REACHING OUT TO ONTARIO

PROTECTING PERSONAL HEALTH INFORMATION

Suzanne Brocklehurst, Registrar

Manuela Di Re, Director of Legal Services and General Counsel

Waterloo

May 31, 2019

Topics

- Consent
- Unauthorized access
- Point-in-time breach reporting
- Annual breach reporting

Consent

General Consent Requirements

- Not permitted to collect, use or disclose personal health information UNLESS:
  - the individual consents and, to the best of your knowledge, it is for a lawful purpose; or
  - the collection, use or disclosure is permitted or required without consent by *PHIPA*
- Consent may be express or implied, except when *PHIPA* specifies that consent must be express
- Consent, whether express or implied, must satisfy the requirements of *PHIPA*

Types of Consent

- There are three types of consent under *PHIPA*:
  - express consent
  - implied consent
  - assumed implied consent
- Assumed implied consent provisions are sometimes referred to as the “circle of care” provisions

Express Consent

- Express consent is not a defined term in *PHIPA*
- Commonly understood as consent that has been clearly and unmistakably given orally or in writing
- In general, express consent is required to:
  - disclose personal health information to a non-custodian
  - disclose personal health information to another custodian for a purpose other than the provision of health care
  - collect, use or disclose personal health information for marketing
  - collect, use or disclose personal health information for fundraising (if it amounts to more than the name and address of the individual)

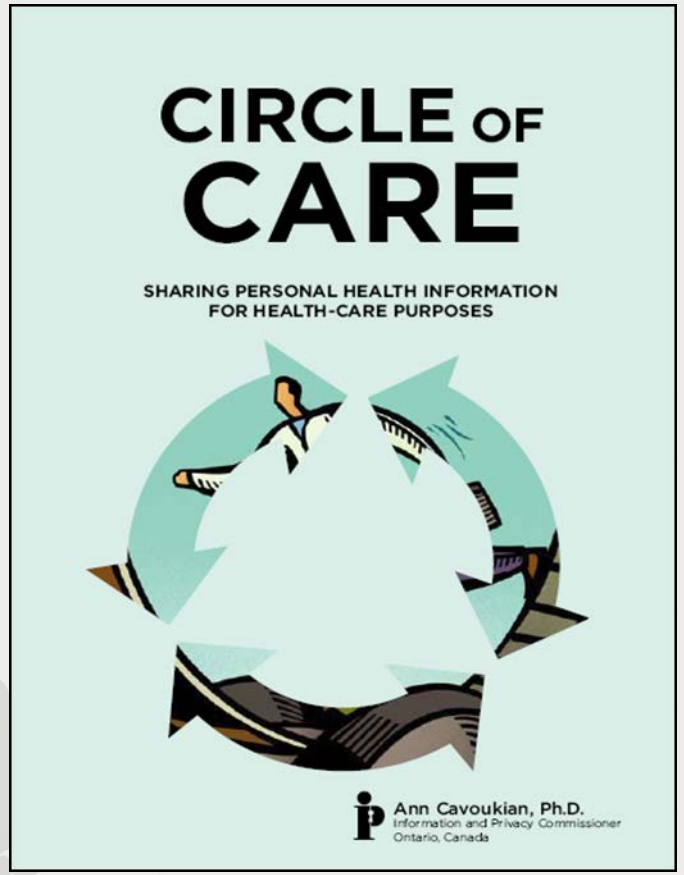
Implied Consent

- In all other circumstances, consent may be implied
- Implied consent is also not a defined term in *PHIPA*
- Commonly understood as a consent that one concludes has been given based on an individual's action or inaction in particular factual circumstances
- For example, consent may be implied:
  - to *collect* or *use* personal health information for any purpose, subject to certain exceptions
  - to *disclose* personal health information to another custodian for the provision of health care

Assumed Implied Consent

Custodians *may* assume implied consent to collect, use or disclose personal health information provided all six conditions are satisfied:

1. The custodian falls within a category of custodians that are entitled to rely on assumed implied consent
2. The personal health information must have been received from the individual, his or her substitute decision-maker or another custodian
3. The personal health information must have been received for providing or assisting in providing health care to the individual
4. The purpose of the collection, use or disclosure must be for providing or assisting in providing health care to the individual
5. In the context of a disclosure, the disclosure must be to another custodian
6. The custodian must not be aware the individual expressly withheld or withdrew consent



Elements for Valid Consent

Consent, whether express or implied, must:

1. Be the consent of the individual or their substitute decision-maker (if applicable)
2. Be knowledgeable, meaning, it must be reasonable to believe that the individual knows:
   - the purpose of the collection, use or disclosure; and
   - that the individual may give or withhold consent
3. Relate to the information
4. Not be obtained by deception or coercion

Consent and Capable Individuals

- Where an individual is capable, consent may be provided by:
  - the individual, or
  - if the individual is sixteen or older, any capable person sixteen years of age or older authorized in writing by the individual to provide consent on his or her behalf
- An individual is capable if he or she is able to:
  - understand information relevant to deciding whether to consent; and
  - appreciate the reasonably foreseeable consequences of giving, not giving, withholding or withdrawing consent
- Individuals are presumed capable regardless of age unless there are reasonable grounds to believe otherwise

Consent and Incapable Individuals

Where an individual is incapable, the following (in order of priority) may consent:

- A substitute decision-maker under the *Health Care Consent Act* with respect to consent necessary for or ancillary to a decision about treatment, long-term care admission or a personal assistance service
- Guardian of the person or guardian of property (with authority)
- Attorney for personal care or attorney for property (with authority)
- Representative appointed by the Consent and Capacity Board
- Spouse or partner
- Child or custodial parent (subject to exceptions)
- Parent with only a right of access
- Brother or sister
- Any other relative
- Public Guardian and Trustee (as a last resort)

Consent and Deceased Individuals

Where an individual is deceased, consent may be provided by:

- the estate trustee; or
- if there is no estate trustee, the person responsible for administering the estate

Consent and Children

1. If a child is capable, the child may consent
2. If a child is capable and 16 or older the child may authorize another capable person who is at least 16 years old to provide consent on his or her behalf provided it is in writing
3. If a child is capable and less than 16, a custodial parent, Children's Aid Society or person lawfully entitled to stand in the place of a parent may consent EXCEPT :
   - if the information relates to treatment about which the child made a decision on their own under the *Health Care Consent Act, 1996*
   - if the information relates to counselling in which the child participated on their own under the *Child and Family Services Act*

   In event of conflict, the decision of the capable child prevails
4. If a child is incapable, the same persons who may consent for an incapable individual can consent for an incapable child

Unauthorized Access

Meaning of Unauthorized Access

- Unauthorized access is when you view, handle or otherwise deal with personal 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

Education and Quality Improvement

- There are a number of provisions in *PHIPA* that permit you to use personal health information without consent, including:
  - for risk and error management
  - to improve or maintain the quality of care and related programs or services
  - for educating agents to provide health care
- There have been a number of instances where custodians or agents have accessed personal health information claiming it was for one of these purposes

Challenges in Establishing "Unauthorized" Access

- Demonstrating such accesses are unauthorized may be difficult where the custodian does not:
  - have policies that set out the purposes for which access is permitted and not permitted in relation to risk management, quality improvement and education
  - have procedures that must be followed when accessing personal health information for these purposes
  - inform agents when access is permitted and is not permitted, through training, notices, flags in electronic systems, agreements, etc.

How to Address Challenges

- Clearly articulate the purposes for which agents may access personal health information
- Implement a policy that sets out whether and in what circumstances an agent is permitted to access information for risk and error management, quality improvement and education
- The policy should require:
  - agents to obtain written authorization prior to accessing information for these purposes
  - that the written authorization set out, at a minimum:
    - ✓ the specific circumstances and particular risk or error management activity(ies), quality improvement activity(ies) and educational purpose(s) for which the personal health information may be accessed
    - ✓ any conditions, restrictions, and limitations imposed on the access

How to Address Challenges

- 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
- Impose appropriate discipline for unauthorized access
- Implement appropriate access controls and data minimization
- Log, audit and monitor access to personal health information

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

Consequences of Unauthorized Access

- Duty to notify
- Review or investigation by the IPC
- Prosecution for offences
- 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

- The member accessed the 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

- The member accessed the 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

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

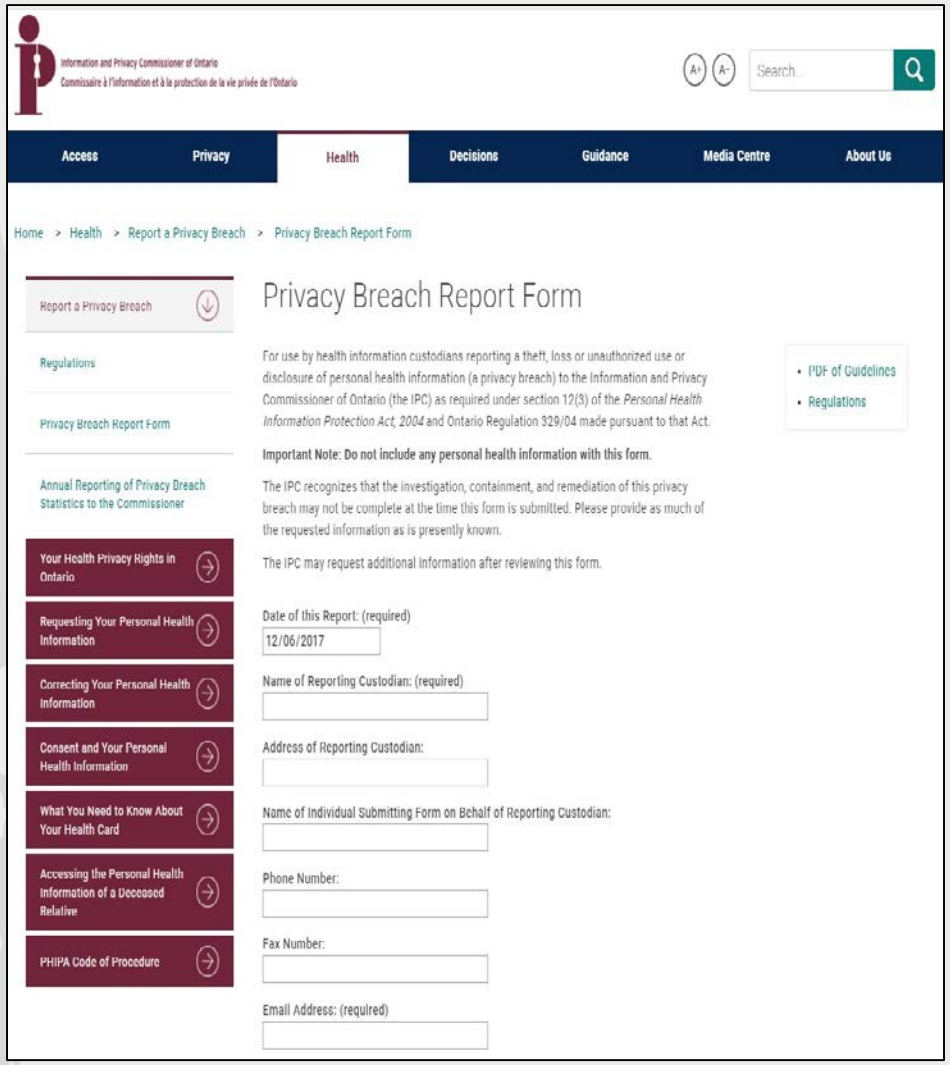
Significant Breach (Cont'd)

- 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:

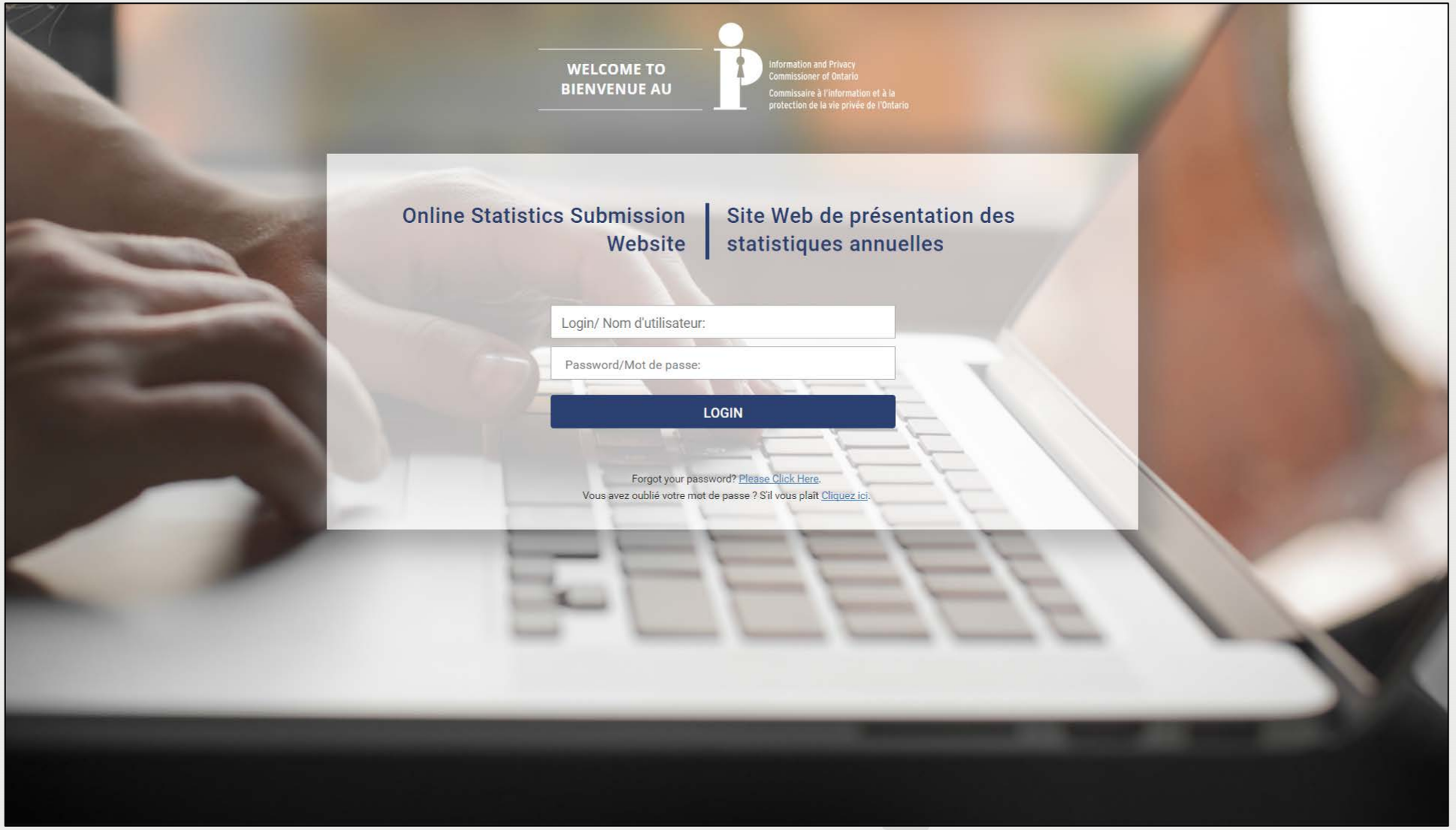
- a description of the breach
- steps taken to contain the breach
- steps taken to notify affected individuals
- steps taken to investigate and remediate the breach



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

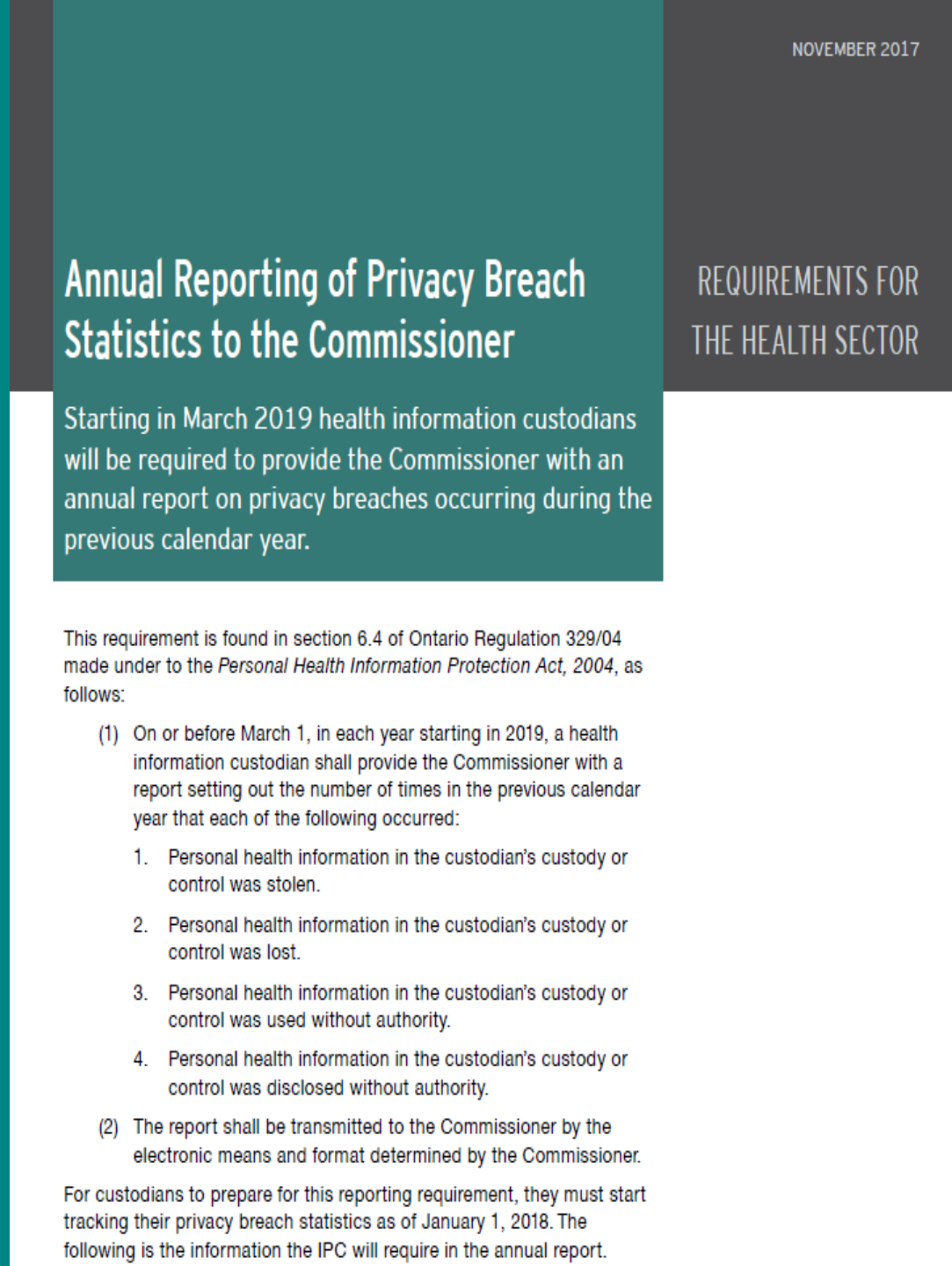
- A notice will be sent that reflects the type of breach reported
- A response to the notice will be requested
- Additional information is required for “snooping” breaches
- Most breaches are resolved at the intake stage when the custodian demonstrates it has taken the steps necessary to notify affected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

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