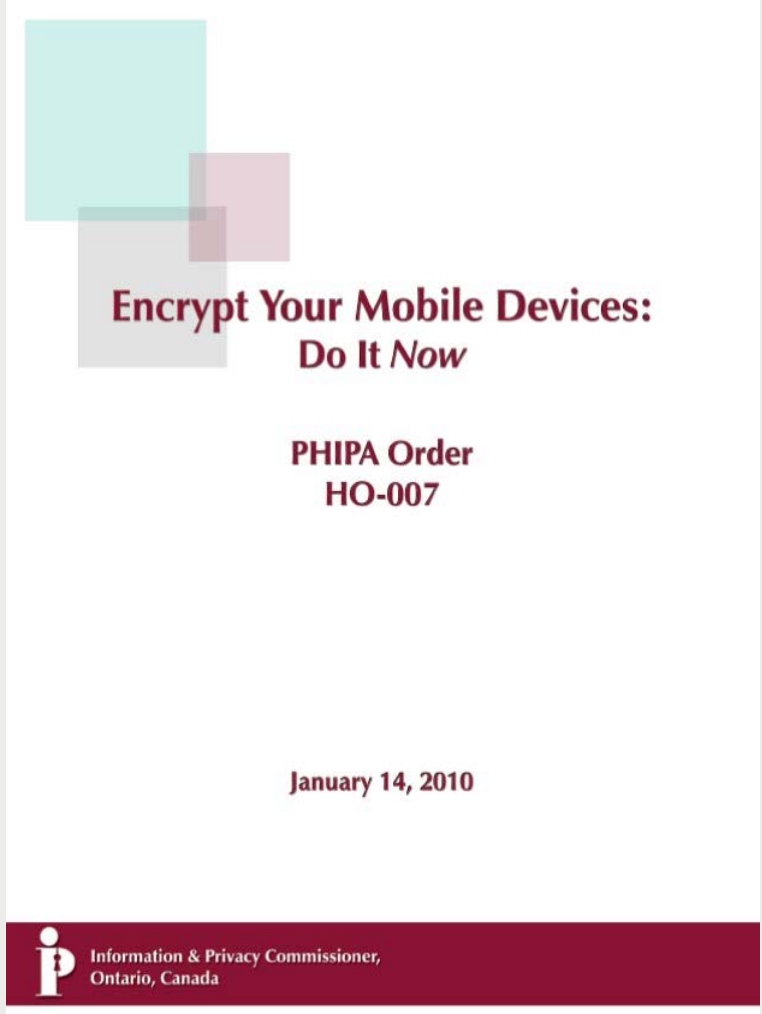


PHIPA Order
HO-011

October 13, 2011

 Information & Privacy Commissioner,
Ontario, Canada


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



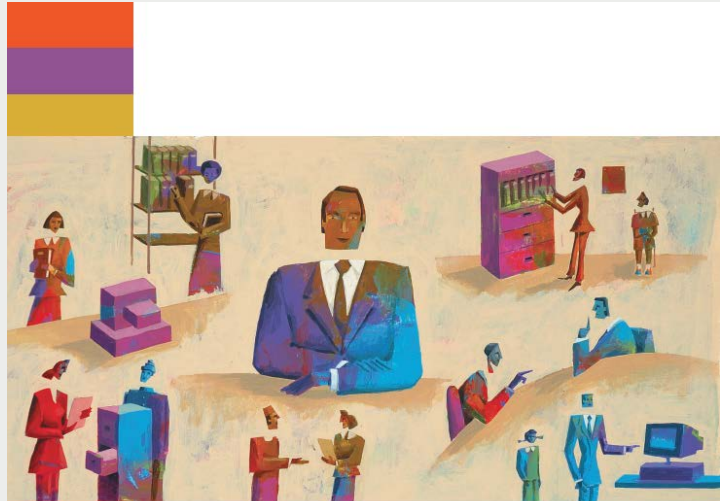
IPC Guidance



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



What to do When Faced With a Privacy Breach: Guidelines for the Health Sector



INFORMATION AND PRIVACY
COMMISSIONER OF ONTARIO

SEPTEMBER 2017

GUIDELINES FOR THE HEALTH SECTOR

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



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

An Ounce of Prevention ...

- a PIA can help identify privacy risks to your practice or institution and provide risk-mitigation strategies
- this guide can help to identify privacy solutions and prepare an effective PIA report



Planning for Success: Privacy Impact Assessment Guide



Information and Privacy
Commissioner of Ontario

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



Annual Reporting of Privacy Breach Statistics

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.

Begin tracking January 1, 2018

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.](#)



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