REACHING OUT TO ONTARIO

Latest Developments in Protecting Personal Health Information

Suzanne Brocklehurst
Registrar

Debra Grant
Director of Health Policy

Sudbury

October 11, 2019

REACHING OUT TO ONTARIO

DEVELOPMENTS IN PROTECTING PERSONAL HEALTH INFORMATION

Debra Grant

Director of Health Policy

Connecting Care Act

- The *Connecting Care Act* was proclaimed into force on June 6, 2019
- It proposes to transform the health system through, among other things, the:
  - establishment of Ontario Health
  - creation of Ontario Health Teams
- The Minister may designate a person, entity or group as an Ontario Health Team
- Designation depends on whether they can deliver integrated and coordinated services in at least three areas identified in the Act (e.g. primary care services, mental health or addictions services, home care or community services)

Operation of Ontario Health Teams

- In the absence of amendments, Ontario Health Teams must comply with the current provisions of the *Personal Health Information Protection Act* (PHIPA)
- To assist in ensuring compliance, Ontario Health Teams should:
  - identify all of the participants in the Ontario Health Team
  - determine whether each participant is a health information custodian
  - identify the purpose(s) of each collection, use and disclosure of personal health information
  - determine whether there is authority for each collection, use and disclosure
  - if the authority is consent, determine the consent required (express/implied/assumed)
  - be transparent with clients about the information practices
  - develop a governance framework and harmonized policies and procedures
    - If all participants are health information custodians, are they acting as independent health information custodians or as a single health information custodian pursuant to an order of the Minister?

Collection, Use and Disclosure

- Not permitted to collect, use or disclose personal health information UNLESS:
  - the individual consents; or
  - the collection, use or disclosure is permitted or required without consent
- There are three types of consent under PHIPA:
  - express
  - implied
  - assumed implied

Transparency Regarding Information Practices

Ensure that you have public facing documents that:

- identify the Ontario Health Team (including all participating organizations)
- describe its governance structure
- describe the personal health information that will be collected
- identify the purpose(s) for which the information will be collected and used
- identify to whom and the purposes for which the information will be shared
- describe how individuals may refuse or withdraw consent
- describe how individuals may make requests for access or correction
- identify the person to contact if they have questions or concerns

UNAUTHORIZED ACCESS

Meaning of Unauthorized Access

- Unauthorized access is when you view, handle or otherwise deal with health information without consent and for purposes not permitted by PHIPA
- For example:
  - when you are not providing health care to the individual
  - when the individual has provided an express instruction
  - when it is not necessary for your employment, contractual or other responsibilities
- The act of viewing the personal health information on its own, without any further action, **is** an unauthorized access
- Unauthorized access is a serious matter, regardless of the motive

How to Address Challenges

- Implement policies that clearly set out the purposes for which access is and is not permitted
- Provide ongoing training and use multiple means of raising awareness such as:
  - confidentiality and end-user agreements
  - privacy notices and privacy warning flags
- Implement appropriate access controls and data minimization
- Log, audit and monitor access to health information
- Immediately terminate access pending an investigation
- Impose appropriate discipline for unauthorized access

Guidance Document

Reduce 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

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

Consequences of Unauthorized Access

- Duty to notify individuals
- Review or investigation by the Information and Privacy Commissioner (IPC)
- Prosecution
- Statutory or common law actions
- Discipline by employers
- Discipline by regulatory bodies

Duty to Notify

Notification of Individual

- A custodian must notify the individual at the first reasonable opportunity if personal health information is stolen, lost or used or disclosed without authority
- In the provincial electronic health record, the custodian must also notify the individual at the first reasonable opportunity if it is collected without authority

Notification of the IPC

- A custodian must also notify the IPC of a theft, loss or unauthorized collection, use or disclosure in the circumstances set out in section 6.3 of the Regulation to PHIPA

Reviews and Investigations by the IPC

- A final order of the IPC may be filed with the court and on filing, is enforceable as an order of the court
- The IPC has issued orders involving unauthorized access, including:
  - HO-002 A registered nurse accessed records of the estranged spouse of her boyfriend to whom she was not providing care over six-weeks during divorce proceedings
  - HO-010 A diagnostic imaging technologist accessed records of the current spouse of her former spouse to whom she was not providing care on six occasions over nine months
  - HO-013 Two employees accessed records to market and sell RESPs

Offences

- It is an offence to wilfully collect, use or disclose personal health information 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, five individuals have been successfully prosecuted:

- **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

*The fine in this case is the highest fine to date for a health privacy breach in Canada - the social worker was ordered to pay a $20,000 fine plus a $5,000 victim surcharge

Reaching out to Ontario

"The various victims have provided victim impact statements which are quite telling in terms of the sense of violation, the loss of trust, the loss of faith in their own health care community, and the utter disrespect [the accused] displayed towards these individuals."

"I have to take [the effect of deterrence on the accused] into consideration, but realistically, it's general deterrence, and that has to deal with every other heath care professional or someone who is governed by this piece of legislation. This is an important piece of legislation …"

- Justice of the Peace, Anna Hampson

Statutory or Common Law Actions

- A person affected by a final order of the IPC or by conduct that gave rise to a final conviction for an offence may start a proceeding for damages for actual harm suffered
- Where the harm was caused willfully or recklessly, the court may award an amount not exceeding $10 000 for mental anguish
- In 2012, the Ontario Court of Appeal recognized a common law cause of action in tort for invasion of privacy called “intrusion upon seclusion”

Discipline by Regulatory Colleges

- The Masters of Social Work student prosecuted was also disciplined by the Ontario College of Social Workers and Social Service Workers in June 2017
- The member admitted and the panel found that the student committed professional misconduct, including by undermining the "trust the public has in social workers and other health care providers"
- The member was reprimanded, her certificate of registration was suspended for six months and she was required to complete an ethics course
- The member was also ordered to pay costs of $5 000 to the College

Discipline by Regulatory Colleges

- A member of the College of Physicians and Surgeons accessed health records of a colleague through the hospital electronic records system without authorization
- The relationship between the member and the colleague was deteriorating and the member questioned the well being and mental health of the colleague
- The member admitted that he engaged in professional misconduct
- The member's certificate of registration was suspended for three months and he was required to complete an individualized instruction in medical ethics
- The member was also ordered to pay costs of $5 000 to the College

Discipline by Regulatory Colleges

- A member of the College of Nurses accessed health records of a patient through the hospital electronic records system without authorization
- The patient's admission and general diagnosis were widely publicized and a privacy notice popped up when the patient's name was clicked in the system
- The member admitted her actions and claimed that she was curious about the patient's age
- The member's certificate of registration was suspended for one month and a number of terms, conditions and limitations were placed on her certificate of registration, including to notify employers of this decision for a 12 month period

Innovative Procurement of Audit Solution

- The IPC agreed to participate in the steering committee to provide the perspective from a regulatory point of view on the procurement of an innovative auditing solution
- Mackenzie Health partnered with the Mackenzie Innovation Institute (Mi2) to facilitate an innovation-based procurement approach
- In collaboration with Mackenzie Innovation Institute (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

UPDATED *PHIPA* DOCUMENTS

New Documents/Web Content

Publications in 2018:

- Privacy Breach Protocol
- Health Cards & Health Numbers
- A Guide to Privacy and Access to Information in Ontario Schools
- Consent and Your Personal Health Information
- Your Health Privacy Rights in Ontario

In Progress

- 3 Year Review webpage
- Fax Guidelines
- PHIPA Brochure and Poster
- Disclosing PHI to Law Enforcement
- Guide to the Personal Health Information Protection Act

Publications in 2019

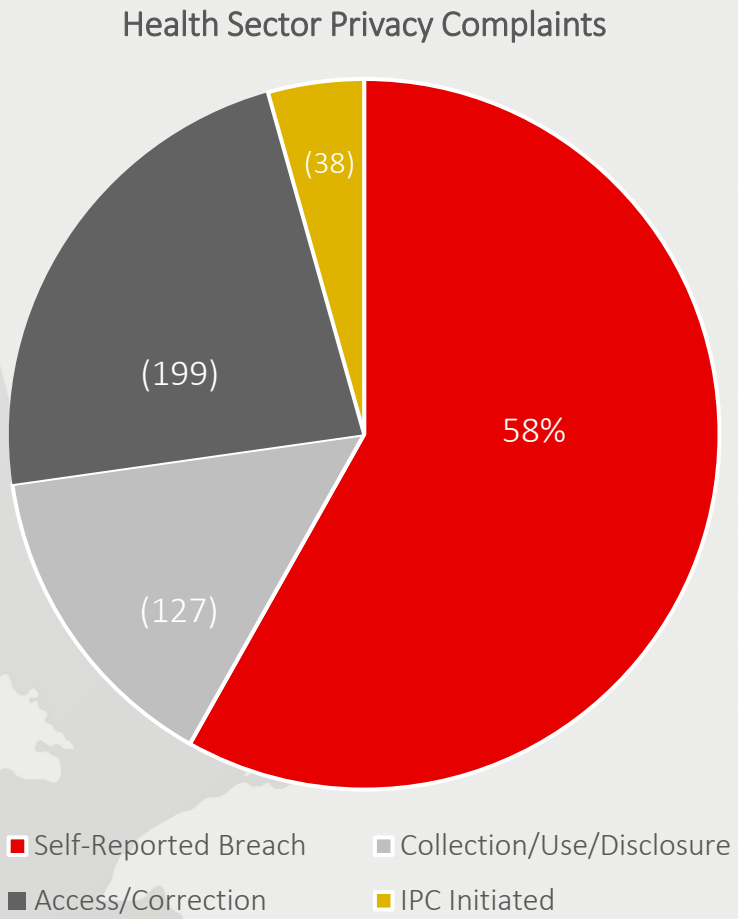
- Avoiding Abandoned Records (Feb 2019)
- Dispelling Some Myths About PHIPA (Feb 2019)
- Succession Planning to Prevent Abandoned Records (Apr 2019)
- Accessing Records of Deceased Relatives (May 2019)

BREACH REPORTING

Suzanne Brocklehurst
Registrar

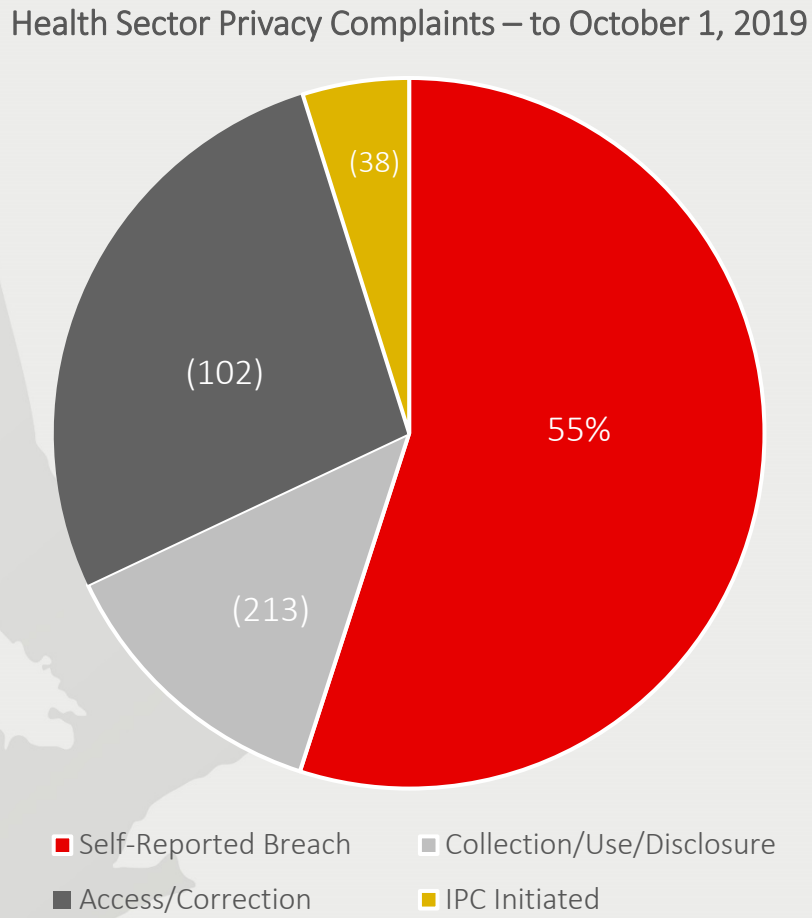
Health Sector Privacy Complaints 2018

- Of the 506 self-reported breaches in 2018:
  - 120 were snooping incidents
  - 15 were ransomware/cyberattack
- Remaining 371 were related to:
  - lost or stolen PHI
  - misdirected information
  - records not properly secured
  - other collection, use and disclosure issues

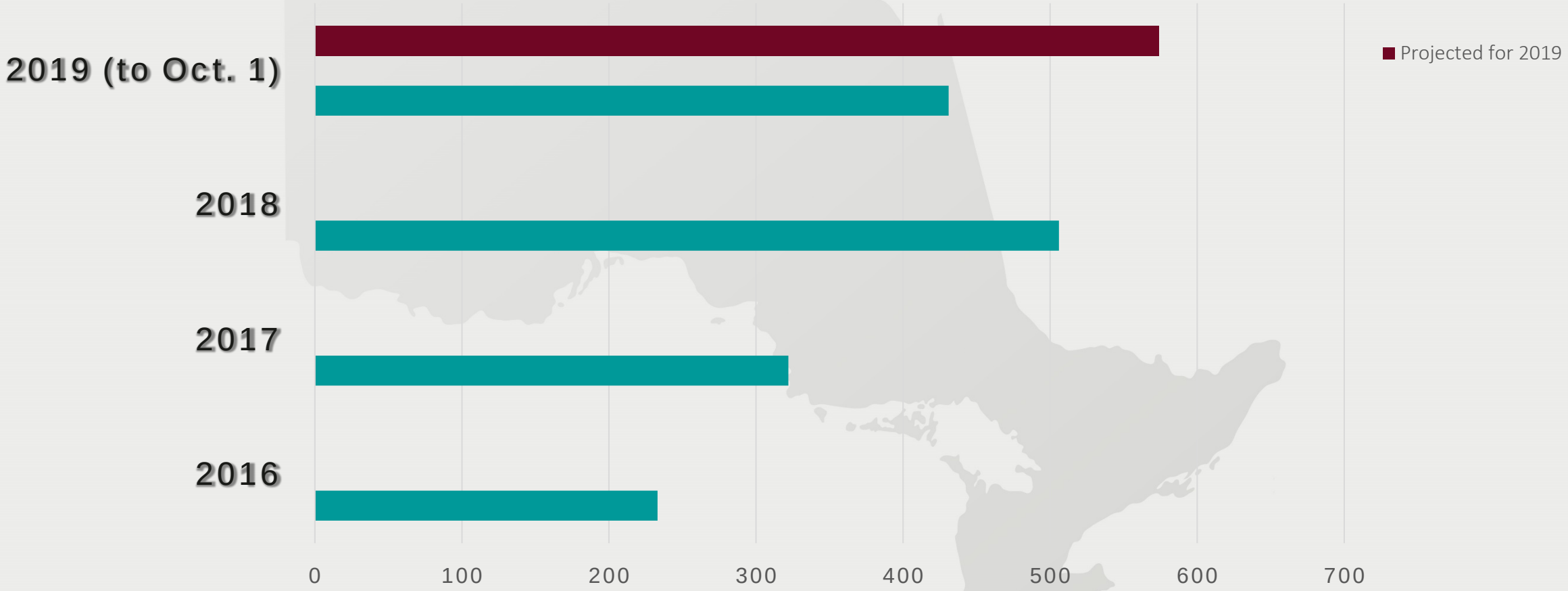


Health Sector Privacy Complaints 2019

- Of the 431 self-reported breaches so far in 2019:
  - 79 were snooping incidents
  - 17 were ransomware/cyberattack
- Remaining 335 were related to:
  - lost or stolen PHI
  - misdirected information
  - records not properly secured
  - other collection, use and disclosure issues



Self-Reported Breaches Before and After Mandatory 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

SEPTEMBER 2017

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

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

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)

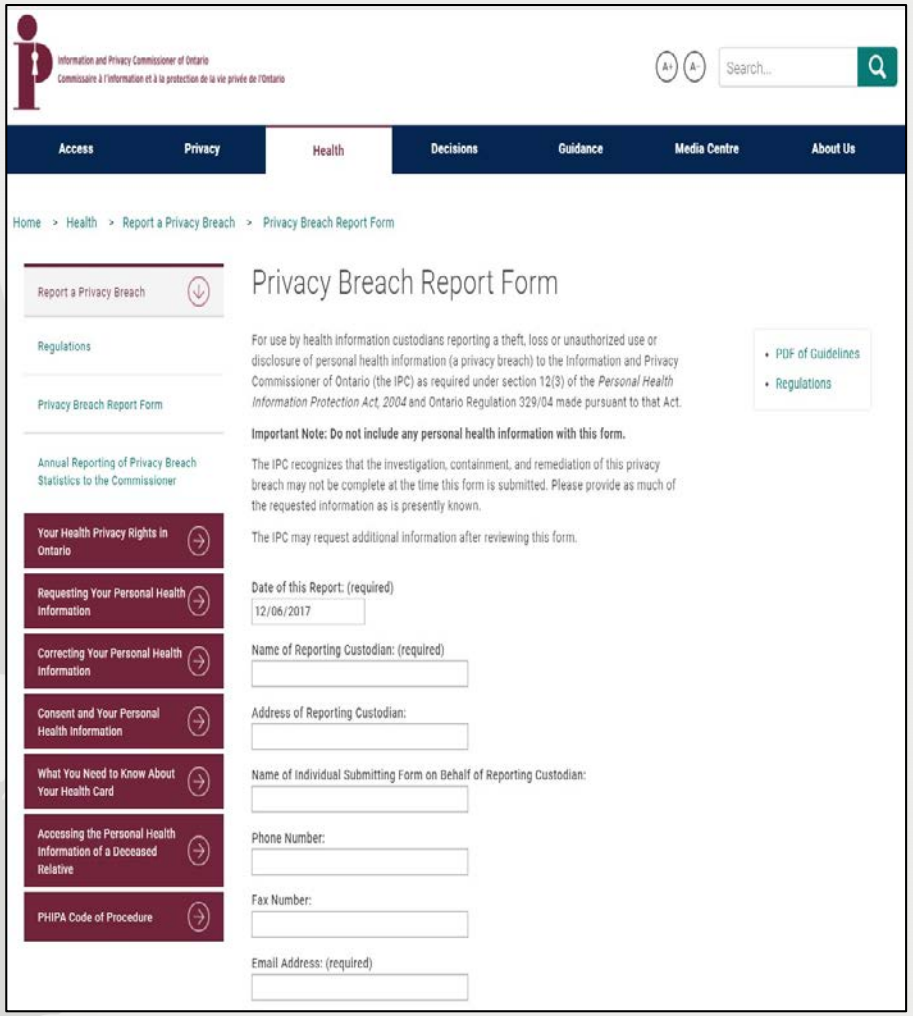
- To determine if a breach is significant, consider all relevant circumstances, including whether:
  - the information is sensitive;
  - the breach involves a large volume of information;
  - the breach involves many individuals' information;
  - more than one custodian or agent was responsible for the 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:

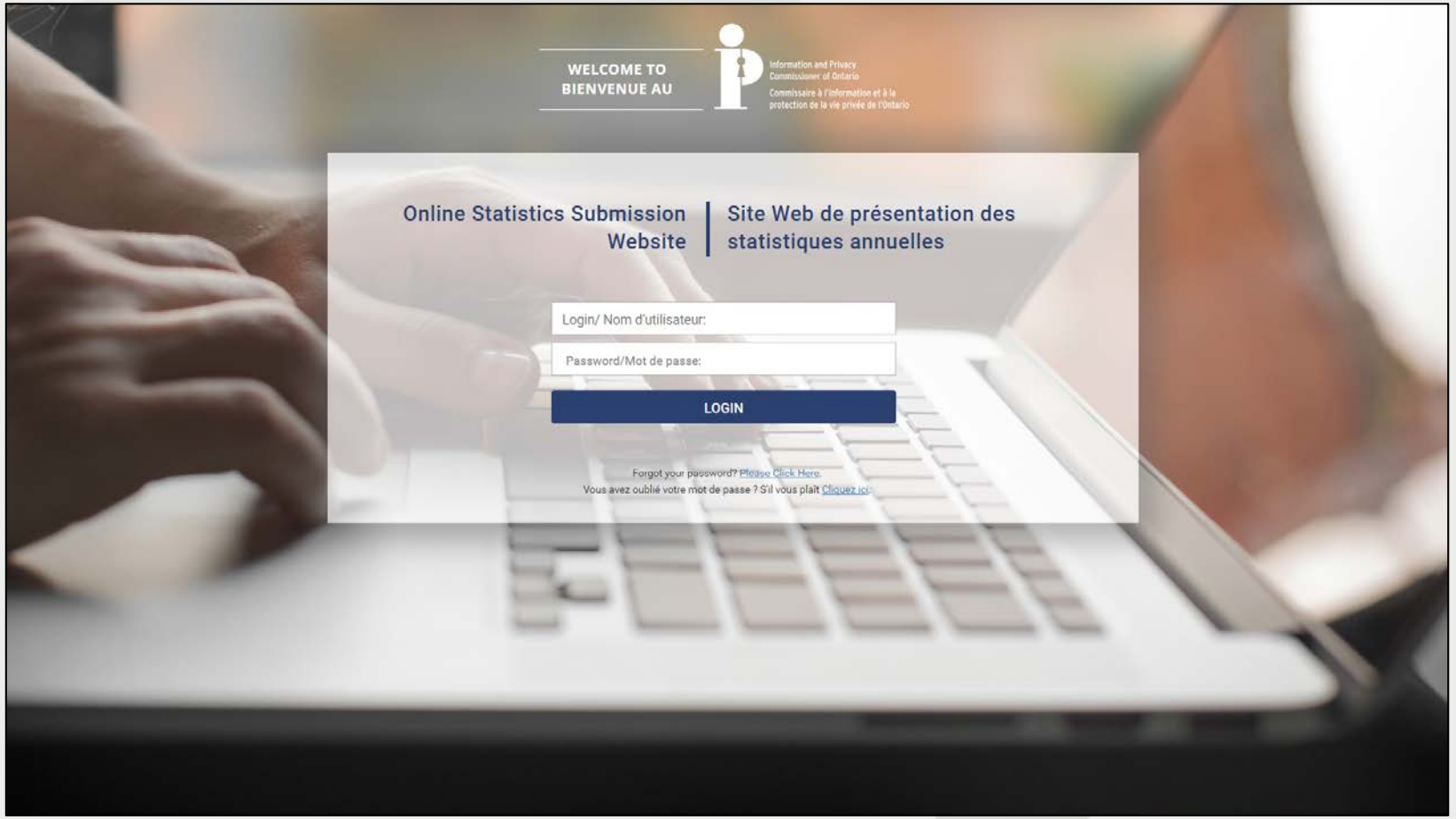
- a description of the breach
- steps taken to contain the breach
- steps taken to notify affected individuals
- steps taken to investigate and remediate the breach



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

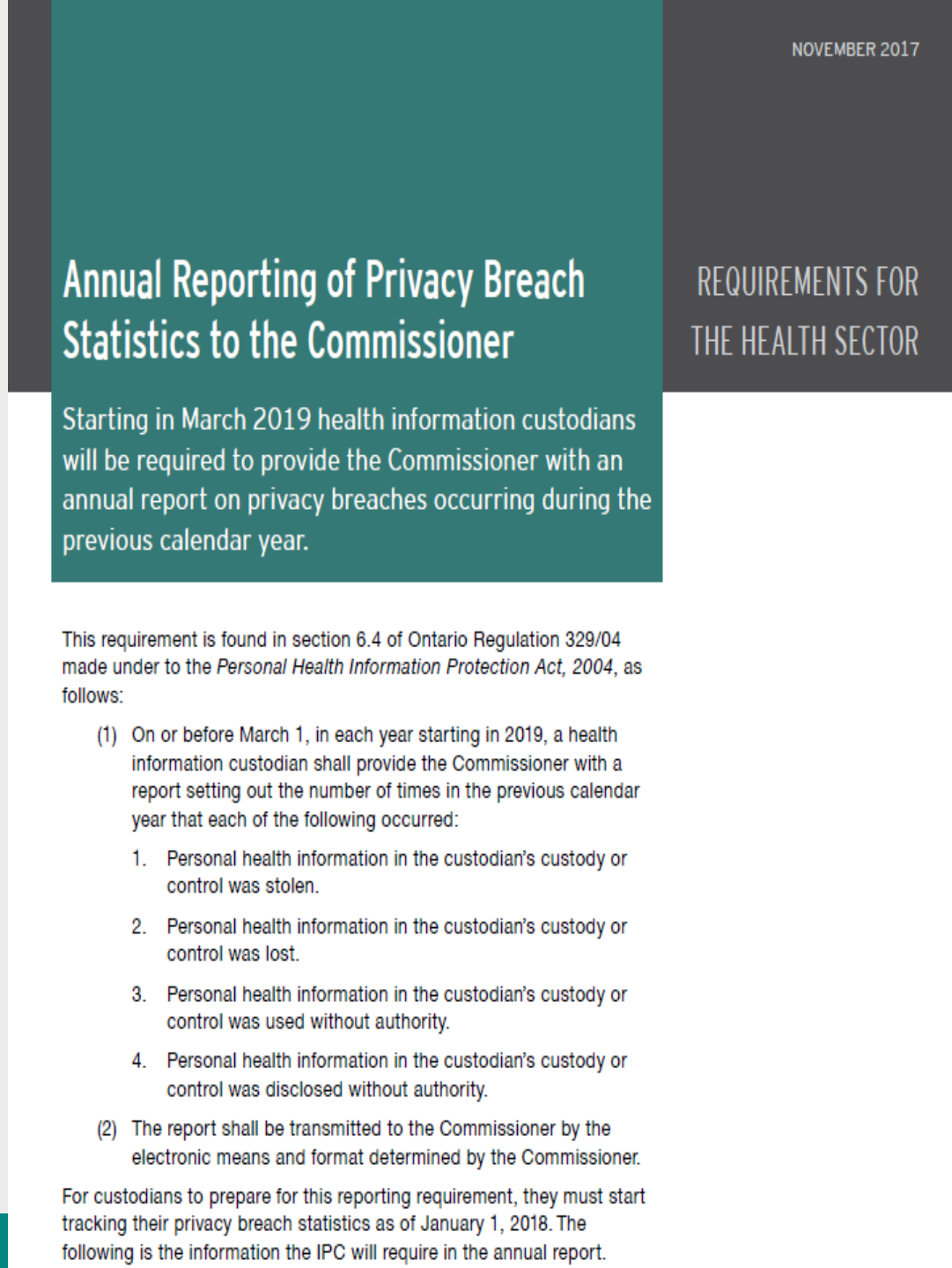
- A notice will be sent that reflects the type of breach reported
- A response to the notice will be requested
- Additional information is required for “snooping” breaches
- Most breaches are resolved at the intake stage when the custodian demonstrates it has taken the steps necessary to notify affected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



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.

Annual Statistical Reports to the Commissioner

- Custodians will be required to:
  - start tracking privacy breach statistics as of January 1, 2019
  - provide the Commissioner with an annual report of the previous calendar year's statistics, 2019 stats are due in March 2020
- annual report must also include breaches that do 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.

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

Annual Statistical Reporting for 2019

- Over 800 custodians submitted reports
- 11,278 individual privacy breaches reported
- Over 10,000 of the breaches reported were due to misdirected faxes, emails and other means

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