# Current Trends & Key Issues Under the *Personal Health Information Protection Act, 2004*

Brendan Gray, Health Law Counsel

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

OSMT Connect - London

September 22, 2018

# DISCLAIMER

THIS PRESENTATION IS:

- PROVIDED FOR INFORMATIONAL PURPOSES,
- NOT LEGAL ADVICE, AND
- NOT BINDING ON THE IPC.

# Topics

1. Quick overview of the application of the *Act*
2. *Bill 119 – Health Information Protection Act*

# Application of the *Act*

# Application of the *Act*

- The *Personal Health Information Protection Act, 2004* came into force on November 1, 2004 (the *Act*)
- The majority of the Act governs "personal health information" in the custody or control of:
  - "Health Information Custodians," or
  - "Agents" of health information custodians
- However, the Act also has broader application
  - For example it contains restrictions on the use and disclosure of personal health information by non-health information custodians that receive personal health information from health information custodians

# Definition of Personal Health Information

Defined as 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

# 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 centre, program or service for community health or mental health whose primary purpose is the provision of health care.
- A hospital, psychiatric facility and independent health facility
- A pharmacy, ambulance service, laboratory or specimen collection centre
- A long-term care home, care home or home for special care
- A medical officer of health of a board of health
- Minister/Ministry of Health and Long-Term Care
- Every local health integration network

# 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

- It is irrelevant whether or not the agent:
  - is employed by the health information custodian
  - is remunerated by the health information custodian
  - has the authority to bind the health information custodian

- A health information custodian remains responsible for personal health information collected, used, disclosed, retained or disposed of by an agent

# Duties Imposed on Health Information Custodians and Their Agents

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

# General Provisions Related to Collection, Use and Disclosure

- Not permitted to collect, use or disclose personal health information if other information will serve the purpose
- Not permitted to collect, use or disclose more personal health information than reasonably necessary
- 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 the Act to be made without consent

# 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; and
   - That the individual may give or withhold consent

3. Relate to the information, and

4. Not be obtained by deception or coercion.

# Notice of Purposes

- A custodian may rely on a *Notice of Purposes* to support the reasonable belief that an individual knows the purpose of the collection, use or disclosure of personal health information unless it is not reasonable

- A *Notice of Purposes*:
  - Must be posted where it is likely to come to the attention of the individual or must be provided to the individual;
  - Must outline the purposes for which the custodian collects, uses or discloses personal health information; and
  - Should advise the individual that he or she has the right to give or withhold consent

- A *Notice of Purposes* is not required when consent may be assumed to be implied but it is a best practice

# Types of Consent

- There are three types of consent under the *Act*:
  - Express consent
  - Implied consent
  - Assumed implied consent
- Assumed implied consent provisions are sometimes referred to as the “circle of care” provisions

# Express Consent

- Consent may be express or implied, except when the Act specifies that consent must be express
- Express consent is not a defined term in the *Act*
- 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
  - 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 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
- 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 health information custodian for the provision of health care

# Assumed Implied Consent

- Sometimes referred to as “Circle of Care”

- Section 20(2) of the *Act* 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.

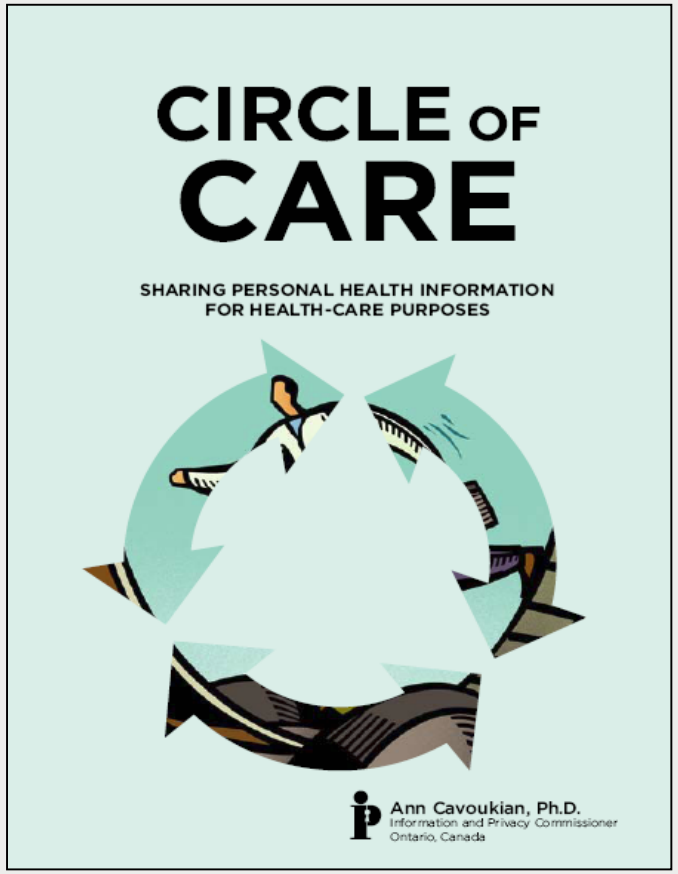
- In the context of a disclosure, the disclosure must be made to another health information custodian

# Circle of Care: Sharing Personal Health Information for Health Care Purposes

The guide was published to clarify the circumstances in which consent may be *assumed* to be implied by custodians

Members of the working group who participated in publishing the guide, included:

- Information and Privacy Commissioner/ Ontario
- College of Physicians and Surgeons of Ontario
- Ontario Association of Community Care Access Centres
- Ontario Association of Non-Profit Homes and Services for Seniors
- Ontario Long Term Care Association
- Ontario Hospital Association
- Ontario Medical Association
- Ontario Ministry of Health and Long-Term Care




**Available at [www.ipc.on.ca](http://www.ipc.on.ca)**

# Withholding and Withdrawing Consent and Express Instructions

- The *Act* provides individuals with 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; and
  - Instruct that their personal health information not be used or disclosed without consent for health care purposes as set out in sections 37(1)(a), 38(1)(a) and 50(1)(e) of the Act
- These are referred to as the “lock-box” provisions, although lock-box is not a term found in the Act

# Duties Arising From Withholding and Withdrawing Consent or Express Instructions

1. 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,
    - The Act permits the collection, use or disclosure to be made without consent, except as set out in sections 37(1)(a), 38(1)(a) and 50(1)(e)
2. Compliance may be achieved through policies, procedures or manual processes and/or electronic or technological means
3. Where a custodian is prevented from disclosing personal health information to certain 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; and
    - The receiving health information custodian may explore the matter with the individual and seek consent to access the locked information

# Collections, Uses and Disclosures Permitted Without Consent

- Collections of personal health information permitted without consent are set out in section 36 of the *Act*
- Uses of personal health information permitted without consent are set out in section 37 of the *Act*
- Disclosures permitted without consent are set out in sections 38 – 48 and section 50 of the *Act*

Example: **Under the *Act,* health information custodians may disclose personal health information as permitted or required under other Acts, subject to any prescribed requirements or restrictions**. A regulation to the *Laboratory and Specimen Collection Centre Licensing Act,* requires disclosure of reportable diseases to a medical officer of health or health unit. The *Act* permits this disclosure as no requirements or restrictions are prescribed.

# Bill 119 – *Health Information Protection Act*

# Bill 119

- Bill 119 was introduced on September 16, 2015
- It amends the *Act*, including by introducing Part V.1
- Part V.1 relates to the provincial electronic health record (provincial EHR)
- All the provisions in the Bill were proclaimed into force on June 3, 2016, with the exception of those related to the provincial EHR

# Breach Notification

- A custodian must notify the individual at the first reasonable opportunity if PHI in its custody or control is stolen, lost or used or disclosed without authority
- In the context of the provincial EHR, the custodian must also notify the individual at the first reasonable opportunity if PHI is collected without authority
- The Commissioner must also be notified if the circumstances surrounding the theft, loss or unauthorized collection, use or disclosure meets certain prescribed requirements

# Breach Notification to the Commissioner

- Regulations prescribing when the Commissioner must be notified came into force October 1, 2017

- The IPC recently published a guidance document explaining 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

# Circumstances Where a Breach Must be Reported to the Commissioner

- A custodian has reasonable grounds to believe that PHI in its 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**
    - The person could be your employee, a health care practitioner with privileges, a third party (such as a service provider), or even someone with no relationship to you
    - Typical example is the "snooping case"
    - You generally do not need to notify the Commissioner when the breach is accidental, for example, when information is inadvertently sent by email or courier to the wrong person
    - However, accidental privacy breaches must be reported if fall into one of the other categories
  - **stolen**
    - An example is where someone has stolen paper records or a laptop or other electronic device
    - You do not need to notify the Commissioner if the information was de-identified or properly encrypted

# Circumstances Where a Breach Must be Reported to the Commissioner (Cont'd)

- **after an initial loss or unauthorized use or disclosure, the PHI was or will be further used or disclosed without authority**
  - An example is where an agent accessed PHI without authority and subsequently used this information to market products or services or to commit fraud (such as health care or insurance fraud)
  - Even if you did not report the initial incident, you must notify the Commissioner of this situation
- **loss or unauthorized use or disclosure is part of a pattern of similar losses or unauthorized uses or disclosures of PHI**
  - An example is you discover that a letter to a patient inadvertently included PHI relating to a different patient. Over a few months, the same mistake is repeated several times because an automated process for generating letters has been malfunctioning for some time
  - You must use your judgment in deciding if a privacy breach is an isolated incident or part of a pattern
  - Take into account, for instance, the time between the breaches and their similarities
  - Keeping track of privacy breaches in a standard format will help you identify patterns.

# Circumstances Where a Breach Must be Reported to the Commissioner (Cont'd)

- **A custodian is required to give notice to a College of an event described in section 17.1 of the *Act* that relates to a loss or unauthorized use or disclosure of PHI**
  - Custodians must give notice to a health regulatory college of an event described in section 17.1
  - Custodians must also give notice to the Commissioner of losses or unauthorized uses and disclosures in the same circumstances a custodian is required to give notice to a health regulatory college under section 17.1
  - Where an agent is a member of a health regulatory college, you must notify the Commissioner of a loss or unauthorized use or disclosure of PHI if:
    - you terminate, suspend or discipline them as a result of the breach
    - they resign and you believe this action is related to the breach
  - Where a health care practitioner with privileges or otherwise affiliated with you is a member of a college, you must notify the Commissioner of a loss or unauthorized use or disclosure of PHI if :
    - you revoke, suspend or restrict their privileges or affiliation as a result of the breach
    - they relinquish or voluntarily restrict their privileges or affiliation and you believe this is related to the breach

# Circumstances Where a Breach Must be Reported to the Commissioner (Cont'd)

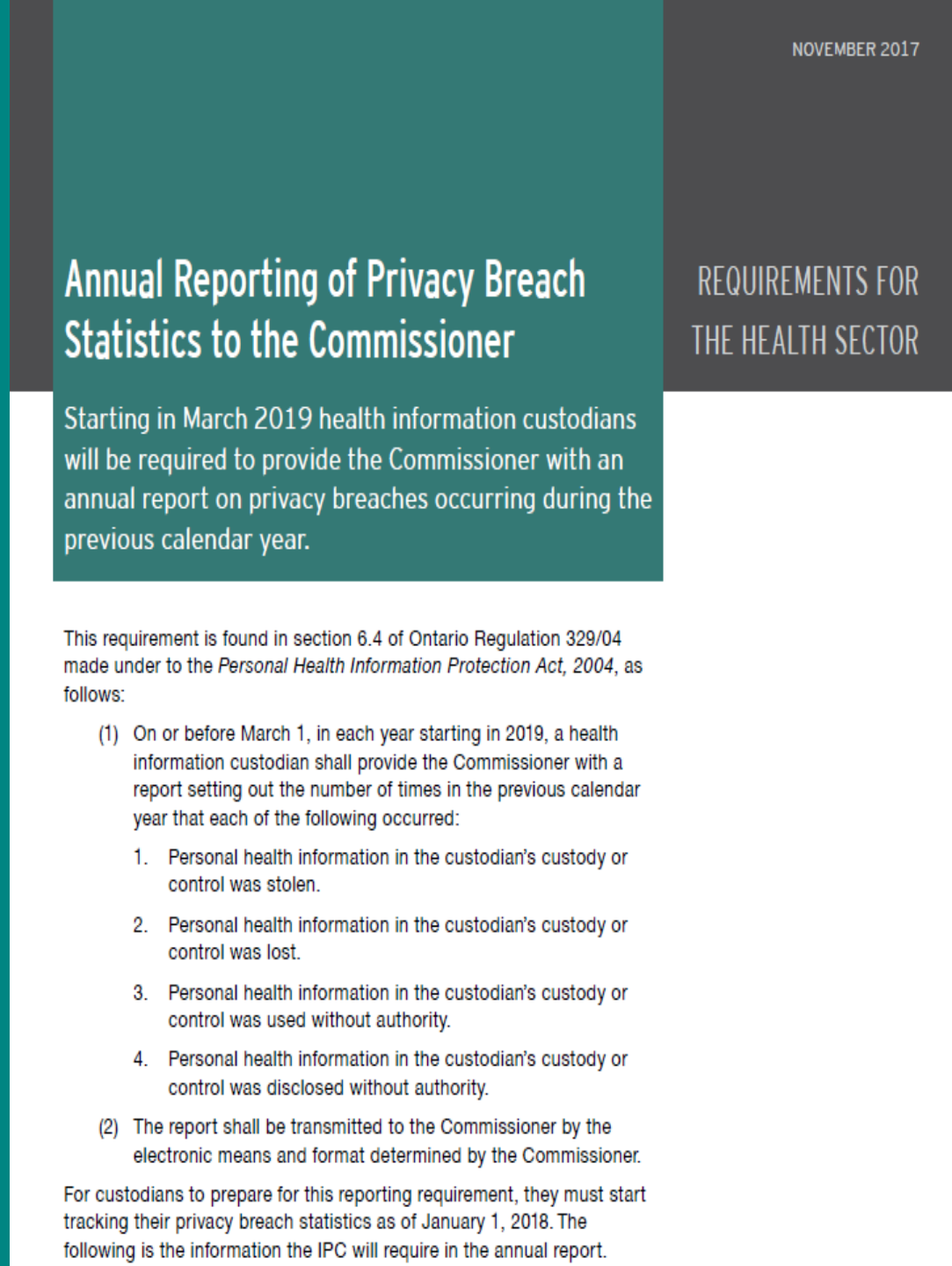
- A custodian would be required to give notice to a College, if an agent of the custodian were a member of the College, of an event described in section 17.1 of the *Act* that relates to a loss or unauthorized use or disclosure of PHI
  - Not all agents of a custodian are members of a college
  - If an agent is not a member, you must still notify the Commissioner in the same circumstances that would have triggered notification to a college, had the agent been a member
- A custodian determines the loss or unauthorized use or disclosure of PHI is significant after considering all relevant circumstances, including whether:
  - the PHI that was lost or used or disclosed without authority is sensitive
  - the loss or unauthorized use or disclosure involved a large volume of PHI
  - the loss or unauthorized use or disclosure involved many individuals' PHI
  - more than one custodian or agent was responsible for the loss or unauthorized use or disclosure of the PHI

# Duty to Notify Individuals

It is important to remember that even if you do not need to notify the IPC, you have a separate duty to notify individuals under section 12(2) of the *Act*.

# Annual Reports to the Commissioner

- Health information custodians must provide the IPC with annual privacy breach statistics starting in March 2019.
- They must track incidents commencing on January 1, 2018 where personal health information was:
    - stolen
    - lost
    - used without authority
    - disclosed without authority
- This annual report must also include breaches that do not meet the criteria for immediate mandatory reporting to the IPC.



NOVEMBER 2017

REQUIREMENTS FOR THE HEALTH SECTOR

## Annual Reporting of Privacy Breach Statistics to the Commissioner

Starting in March 2019 health information custodians will be required to provide the Commissioner with an annual report on privacy breaches occurring during the previous calendar year.

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.

# QUESTIONS?

# 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