Providing Electronic Services to Health Information Custodians

Nicole Minutti

Senior Health Policy Advisor

Information and Privacy Commissioner of Ontario

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

Children's Treatment Network – Privacy Working Group Meeting

Dec 6, 2018

Outline

1. Application of PHIPA
2. Duties of Custodians and Agents
    - Collection, use and disclosure
    - Access and correction
    - Transparency of information practices
    - Security
3. Electronic Service Providers and Health Information Network Providers
4. Electronic Health Records

1. Application of PHIPA

PHIPA sets out rules for the collection, use and disclosure of personal health information by health information custodians

Application of PHIPA

- Ontario's *Personal Health Information Protection Act* (PHIPA) sets out rules for the collection, use and disclosure of personal health information by health information custodians

- PHIPA applies to personal health information in the custody or control of:
  - Health information custodians
  - Agents of health information custodians

Personal Health Information

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

Health Information Custodians

- Health information custodians include:
  - Health care practitioners
  - Group practices of health care practitioners
  - Service providers who provide community services
  - Hospitals, psychiatric facilities and independent health facilities
  - Long-term care homes, retirement homes and homes for special care
  - Pharmacies, ambulance services, labs and specimen collection centres
  - Centres, programs or services for community health or mental health
  - Medical officers of health
  - Minister/Ministry of Health and Long-Term Care
  - Public Health Ontario
  - Local Health Integration Networks

Agents

- An agent is a person who is authorized by a custodian to act for or on their behalf regarding personal health information
- It does not matter whether or not the agent:
  - Is employed by the custodian
  - Is paid by the custodian
  - Has the authority to bind the custodian
- A custodian remains responsible for the personal health information that is collected, used, disclosed and retained or disposed of by an agent

2. Duties of Custodians and Agents

Health information custodians have a number of duties under PHIPA related to:

- Collection, use and disclosure
- Access and correction
- Transparency of information practices
- Security

Duties of Custodians and their Agents

- Custodians have a number of duties under PHIPA which generally fall into four categories:
  - **2a.** Collection, use and disclosure
  - **2b.** Access and correction requests
  - **2c.** Transparency of information practices
  - **2d.** Security

2a. Collection, Use and Disclosure

Under PHIPA, custodians are not permitted to collect, use or disclose personal health information unless

- The individual consents, or
- The collection, use or disclosure is permitted or required by PHIPA

LIMITING PRINCIPLES

- Custodians are not permitted to collect, use or disclose PHI if other information will serve the purpose
- Custodians are not permitted to collect, use or disclose more PHI than is reasonably necessary for the purpose

2b. Access and Correction Requests

ACCESS

- Individuals have a right of access to their health records with some exceptions
- Custodians must respond within 30 days (with the possibility of a 30 day extension)

CORRECTION

- Individuals may request correction of their health records
- Custodians must respond within 30 days
- If the individual shows that it is not accurate, custodians must correct the record unless:
  - It was not originally created by the custodian and they do not have sufficient expertise, knowledge or authority to correct the record; or
  - It consists of professional opinion or observation that the custodian has made in good faith

2c. Transparency of Information Practices

CONTACT PERSON

- Custodians must designate a contact person responsible for
  - Facilitating their compliance with PHIPA
  - Ensuring that all agents are appropriately informed of their duties under PHIPA
  - Responding to inquiries from the public about their information practices
  - Responding to requests for access to or correction of health records
  - Receiving complaints from the public about their compliance with PHIPA

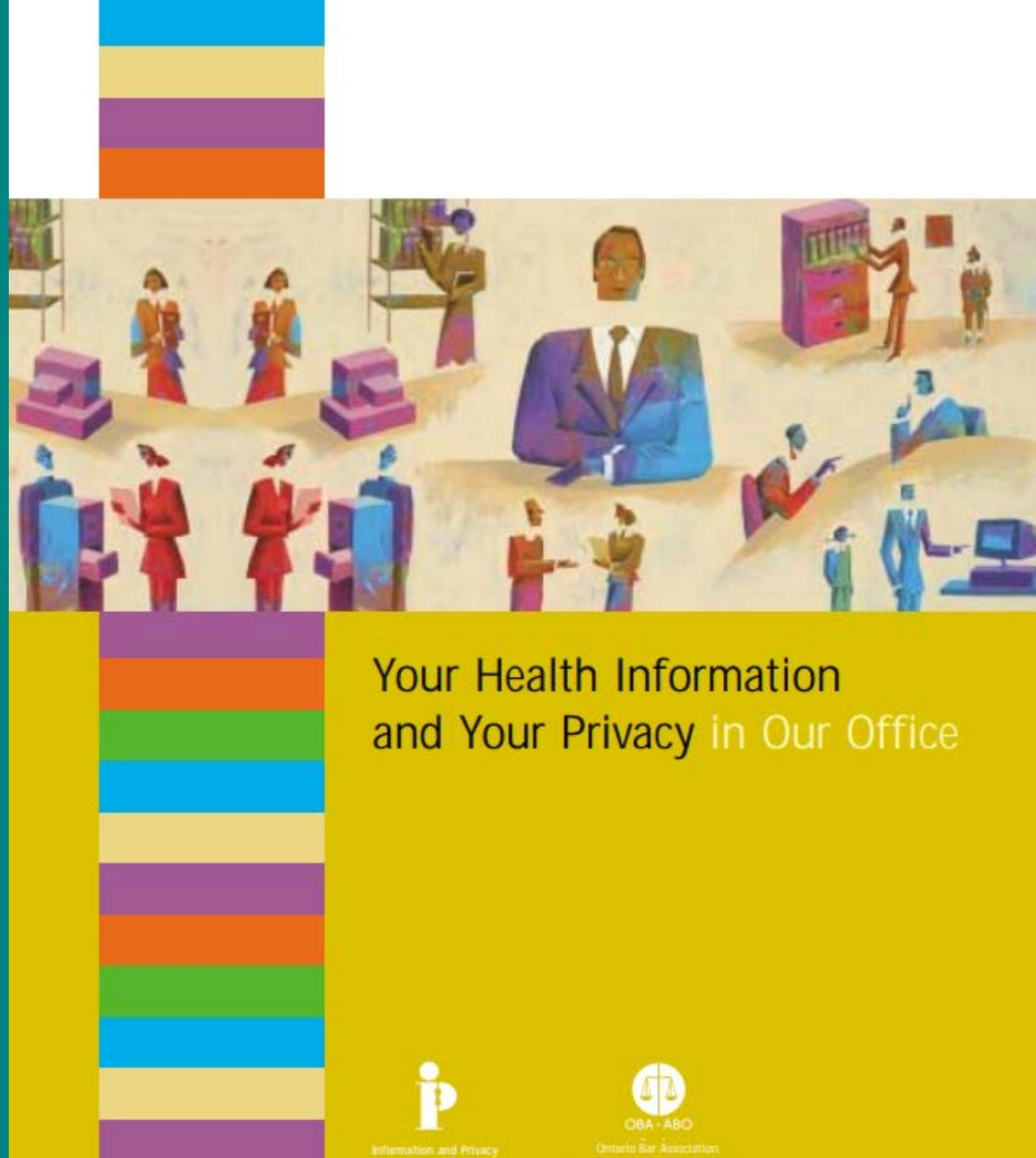
WRITTEN PUBLIC STATEMENT

- Custodians must make available to the public a written statement that:
  - Provides a general description of their information practices
  - Describes how to contact the contact person
  - Describes how to obtain access to or request correction of a health record
  - Describes how to make a complaint to the custodian and to the Commissioner

Your Health Information and Your Privacy

The IPC provides downloadable posters and brochures that custodians may provide to individuals

https://www.ipc.on.ca/health/your-health-privacy-rights-in-ontario/your-health-information-and-your-privacy-in/



Cont'd

2c. Transparency of Information Practices

NOTIFICATION

- If a custodian uses or discloses personal health information without consent, outside the scope of its written information practices, the custodian must:
  - Inform the individual at the first reasonable opportunity
  - Make a note of the uses and disclosures
  - Keep the note as part of the health record about the individual

2d. Security

- Custodians must take reasonable steps to ensure that personal health information is protected against
  - theft, loss and unauthorized collection, use or disclosure
  - unauthorized copying, modification, or disposal

NOTICE OF THEFT, LOSS, ETC. TO INDIVIDUAL

- If personal health information is stolen, lost, used or disclosed without authority, custodians must:
  - Notify individuals at the first reasonable opportunity
  - Inform the individuals, in the notice, that they are entitled to make a complaint to the IPC

NOTICE TO COMMISSIONER

- Under prescribed circumstances, custodians must notify the Commissioner

Point-in-Time Reporting of Breaches to the IPC

- Custodians must notify the IPC of a breach, when it is discovered, 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
- *To determine if a breach is significant, custodians must consider all relevant circumstances, including whether the breach involves:
  - Information that is considered sensitive
  - A large volume of information
  - The personal health information of many individuals
  - More than one custodian or agent who are responsible for the breach

Breach Notification to the IPC

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

https://www.ipc.on.ca/wp-content/uploads/2017/08/health-privacy-breach-notification-guidelines.pdf

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

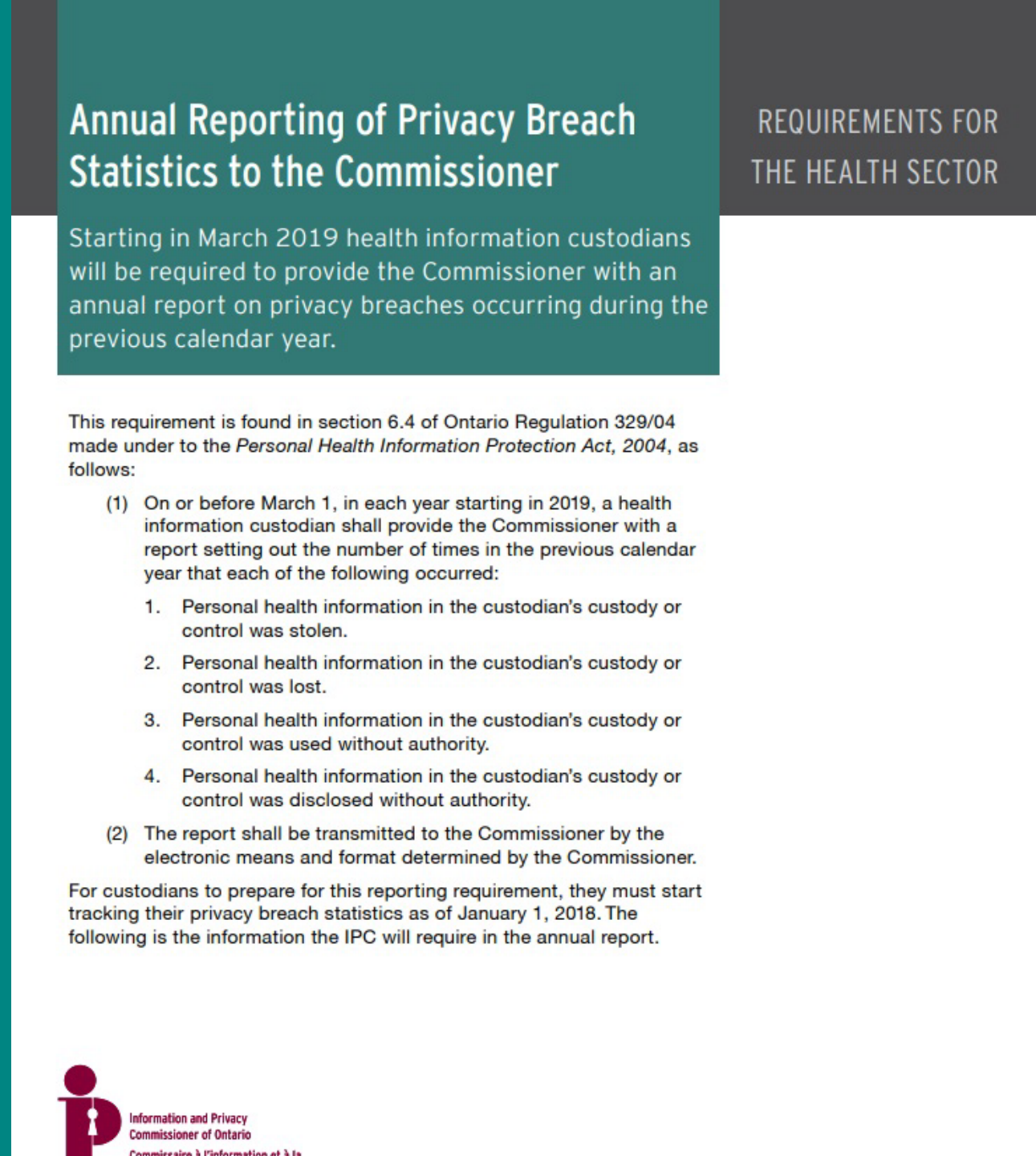
Annual Statistical Reporting of Breaches to IPC

- In addition to the point-in-time reporting requirements, custodians are required to report breaches to the IPC on an annual basis
- The report must include all breaches of personal health information that required notification to affected individuals
- The report must set out the number of times in the previous calendar year that personal health information was stolen, lost, used or disclosed without authority
- Custodians are required to have started tracking privacy breach statistics as of January 1, 2018
- Custodians must provide the Commissioner with an annual report of the previous calendar year's statistics starting in March 2019

Annual Reports to the Commissioner

This guidance document outlines the specific information that must be reported for each category of breach

https://www.ipc.on.ca/wp-content/uploads/2017/11/annual-breach-statistics-rptg-2.pdf



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.

Information and Privacy Commissioner of Ontario

3. Electronic Service Providers & Health Information Network Providers

ESPs and HINPs supply services that enable custodians to collect, use, modify, disclose, retain or dispose of personal health information electronically

Electronic Service Providers

- An electronic service provider (ESP) is a person who supplies services that enable a custodian to collect, use, modify, disclose, retain or dispose of personal health information electronically
- ESPs must comply with prescribed requirements
- When the ESP is not an agent of the custodian:
  - It shall not use any personal health information to which it has access, except as necessary in the course of providing the service
  - It shall not disclose the personal health information
  - It shall not permit any person acting on its behalf to access the information unless the person complies with the restrictions that apply to the ESP

Health Information Network Providers

- Health information network providers (HINPs) are a specific type of electronic service provider
- A HINP is a person who provides services to two or more custodians, where the services are provided primarily to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians
- Custodians are not considered to be disclosing personal health information when making the information available to HINPs for the purpose of providing HINP services and the HINP is not considered to be collecting the information

Health Information Network Provider Requirements

- There are a number of requirements for HINPs in addition to those for ESPs

NOTIFICATION

- Notify every custodian of a breach at the first reasonable opportunity

PLAIN LANGUAGE DESCRIPTION OF SERVICES

- Provide to each applicable custodian a plain language description of its services including a general description of safeguards to protect against breaches

PUBLIC DISCLOSURE

- Make the plain language description of its services available to the public
- Make available to the public any directives, guidelines and policies related to its services
- Make available a general description of the safeguards implemented

Cont'd

Health Information Network Provider Requirements

THREAT, VULNERABILITIES AND RISKS ASSESSMENT

- Perform and provide each custodian a written copy of the results of the following assessments:
  - Threats, vulnerabilities and risks to the security and integrity of the personal health information (e.g. a TRA)
  - How the services may affect the privacy of the individuals who are subject of the information (e.g. a PIA)

THIRD PARTY RESTRICTIONS

- Ensure any third party retained agrees to comply with the restrictions and conditions to comply with PHIPA

WRITTEN AGREEMENT

- HINPs must enter into written agreements with each custodian that:
  - Describes the services the HINP is required to provide for the custodian
  - Describes the administrative, technical and physical safeguards
  - Requires the HINP to comply with PHIPA

When Custodians are also Electronic Service Providers

- ESPs cannot collect, use, or disclose any of the personal health information they have access to in the course of providing ESP services to custodians
- An organization that is both a custodian within a health information network and is the network's HINP must make clear its authorities under each role
- Written agreements must set out the purposes, if any, the custodian is permitted to collect, use and disclose personal health information from the network

When Agents are also Electronic Service Providers

- ESPs cannot collect, use, or disclose any of the personal health information they have access to in the course of providing ESP services to custodians
- Agents cannot collect, use or disclose any personal health information, except as permitted by the custodian(s) of which it is an agent - they cannot collect, use or disclose personal health information for their own purposes
- An organization that is both an agent of a custodian(s) within a health information network and is the network's HINP must make clear its authorities under each role
- Written agreements should set out the purposes, if any, the organization, as an agent, is permitted to collect, use and disclose personal health information on the custodian(s)' behalf

5. Electronic Health Records

There are specific requirements under PHIPA when custodians provide personal health information to eHealth Ontario for the purpose of electronic health records

eHealth Ontario

- Custodians who provide personal health information to eHealth Ontario for the purpose of the EHR are not considered to be disclosing the information and eHealth Ontario is not considered to be collecting the information
- "Electronic health record" means a record of personal health information created or maintained by eHealth Ontario to enable custodians to disclose personal health information to one another electronically for the purpose of providing health care

eHealth Ontario Prescribed Requirements (until proclamation of Bill 119)

- eHealth Ontario must limit personal health information to what is reasonably necessary for the EHR
- Must not permit employees to access personal health information unless acting on behalf of eHealth Ontario and complying with applicable restrictions
- Must notify, at the first reasonable opportunity, every custodian that provided eHealth Ontario with personal information if the information is breached
- Must make available to the public and custodians:
  - Plain language description of the EHR including a general description of administrative, technical and physical safeguards to protect the information
  - Directives, guidelines and policies that apply to the personal health information in the EHR

eHealth Ontario Prescribed Requirements (until proclamation of Bill 119)

Cont'd

- Must perform and provide each custodian with a written copy and provide a public summary of the results of the following assessments:
  - Threats, vulnerabilities and risks to the security and integrity of the personal health information contained in the EHR (e.g. a TRA)
  - How the EHR may affect the privacy of the individuals who are subject of the information (e.g. a PIA)
- Must take reasonable steps to keep a record of all accesses to the EHR which identifies the person who accessed the information, the date, time and location of the access (audit logs)

Amendments to PHIPA - Bill 119

- Bill 119 was introduced on September 16, 2015 and received Royal Assent May 18, 2016
- Proclaimed into force on June 3, 2016 (except Part V.1 related to the provincial EHR)
- Once proclaimed, s. 6.2 of the regulation will be revoked and s. 55.1 will come into force

The provisions not yet proclaimed will:

- Set out the rules for collection, use and disclosure of personal health information in a provincial EHR
- Establish processes by which individuals can implement consent directives with respect to their personal health information
- Establish processes by which individuals can access their records of personal health information from the provincial EHR

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