PHIPA Overview

Dara Lambie

Legal Counsel

Information and Privacy Commissioner of Ontario

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

Canadian Association of Aesthetic Medicine

October 26, 2019

Privacy Law In Ontario and Canada

Federal Public Sector	Ontario Public Sector	Ontario Health Sector	Private Sector
Government of Canada e.g. federal ministries, agencies, crown corporations *Privacy Act*	Government of Ontario e.g. provincial ministries, agencies, hospitals, universities, cities, police, schools, *Freedom of Information and Protection of Privacy Act* (*FIPPA*) *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)	Health care individuals, organizations ("health information custodians") e.g. hospitals, clinics, pharmacies, labs, doctors, dentists, nurses *Personal Health Information Protection Act* (*PHIPA*)	Private sector businesses *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)
Privacy Commissioner of Canada oversight	Information and Privacy Commissioner of Ontario oversight	Information and Privacy Commissioner of Ontario oversight	Privacy Commissioner of Canada oversight

Information and Privacy Commissioner of Ontario

- **Brian Beamish** appointed by Ontario Legislature (March 2015)
- 5 year term
- The Commissioner is an officer of the Legislature who is appointed by and reports to the Legislative Assembly of Ontario, and is independent of the government of the day

Information and Privacy Commissioner of Ontario

- The IPC's mandate:
  - Investigate privacy complaints related to personal information
  - Resolve appeals when there is a refusal to grant access to information
  - Ensure compliance with the acts
  - Review privacy policies and information practices
  - Conduct research on access and privacy issues and provide comment on proposed government legislation and programs
  - Reach out and educate the public, media and other stakeholders about Ontario's access and privacy laws and current issues affecting access and privacy

https://www.ipc.on.ca/about-us/role-and-mandate/

Topics

- Overview of *Personal Health Information Protection Act (PHIPA)*
- Breach Reporting
- Electronic Health Record

Overview of *Personal Health Information Protection Act* (PHIPA)

Application of PHIPA

- The majority of PHIPA governs “personal health information” in the custody or control of:
  - “Health Information Custodians,” or
  - “Agents” of health information custodians
- However, PHIPA also has broader application, for example:
  - It restricts the use and disclosure of personal health information by non-health information custodians that receive personal health information from health information custodians
  - It regulates people and organizations that provide electronic services to health information custodians but are not agents

Definition of Personal Health Information

- "Personal health information" is identifying information about an individual in oral or recorded form that:
  - Relates to an individual's physical or mental health, including information that consists of the health history of the individual's family
  - Relates to the provision of health care to the individual, including the identification of a person as a provider of health care to the individual
  - Identifies an individual's substitute decision-maker
  - Relates to payments or eligibility for health care
  - Is the individual's health number
  - Is a plan of service under the *Home Care and Community Services Act, 1994* for the individual
  - Relates to the donation of body parts or bodily substances

Identifying Information

- Information is “identifying” when it identifies an individual or when it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual
- It is not necessary for the individual to be actually named for the information to be considered personal health information
  - See, for example, PHIPA Decision 82 and PHIPA Decision 80

Mixed Records

- “Personal health information” includes information that is not health related (e.g. a patient address) where it is found in a record that contains other information contained within the definition of “personal health information”
- This is referred to as the “mixed record” rule

Definition of Health Information Custodian

- Health information custodians include:
  - A health care practitioner who provides health care
  - A person who operates a group practice of health care practitioners who provide health care
  - A service provider under the *Home Care and Community Services Act*
  - A community care access corporation
  - A hospital, psychiatric facility and independent health facility
  - A long-term care home, care home, home for special care, or retirement home
  - A pharmacy, ambulance service, laboratory or specimen collection centre
  - A centre, program or service for community health or mental health whose primary purpose is the provision of health care
  - A medical officer of health of a board of health

Definition of Agent

- An agent is a person that, with the authorization of a health information custodian, acts for or on behalf of the custodian in respect of personal health information
- Includes:
  - Employees
  - Volunteers
  - Persons with privileges (e.g. a doctor with privileges in a hospital)
- A health information custodian remains responsible for personal health information collected, used, disclosed, retained or disposed of by an agent

Duties Of Health Information Custodians and Agents

- A number of duties are imposed on health information custodians and their agents under PHIPA
- These duties generally fall into four categories:
  - Collection, use and disclosure of personal health information
  - Security of personal health information
  - Transparency of information practices
  - Responding to requests for access to and correction of records of personal health information

Collection, Use and Disclosure

- Health information custodians may not:
  - Collect, use or disclose personal health information UNLESS:
    - the individual consents, or
    - the collection, use or disclosure is permitted or required by PHIPA to be made without consent
  - Collect, use or disclose personal health information if other information will serve the purpose
  - Collect, use or disclose more personal health information than is reasonably necessary

Types of Consent

- Consent must be express in certain circumstances
- In other circumstances, consent may be implied
- In some circumstances, a health information custodian may assume that they have the individual's implied consent
  - "assumed implied consent"

Express Consent

- Express consent is not a defined term in PHIPA
- It is 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-health information custodian
  - Disclose personal health information to another health information custodian for a purpose other than the provision of health care, including:
    - collecting, using or disclosing personal health information for marketing
    - collecting, using or disclosing personal health information for fundraising (subject to limited exceptions)

Implied Consent

- Implied consent is not a defined term in the *Act*
- Commonly understood as a consent that one concludes has been given based on an individual's action or inaction in particular factual circumstances

Assumed Implied Consent

- Section 20(2) of the PHIPA provides:

  (2) A health information custodian described in paragraph 1, 2, 3 or 4 of the definition of "health information custodian" in subsection 3 (1), that receives personal health information about an individual from the individual, the individual's substitute decision-maker or another health information custodian for the purpose of providing health care or assisting in the provision of health care to the individual, is entitled to assume that it has the individual's implied consent to collect, use or disclose the information for the purposes of providing health care or assisting in providing health care to the individual, unless the custodian that receives the information is aware that the individual has expressly withheld or withdrawn the consent.

- In the context of a disclosure, the disclosure must be made to another health information custodian
- Sometimes referred to as "Circle of Care"

Elements for Valid Consent

- Consent, whether express or implied, must:

1. Be the consent of the individual (or his or her substitute decision-maker where applicable)

2. Be knowledgeable, meaning, it must be reasonable to believe that the individual knows:
   - The purpose of the collection, use or disclosure
   - That the individual may give or withhold consent

3. Relate to the information

4. Not be obtained by deception or coercion

Withholding and Withdrawing Consent and Express Instructions

- PHIPA gives individuals the right, subject to certain exceptions, to expressly:
  - Withhold or withdraw consent to the collection, use or disclosure of personal health information, including for the purpose of providing health care
  - Instruct that their personal health information not be used or disclosed without consent for health care purposes in specific circumstances
- These are referred to as the “lock-box” provisions, although lock-box is not a term found in PHIPA

Withholding and Withdrawing Consent or Express Instructions

Cont'd

- A custodian must comply with the decision to withhold or withdraw consent or to provide an express instruction unless:
  - The individual changes his or her mind
  - PHIPA permits the collection, use or disclosure to be made without consent
- Where a custodian is prevented from disclosing personal health information to other custodians that is believed to be reasonably necessary for the provision of health care:
  - The disclosing health information custodian **must** notify the other health information custodian of that fact
  - The receiving health information custodian may explore the matter with the individual and seek consent to access the withheld information

Uses and Disclosures Without Consent

- Uses of personal health information permitted without consent are set out in section 37 of PHIPA
- Disclosures permitted without consent are set out in sections 38 – 48 and section 50 of PHIPA

Uses

- Examples
  - Planning or delivering programs or services that the custodian provides or funds or for allocating resources to, evaluating, or monitoring the programs or services
  - Risk management, error management and quality control
  - Educating agents to provide health care
  - Obtaining payment or processing, monitoring, verifying or reimbursing claims for payment for the provision of health care
  - A proceeding or contemplated proceeding in which the custodian or their agent is expected to be a party or witness
  - Research in compliance with PHIPA

Disclosures

- Examples
  - Contacting a relative, friend or substitute decision-maker if the individual is injured, incapacitated or ill and unable to give consent
  - Determining or verifying the eligibility of an individual to receive publicly funded health care
  - A proceeding or contemplated proceeding in which the custodian or their agent is expected to be a party or witness
  - Complying with
    - a summons, order or similar requirement issued in a proceeding
    - a procedural rule that relates to the production of information in a proceeding
  - Complying with a warrant
  - As required by a law of Ontario or Canada

Cont'd

Disclosures

- Examples
  - To public health authorities for a purpose in the *Health Protection and Promotion Act*
  - Eliminating or reducing a significant risk of serious bodily harm
  - Research
    - Must comply with section 44 of PHIPA which requires the researcher to
      - make an application to and get the approval of a research ethics board
      - produce a research plan
      - enter into an agreement with the custodian disclosing the personal health information

Capacity and Substitute Decision-Makers

- An individual is capable of consenting to the collection, use or disclosure of personal health information if the individual is able to:
  - Understand the relevant information; and
  - Appreciate the consequences of giving or withholding consent
- A custodian may presume the individual is capable, unless there are reasonable grounds to believe that the individual is incapable
- If the individual is determined to be incapable of consenting to the collection, use or disclosure of personal health information, PHIPA sets out who may act on their behalf as their substitute decision-maker

Practices to Protect Personal Health Information—Accuracy

- Health information custodians must take reasonable steps to ensure that personal health information is as accurate, complete and up-to-date as is necessary for the purposes for which the custodian uses the information

Practices to Protect Personal Health Information—Security

- Health information custodians must take steps that are reasonable in the circumstances to ensure that:
  - Personal health information in their custody or control is protected against theft, loss and unauthorized use or disclosure
  - records containing personal health information are protected against unauthorized copying, modification or disposal
- Health information custodians must ensure that records of personal health information are retained, transferred and disposed of in a secure manner

Agents and Service Providers to Custodians

- Health information custodians may engage agents to collect, use, disclose, retain or dispose of personal health information on the custodian's behalf
- Health information custodians remain responsible for the personal health information while it is being processed or accessed by an agent on their behalf
- The regulations to PHIPA set out the requirements that people or organizations that act as electronic service providers to custodians must meet

Accountability and Transparency

- Health information custodians must designate a contact person who is authorized to:
  - Help the custodian to comply with PHIPA
  - Ensure that all agents are informed of their duties under PHIPA
  - Respond to inquiries about the custodian's information practices
  - Respond to requests for access or correction of records
  - Receive complaints about contraventions of the PHIPA

Cont'd

Accountability And Transparency

- A health information custodian must have a written public statement that describes:
  - The custodian's information practices
  - How to reach the contact person or the custodian, if the custodian does not have a contact person
  - How an individual may obtain access to or request correction of a record
  - ow to make a complaint to the custodian and the Commissioner

Access

- Subject to some exceptions, health information custodians must provide individuals with access to records containing their own personal health information upon request
- The custodian has 30 days to respond to a request for access
- A 30-day time extension is allowed if meeting the 30-day time limit would unreasonably interfere with the operations of the custodian or if more than 30 days is required to undertake consultations necessary to respond to the request
- A person who is not satisfied with the response received to an access request may make a complaint to the IPC

Cont'd

Access

- The right of access does not apply to:
  - Quality of care information
  - Personal health information collected or created for a quality assurance program under the Health Professions Procedural Code
  - Raw data from standardized psychological tests or assessments
- Custodians do not have to provide access if:
  - The information is subject to legal privilege that restricts disclosure
  - Another provincial or federal act or a court order prohibits disclosure
  - The information was collected or created for a proceeding
  - The information was collected or created during an inspection, investigation etc.
  - Access could result in serious harm to any person or the identification of a person who provided the information
  - The custodian is a government institution that could refuse access under the access and privacy legislation that applies to government organizations

Correction

- If an individual believes that a record of personal health information is not as accurate or complete as necessary for its purpose, the individual may make a written request to the custodian to correct the record
- The custodian has 30 days to respond to the request
- A 30- day extension is permitted if responding to the request within 30 days would unreasonably interfere with the activities of the custodian or more than 30 days is needed to undertake consultations to respond to the request
- The custodian is not required to correct a record if the custodian did not create the record or the record consists of a professional opinion made in good faith

Correction

Cont'd

- Corrections can be made by striking out incorrect information in a way that does not obliterate the information or by labelling the information as incorrect, severing it from the record, and storing in separately but linked to the record
  - If it is not possible to record the correct information in the record, the custodian must ensure that there is a system in place to inform anyone who accesses the record that the information is not correct and to direct the person to the correct information
- If the custodian refuses the correction request, the individual may prepare a statement of disagreement and require the custodian to attach it to the record
- A person who is not satisfied with the response received to a correction request may make a complaint to the IPC

Data Breach Notification And Reporting

Breach Notification And Reporting

- Notification of Individual:
  - A health information custodian must notify an affected individual at the first reasonable opportunity if personal health information is stolen, lost or used or disclosed without authority
- Reporting to Commissioner:
  - A custodian must notify the IPC if the circumstances surrounding the theft, loss or unauthorized use or disclosure meet thresholds prescribed by regulation
  - A custodian must:
    - start tracking privacy breach statistics as of January 1, 2018
    - provide the IPC with an annual report of the previous calendar year's statistics, starting in March 2019

Point-In-Time Breach Reporting

- Section 6.3 of *Ontario Regulation* 329/04 under *PHIPA* prescribes when a Custodian must notify the IPC of a theft, loss or unauthorized use or disclosure of personal health information:
    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 Commissioner

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

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

6.3 (1) The following are the circumstances in which a health information custodian is required to notify the Commissioner for the purposes of subsection 12 (3) of the Act:

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

- Example: A nurse looks at his or her neighbor's medical record for no work related purpose—the "snooping" case

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

- Example: Someone has stolen paper records, a laptop or other electronic storage device containing personal health information.
- Example: Personal health information is subject to a ransomware or other malware attack, or the information has been seized through use of a portable storage device.

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

- Example: A custodian inadvertently sends a fax containing patient information to the wrong person. Although the recipient returned the fax to the custodian, the HIC becomes aware that he or she kept a copy and is threatening to make the information 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

- Example: A letter to a patient inadvertently included information relating to a different patient. The same mistake re-occurs several times because an automated process for generating letters has been malfunctioning for some time

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

- Where a custodian is required by section 17.1 of PHIPA to report an employee or a person with privileges (e.g. a doctor who has privileges in a hospital) to that person's regulatory college, the custodian must report to the IPC
- Example: A doctor who has privileges at a hospital accesses PHI about his or her ex-spouse for a reason other than providing health care. The hospital suspends the doctor's privileges. The hospital must report this to the College of Physicians and Surgeons of Ontario and to the Commissioner

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

- If an agent or employee of a HIC is not a member of a regulated health professional college, the HIC must still notify the Commissioner in the same circumstances that would have triggered notification to a college, had the agent been a member
- 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

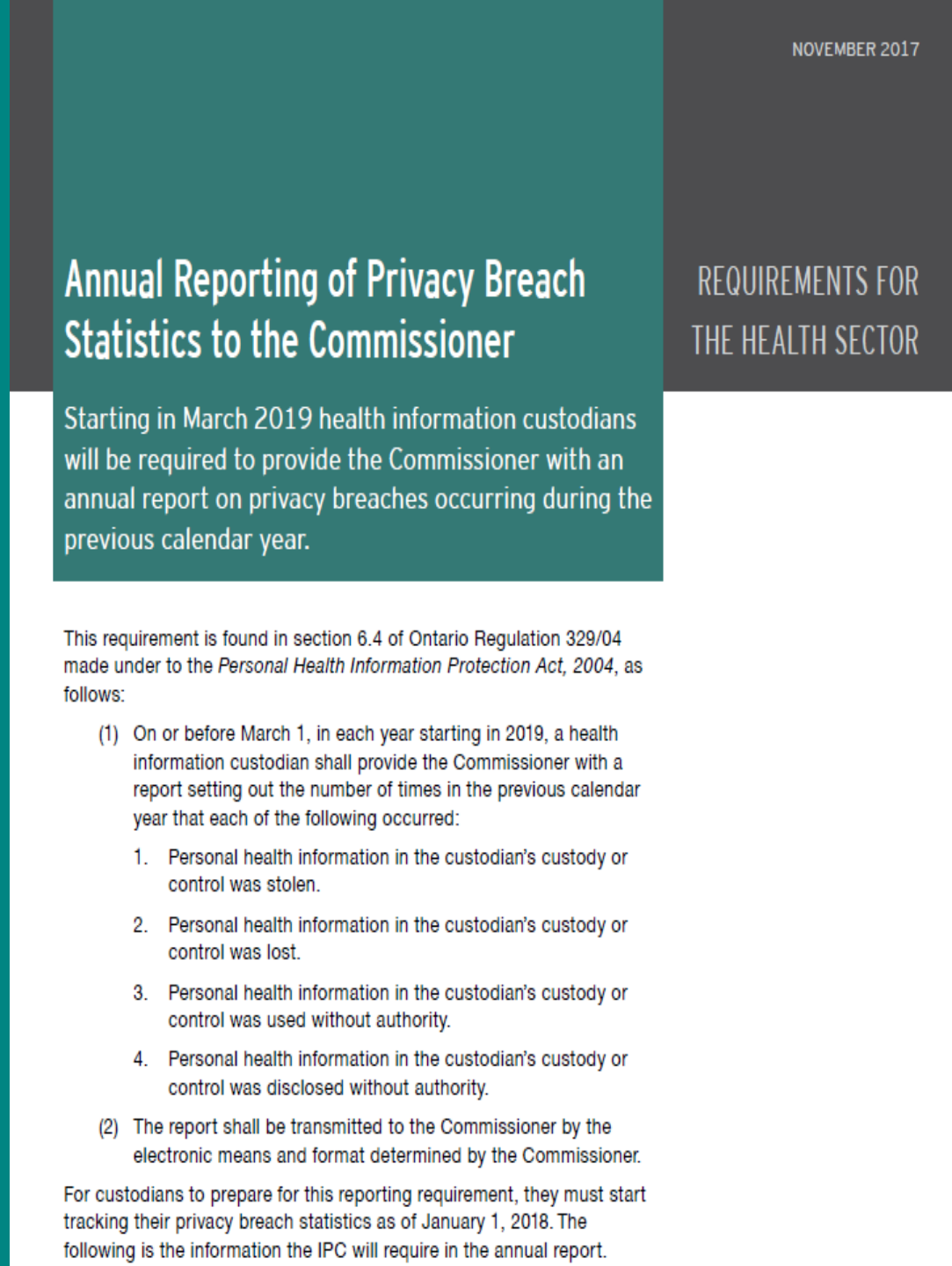
- To determine if a breach is significant, consider all the relevant circumstances, including whether:
  - The information is sensitive
  - The breach involves a large volume of information
  - The breach involves many individuals' information
  - More than one custodian or agent was responsible for 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
- Example: Disclosing a large volume of information about a number of patients to an unintended recipient

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 Reports to the Commissioner

- The IPC has released a guidance document about the statistical reporting requirement.
- 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 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 IPC at the time they occurred
- Will be collected through the IPC's Online Statistics Submission Website
  - https://statistics.ipc.on.ca/web/site/login

Provincial Electronic Health Record

Part V.1 of PHIPA

- Bill 119 (passed May 2016) amended PHIPA, including by introducing Part V.1
- Part V.1 relates to the provincial electronic health record (provincial EHR)
- All the provisions in Bill 119 were proclaimed into force on June 3, 2016, with the exception of those related to the provincial EHR, Part V.1 which are still not in force

Governance Model

- No custodian will have sole custody or control of PHI in the provincial EHR – it will be shared
- A custodian will only have custody or control of PHI if it:
  - Creates and contributes the PHI to the provincial EHR
  - Collects the PHI from the provincial EHR

Responsibility for Developing and Maintaining the Provincial EHR

- The provincial EHR will be developed and maintained by a prescribed organization
- The prescribed organization will be required to comply with certain requirements, including:
  - Logging, auditing and monitoring instances where PHI is viewed, handled or otherwise dealt with
  - Logging, auditing and monitoring instances where consent directives are made, withdrawn, modified and overridden
  - Conducting threat and risk assessments
  - Having and complying with practices and procedures that are approved by the IPC every three years

Collection, Use and Disclosure

- In general, custodians will only be permitted to collect personal health information from the provincial EHR:
  - To provide or assist in the provision of health care to the individual to whom the PHI relates, or
  - If a custodian has reasonable grounds to believe it is necessary to eliminate or reduce a significant risk of serious bodily harm
- If personal health information is collected to provide health care, it may subsequently be used or disclosed for any purpose permitted by PHIPA
- If collected to prevent a significant risk of serious bodily harm, it may only be used and disclosed for this purpose
- Special definitions of collection, use and disclosure will apply

Collection, Use and Disclosure

- When a custodian views, handles or otherwise deals with all or a part of an individual's personal health information through the EHR and the information was provided by another custodian:
  - The custodian is considered to be collecting the personal health information if it is viewing, handling or otherwise dealing with the information for the first time
  - The custodian is considered to be using the personal health information each time it subsequently views, handles or otherwise deals with the information
- When a custodian views, handles or otherwise deals with an individual's personal health information that the custodian provided to the EHR itself, it will be considered a use
- When a custodian provides an individual's personal health information to the EHR, it is considered to be disclosing it only when another custodian accesses it through the EHR.

Directed Disclosures

- The Minister will be able to direct the disclosure of personal health information contributed by more than one custodian:
  - To prescribed registries (e.g. Cardiac Care Network of Ontario) for the purposes of section 39(1)(c) of *PHIPA*
  - To prescribed entities (e.g. Cancer Care Ontario) for the purposes of section 45 of *PHIPA*
  - To certain public health authorities (e.g. medical officers of health) for the purposes of section 39(2) of *PHIPA*
  - For research purposes in accordance with section 44 of *PHIPA*
- Prior to directing the disclosure, the Minister must consult with the advisory committee

Consent Directives

- Individuals cannot opt out of having their personal health information included in the provincial EHR
- Once included, however, individuals will have the right to implement consent directives
- A consent directive withholds or withdraws the consent of an individual to the collection, use or disclosure of his or her personal health information for health care purposes

Consent Overrides

- A custodian will be permitted to override a directive:
  - With the express consent of the individual; or
  - Where there are reasonable grounds to believe it is necessary to eliminate or reduce a significant risk of serious bodily harm to:
    - the individual; or
    - another person if it is not reasonably possible to get timely consent

Notice of Consent Overrides

- Where a directive is overridden, the prescribed organization will be immediately required to provide written notice to the custodian that collected the personal health information
- Upon receipt of the notice, the custodian is required to:
  - Notify the individual to whom the personal health information relates at the first reasonable opportunity; and
  - Where the personal health information is collected to eliminate or reduce a significant risk of serious bodily harm to a third person, provide additional written notice to the Commissioner

Questions?

HOW TO 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