Breach Reporting and Record Keeping under *PHIPA*

Manuela Di Re

Director of Legal Services and General Counsel

Information and Privacy Commissioner of Ontario

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

Privacy Law Summit 2018

Ontario Bar Association, Twenty Toronto Street

April 12, 2018

Amendments to *PHIPA*—Bill 119

- Bill 119 amended the *Personal Health Information Protection Act* (*PHIPA*) in a variety of ways, including implementing mandatory breach reporting to the Information and Privacy Commissioner of Ontario (IPC)
- Introduced on September 16, 2015
- Received Royal Assent May 18, 2016
- Proclaimed into force on June 3, 2016 (except Part V.1 related to the provincial electronic health record)
- Regulations prescribing circumstances in which breaches must be reported to the IPC took effect October 1, 2017

Breach Notification

- Pre-Existing:
  - A health information custodian must notify an affected individual at the first reasonable opportunity if personal health information in its custody or control is stolen, lost or used or disclosed without authority
- In addition:
  - A custodian must notify the IPC if the circumstances surrounding the theft, loss or unauthorized use or disclosure meet the prescribed requirements
  - A custodian must also, on or before March 1 in each year starting in 2019, provide the IPC with a statistical report of breaches in the previous calendar year

Point-In-Time 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—contd

- 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.

Statistics

	October 1, 2017-December 31, 2017	October 1, 2016-December 31, 2016
Total Breaches	125	58
Misdirected/Lost	36.7%	28%
Snooping	24%	24%
Unauthorized collection, use, disclosure	18.4%	15%
Stolen/Inadequately secured	20.9%	33%

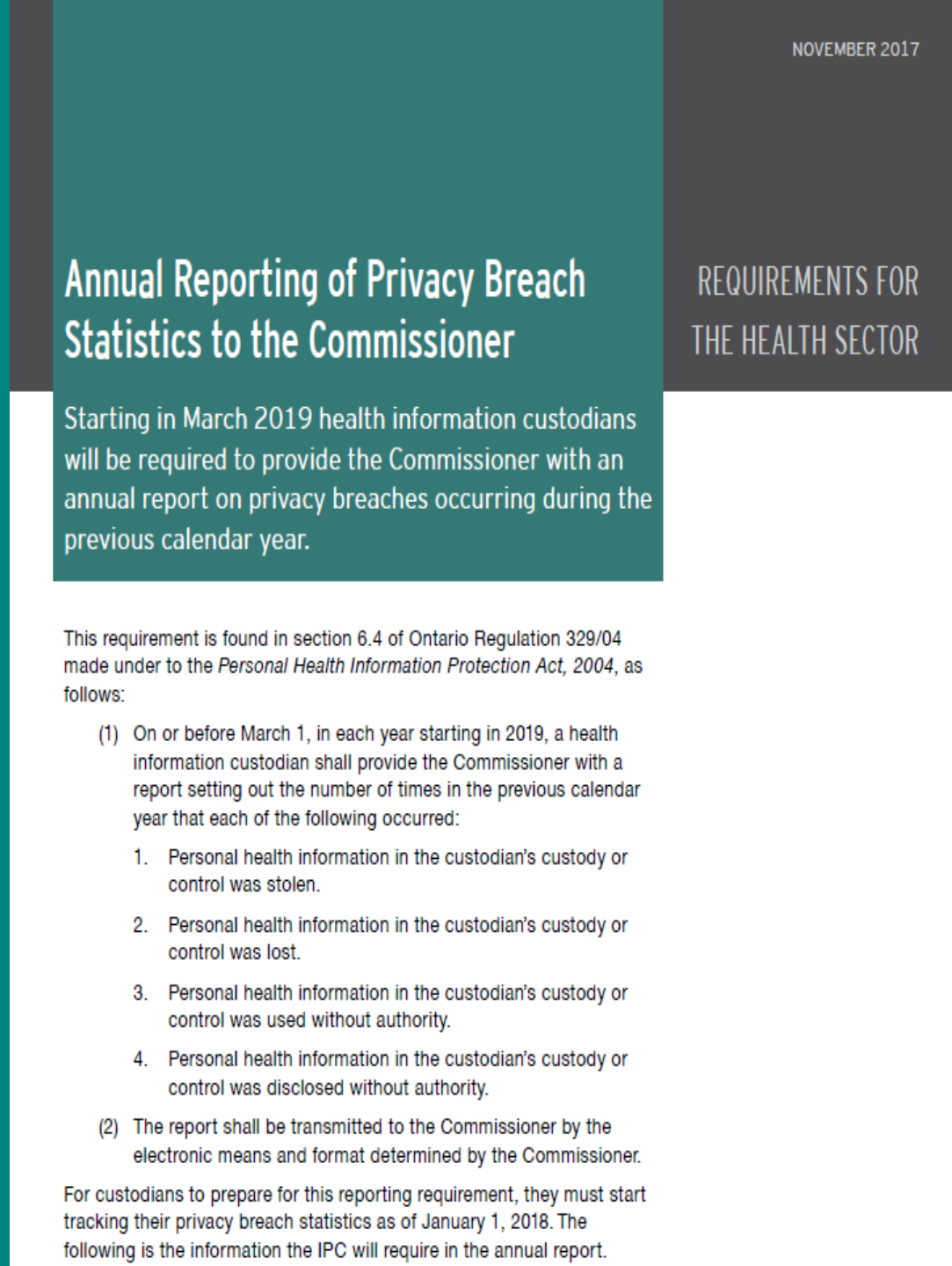
- The total number of breaches reported between October 1, 2017-December 31, 2017 represents a 115% increase over the same period in the previous year.

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.
- 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 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 Commissioner at the time they occurred.
- Will be collected through the IPC's Online Statistics Submission Website
  - https://statistics.ipc.on.ca/web/site/login

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