

REACHING OUT
TO ONTARIO

PROTECTING PERSONAL HEALTH INFORMATION

Debra Grant, Director of Health Policy
Suzanne Brocklehurst, Registrar

Barrie

November 23, 2018

Topics

- Abandoned records
- Unauthorized access
- Point-in-time breach reporting
- Annual breach reporting

REACHING OUT
TO ONTARIO

Abandoned Records



Abandoned Records

- Since *PHIPA* came into effect, the IPC has investigated numerous instances of abandoned health records
- This typically occurs when a custodian relocates, retires, becomes incapacitated or otherwise ceases to practice
- Despite the legislative requirements to safeguard PHI in the custody or control of a custodian, records of PHI continue to be abandoned
- No entity or person has the authority to assume custody and control of abandoned records
- This may lead to privacy breaches, patients not being able to exercise their right of access, and health care providers not have accurate and complete information for health care purposes

Previous Guidance

- In 2007, the IPC issued guidance on how to avoid abandoned records
 - *How to Avoid Abandoned Records: Guidelines on the Treatment of Personal Health Information, in the Event of a Change in Practice*
 - *Checklist for Health Information Custodians in the Event of a Planned or Unforeseen Change in Practice*
- The guidance focused on what to do in the event of a change in practice

How to Avoid Abandoned Records

- Who is the custodian in the event of a change in practice?
- What obligations are imposed on custodians in the event of a change in practice?
- What are best practices in the event of a change in practice?

**How to Avoid Abandoned Records:
Guidelines on the Treatment of
Personal Health Information,
in the Event of a Change in Practice**

Ongoing Challenges

- Custodians are not being proactive, and records are being left behind or disposed of in an unsecure manner
- It may be difficult to identify or locate the custodian
- There may be no plan for transferring custody and control if the practitioner becomes incapacitated or dies
- There may be no plan for ongoing retention of records when a practitioner retires or relocates to another jurisdiction

Jurisdictional Scan – Codes of Conduct

- Some regulatory colleges have included the requirement for members to notify the college before they leave or move their practice in their policies and codes of conduct
- Notification must include the location and disposition of records and a named successor who will provide continued access to the records
- Some regulatory colleges have made the abandonment of health records an act of professional misconduct

Jurisdictional Scan – Amendments to Health Privacy Law

- Some jurisdictions supplemented the initiatives of regulatory colleges with amendments to their health privacy legislation
- Saskatchewan amended its *Health Information Protection Act* to authorize the Ministry of Health to appoint a person to act in place of a former trustee who abandoned records
- Additionally, abandoning records in Saskatchewan is now subject to a liability offence of up to \$50,000 for individuals
- Saskatchewan includes a reverse onus clause – this means trustees must demonstrate that they took reasonable steps to prevent the abandonment of the records

Jurisdictional Scan – Amendments to Laws Governing Providers

- Some jurisdictions supplemented the initiatives of regulatory colleges with amendments to legislation governing providers
- Manitoba amended its *Regulated Health Professions Act*
- This amendment has not yet been proclaimed
- When proclaimed, the College will be permitted to appoint a member to take over the responsibility of securing the records or apply to the Court to designate a custodian
- Members of each college will have a duty to ensure that their records are not abandoned
- Members who abandon health records will be guilty of an offence and liable to a fine up to \$50,000

Strategy to Prevent Abandoned Records

- One-page document encouraging health care professionals to develop and implement a plan of succession
- Updating previous guidance documents
- Two documents – the guidance and the checklist – have been combined into one

Avoiding Abandoned Records

- Who is the custodian?
 - in the event of death? bankruptcy? transfer?
 - in a group practice?
- What obligations do custodian have?
 - must retain, transfer and disposed of records in a secure manner
 - must take reasonable steps to prevent privacy breaches
 - must notify individuals of a transfer
- How to avoid abandoned records?
 - succession plan setting out roles and responsibilities
- What to do if you discover abandoned records

REACHING OUT
TO ONTARIO

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

Examples of Unauthorized Access – Education and Quality Improvement

- There have been a number of instances where agents have accessed PHI claiming it was for:
 - their own educational purposes
 - to improve the quality of the health care they provide
 - other uses permitted by *PHIPA*
- Demonstrating such accesses are unauthorized may be difficult where the custodian does not:
 - have clear policies specifying the purposes for which access is and is not permitted
 - have procedures that must be followed when accessing information for purposes other than providing care
 - inform agents what access is permitted and is not permitted, including through training, notices, flags, agreements, etc.

Examples of Unauthorized Access – Health Professionals with Privileges

- Agents may have off-site practices where they, and their staff, have access to PHI on the custodian's electronic information system
- For example, a doctor with privileges at a hospital may operate a clinic where he or she employs administrative staff and this staff may have access to the hospital's information system
- Where this doctor employs staff with access to PHI in the custody or control of the hospital, both the doctor and hospital are responsible for the activities of the staff

Health Professionals with Privileges

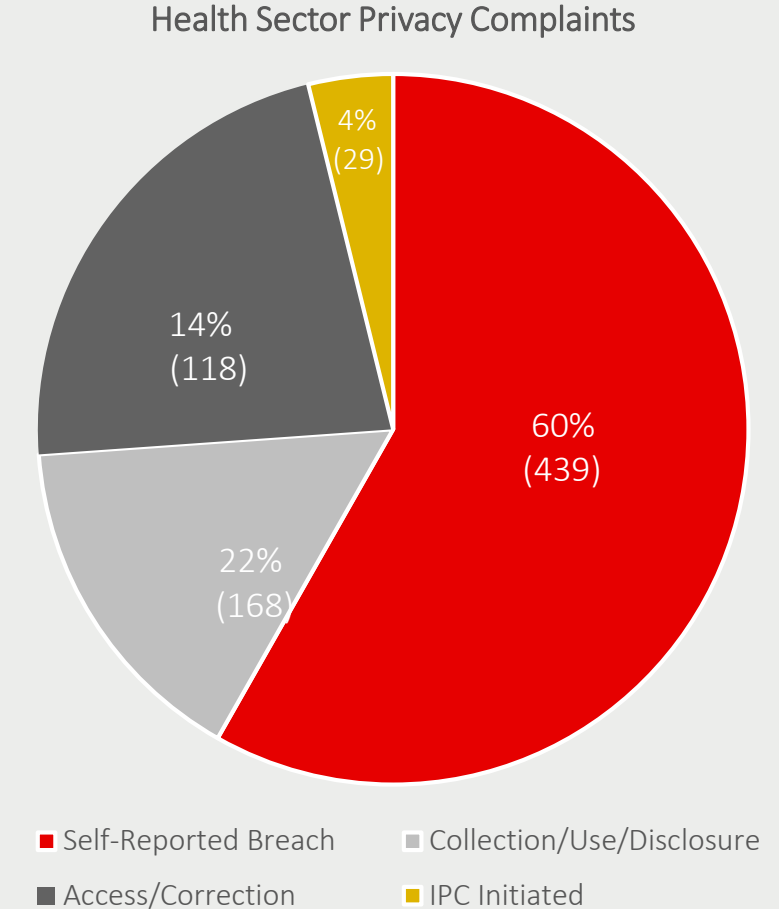
- The roles of the hospital, doctor and doctor's staff should be specified, in a written agreement, to clarify who is:
 - a custodian,
 - an agent of the hospital, and
 - an agent of the health professional
- The agreement should also clarify who is responsible for ensuring there is appropriate training, that confidentiality agreements are signed, that policies and procedures are followed, etc.

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

Health Sector Privacy Complaints 2018

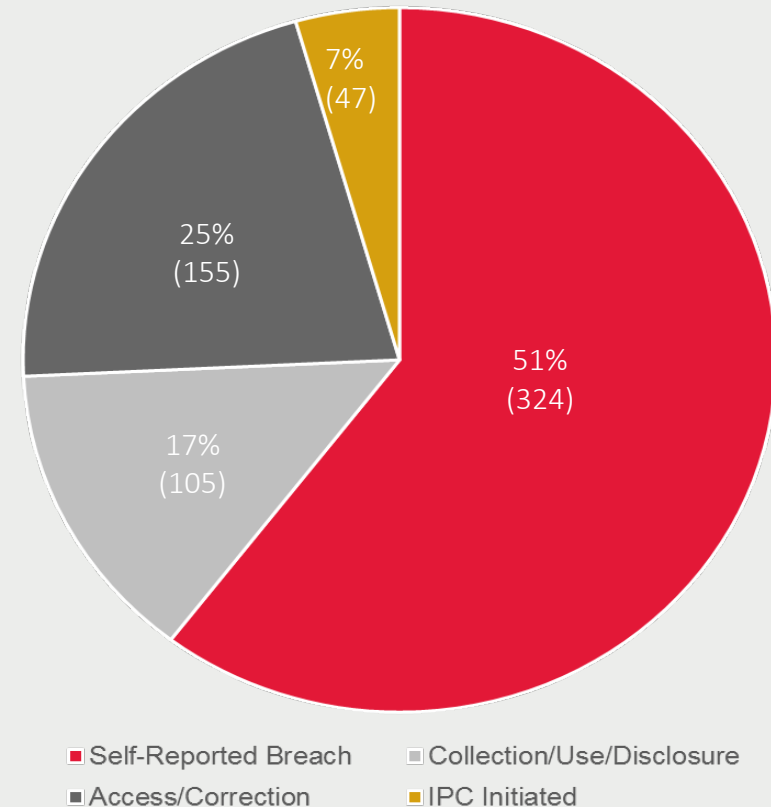
- Of the 439 self-reported breaches in 2018:
 - 108 were snooping incidents
 - 11 were ransomware/cyberattack
- Remaining 316 were related to:
 - lost or stolen PHI
 - misdirected information
 - records not properly secured
 - other collection, use and disclosure issues



Health Sector Privacy Complaints 2017

- Of the 324 self-reported breaches in 2017:
 - 60 were snooping incidents
 - 8 were ransomware/cyberattack
- Remaining 256 were related to:
 - lost or stolen PHI
 - misdirected information
 - records not properly secured
 - other collection, use and disclosure issues

Health Sector Privacy Complaints



Health Sector Privacy Complaints 2015/2016

2016

- There were 56 snooping incidents reported to the IPC by HICs, 36 of which were hospitals
- 16 snooping complaints were submitted to the IPC by individuals, 14 of which were against hospitals, (4 of these were submitted by both the HIC and individual)

2015

- There were 31 snooping incidents reported to the IPC by HICs, 19 of which were hospitals
- 18 snooping complaints were submitted to the IPC by individuals, 11 of which were against hospitals, (7 of these were submitted by both the HIC and individual)

Orders HO-002, HO-010 and HO-013

Our office has issued three orders involving unauthorized access:

- **Order HO-002**

- a registered nurse accessed records of the estranged spouse of her boyfriend to whom she was not providing care
- they were accessed over six-weeks during divorce proceedings

- **Order HO-010**

- a diagnostic imaging technologist accessed records of the current spouse of her former spouse to whom she was not providing care
- they were accessed on six occasions over nine months

- **Order HO-013**

- two employees accessed records to market and sell RESPs

**Snooping on
patients could
cost you:**



**IS SNOOPING
ON PATIENTS
WORTH IT?**

**Your
reputation**

**Your
career**

**College
disciplinary
action**

**\$50,000
in fines**

**A civil
lawsuit**

RESPECT
PATIENT PRIVACY
www.ipc.on.ca

To address the issue of unauthorized access, the IPC launched an educational campaign that asks the question, *“Is it worth it?”*

The materials feature stark messages about the possible consequences of getting caught snooping, including:

- damage to professional reputations
- termination by employers
- disciplinary action by regulatory colleges or professional associations
- fines and even civil lawsuits

Guidance Document: Detecting and Deterring Unauthorized Access

- impact of unauthorized access
- reducing the 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



How to Reduce the Risk...

- Clearly articulate the purposes for which employees, staff and other agents may access PHI
- Provide ongoing training and use multiple means of raising awareness such as:
 - confidentiality and end-user agreements
 - privacy notices and privacy warning flags
- Immediately terminate access pending an investigation
- Implement appropriate access controls and data minimization
- Log, audit and monitor access to PHI
- Impose appropriate discipline for unauthorized access

Amendments to PHIPA

- The *Health Information Protection Act* was introduced on September 16, 2015 to amend *PHIPA*
- All provisions except those relating to the provincial EHR have been proclaimed
- Amendments to:
 - clarify that merely viewing personal health information is a use
 - require privacy breaches, including unauthorized access, to be reported to our office and to relevant regulatory colleges, in some circumstances
 - remove the requirement that prosecutions be started within six months of when the offence occurred
 - double fines for offences from \$50,000 to \$100,000 for individuals and \$250,000 to \$500,000 for organizations

Offences

- It is an offence to wilfully collect, use or disclose PHI in contravention of *PHIPA*
- Consent of the Attorney General is required to commence a prosecution for offences under *PHIPA*
- On conviction, an individual may be liable to a fine of up to \$100,000 and a corporation of up to \$500,000

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

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
- Agreed 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) to facilitate 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 involving personal health information 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
- IPC not involved in the procurement process

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

Privacy Breach Reporting

- The more effective the auditing and monitoring, the more privacy breaches that will be detected
- Resources are required to address breaches
- 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

REACHING OUT
TO ONTARIO

Breach Reporting



Breach Reporting

- Section 6.3 of *Ontario Regulation 329/04* states a health information custodian must notify the IPC of a theft, loss or unauthorized use or disclosure in the following circumstances:
 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

Breach Notification to the IPC

- The IPC has published a guidance document providing more detail about when a breach must be reported

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

Use or Disclosure Without Authority

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.
 - Custodians must notify the IPC where there are reasonable grounds to believe the person committing the breach knew or ought to have known their use or disclosure was not permitted by the custodian or *PHIPA*
 - **Example:** A nurse looks at his or her neighbour's medical record for no work-related purpose.

Stolen Information

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

- Custodians must notify the IPC of the theft of paper or electronic records containing personal health information
- **Example:** Theft of a laptop computer containing identifying personal health information that was not encrypted or properly encrypted

Further Use or Disclosure Without Authority After Breach

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.

- Custodians must notify the IPC where there are reasonable grounds to believe that the personal health information subject to the breach was or will be further used or disclosed without authority (e.g. to market products or services, for fraud, to gain a competitive advantage in a proceeding, etc.)
- **Example:** A custodian inadvertently sends a fax containing patient information to the wrong recipient and although the recipient returned the fax, the custodian becomes aware that he or she kept a copy and is threatening to make it public

Pattern of Similar Breaches

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 pattern may indicate systemic issues that need to be addressed
- **Example:** A letter to a patient inadvertently included information of another patient. The same mistake re-occurs several times in the course of a couple months as a result of a new automated process for generating letters

Disciplinary Action Against a College Member

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

- The purpose of this section is to require the IPC to be notified of losses or unauthorized uses and disclosures in the same circumstances a custodian is required to notify a college under section 17.1 of *PHIPA*
- **Example:** A hospital suspends the privileges of a doctor for accessing the personal health information of his or her ex-spouse for no work-related purpose. The hospital must report this to the College of Physicians and Surgeons of Ontario and to the IPC.

Disciplinary Action Against a Non-College Member

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 *PHIPA* that relates to a loss or unauthorized use or disclosure of personal health information.

- Recognizes that not all agents of a custodian are members of a College
- The purpose of this section is to require custodians to notify the IPC of losses or unauthorized uses and disclosures in the same circumstances that a custodian is required to notify a college under section 17.1 of *PHIPA*
- **Example:** A hospital registration clerk posts information about a patient on social media and the hospital suspends the clerk. The clerk does not belong to a regulated health professional college.

Significant 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.

Significant Breach (Cont'd)

- To determine if a breach is significant, consider all relevant circumstances, including whether:
 - the information is sensitive;
 - the breach involves a large volume of information;
 - the breach involves many individuals' information;
 - more than one custodian or agent was responsible for the breach.
- **Example:** Disclosing mental health information of a patient to a large email distribution group rather than just to the patient's healthcare practitioner.

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 website for the Information and Privacy Commissioner of Ontario. The page is titled "Privacy Breach Report Form" and is part of a navigation menu that includes "Access", "Privacy", "Health", "Decisions", "Guidance", "Media Centre", and "About Us". The "Health" tab is selected. The page content includes a search bar, a breadcrumb trail (Home > Health > Report a Privacy Breach > Privacy Breach Report Form), and 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 an "Important Note" and a form with fields for "Date of this Report", "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
Commissaire 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.

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)

Address of Reporting Custodian:

Name of Individual Submitting Form on Behalf of Reporting Custodian:

Phone Number:

Fax Number:

Email Address: (required)

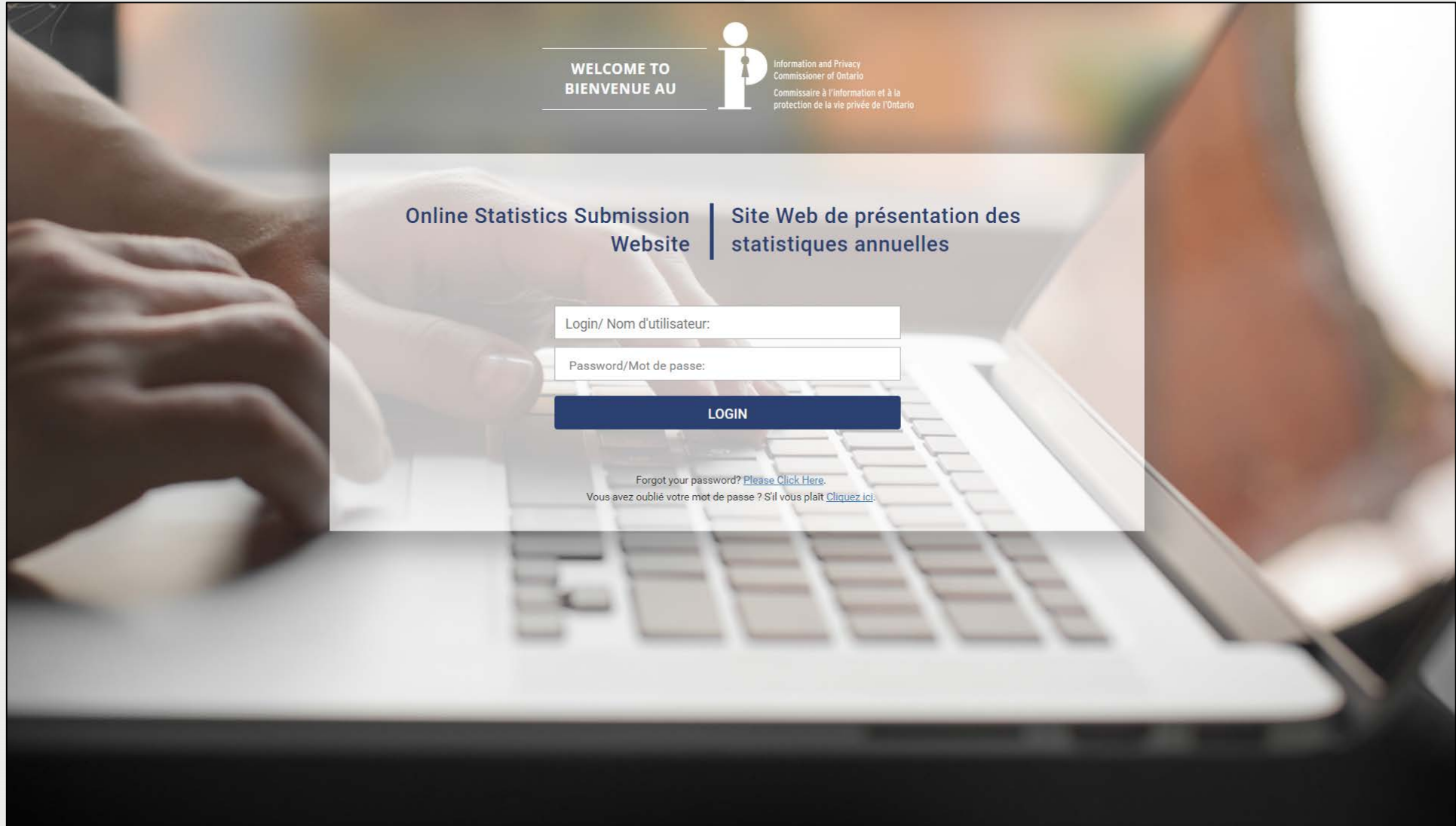
[PDF of Guidelines](#)

[Regulations](#)

You reported a breach to the IPC. What happens next?

- A notice will be sent that reflects the type of breach reported
- A response to the notice will be requested
- Additional information is required for “snooping” breaches
- Most breaches are resolved at the intake stage when the custodian demonstrates it has taken the steps necessary to notify affected parties, contain the breach and prevent future breaches.

REACHING OUT TO ONTARIO



Annual Reports to the Commissioner

- The IPC has released a guidance document about the statistical reporting requirement
- The guidance document outlines the specific information that must be reported for each category of breach

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.

REQUIREMENTS FOR
THE HEALTH SECTOR

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.

Annual Statistical Reports to the Commissioner

- Custodians will be required to:
 - start tracking privacy breach statistics as of January 1, 2018
 - provide the Commissioner with an annual report of the previous calendar year's statistics, starting in March 2019
- Annual report must also include breaches that do not meet the criteria for immediate mandatory reporting to the IPC

Annual Reports to the Commissioner

6.4 (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.

Stolen

- Total number of incidents where personal health information was stolen.
- Of the total in this category, the number of incidents where:
 - theft was by an internal party (such as an employee, affiliated health practitioner, or electronic service provider)
 - theft was by a stranger
 - theft was the result of a ransomware attack
 - theft was the result of another type of cyberattack
 - unencrypted portable electronic equipment (such as USB keys or laptops) was stolen
 - paper records were stolen

Lost

- Total number of incidents where personal health information was lost.
- Of the total in this category, the number of incidents where:
 - loss was a result of a ransomware attack
 - loss was the result of another type of cyberattack
 - unencrypted portable electronic equipment (such as USB key or laptop) was lost
 - paper records were lost

Used Without Authority

- Total number of incidents where personal health information was used (e.g., viewed, handled) without authority
- Of the total in this category, the number of incidents where
 - unauthorized use was through electronic systems
 - unauthorized use was through paper records

Disclosed without Authority

- Total number of incidents where personal health information was disclosed without authority
- Of the total in this category, the number of incidents where:
 - unauthorized disclosure was through misdirected faxes
 - unauthorized disclosure was through misdirected emails

In All Categories

- For each category of breach, the number of incidents where:
 - one individual was affected
 - 2 to 10 individuals were affected
 - 11 to 50 individuals were affected
 - 51 to 100 individuals were affected
 - over 100 individuals were affected

Additional Notes

- Count each breach only once. If one incident includes more than one category, choose the category that it best fits.
- Include all thefts, losses, unauthorized uses and disclosures in the year even if they were not required to be reported to the Commissioner at the time they occurred.
- It will be collected through the IPC's Online Statistics Submission Website
 - <https://statistics.ipc.on.ca/web/site/login>

REACHING OUT
TO ONTARIO

CONTACT US

Office of the 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

