An Update on PHIPA from the IPC

Brian Beamish

Information and Commissioner Of Ontario

Information and Privacy Commissioner of Ontario

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

Osgoode Legal Guide to Privacy & Information Management in Healthcare

Toronto, Canada

April 9, 2019

Mandatory *PHIPA* Breach Reporting

- As of October 1, 2017, health information custodians must notify IPC of certain privacy breaches
  - use or disclosure without authorization
  - stolen information
  - further use or disclosure
  - breaches occurring as part of a pattern
  - breaches related to a disciplinary action against a college or non-college member
  - significant breaches
- Custodians began collecting breach statistics in January 2018 for reporting in March 2019

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

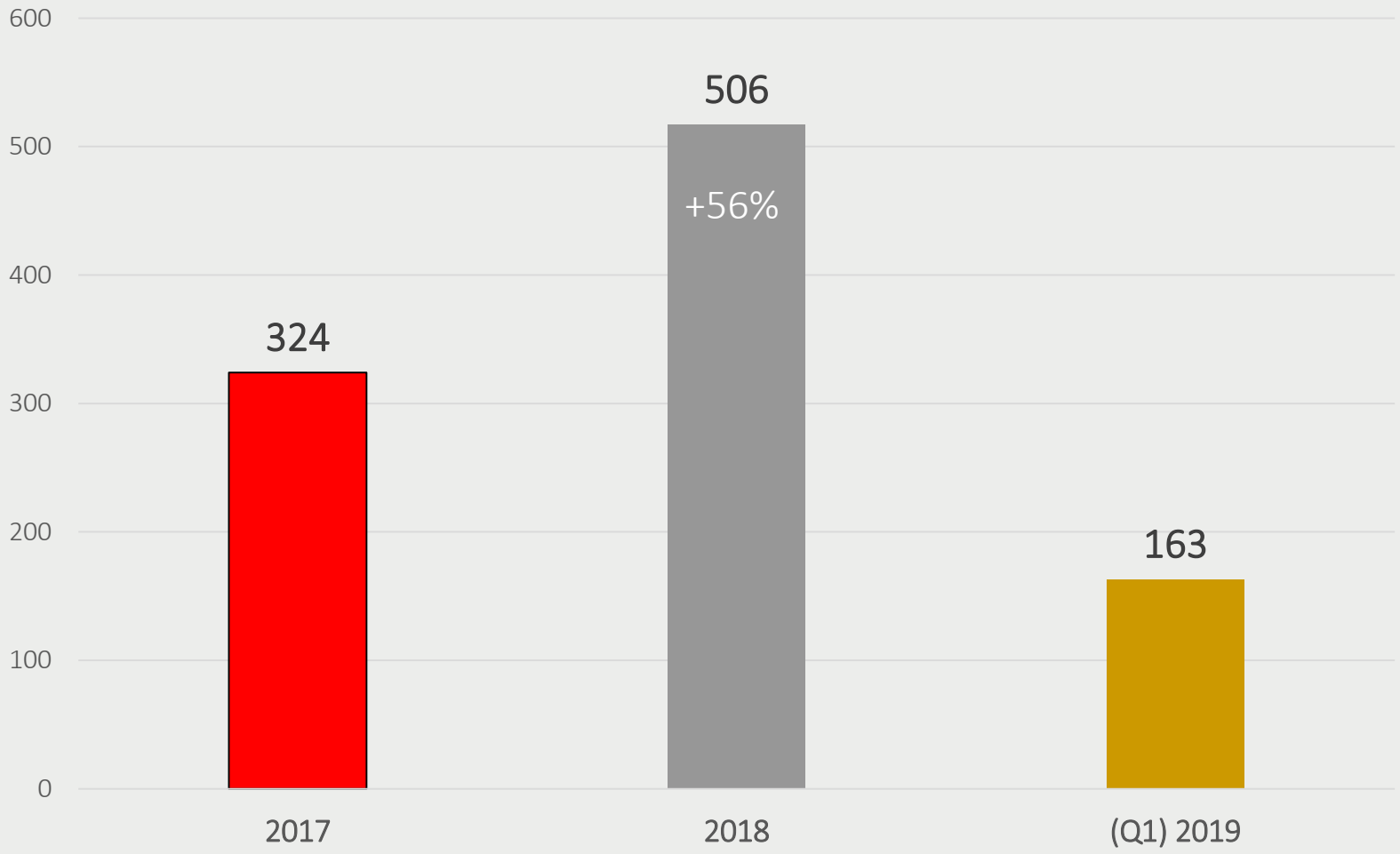
This category covers situations where the person committing the breach knew or ought to have known that their actions are not permitted either by the act or the responsible custodian. An example would be where a

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

When You May Not Need to Report a Breach

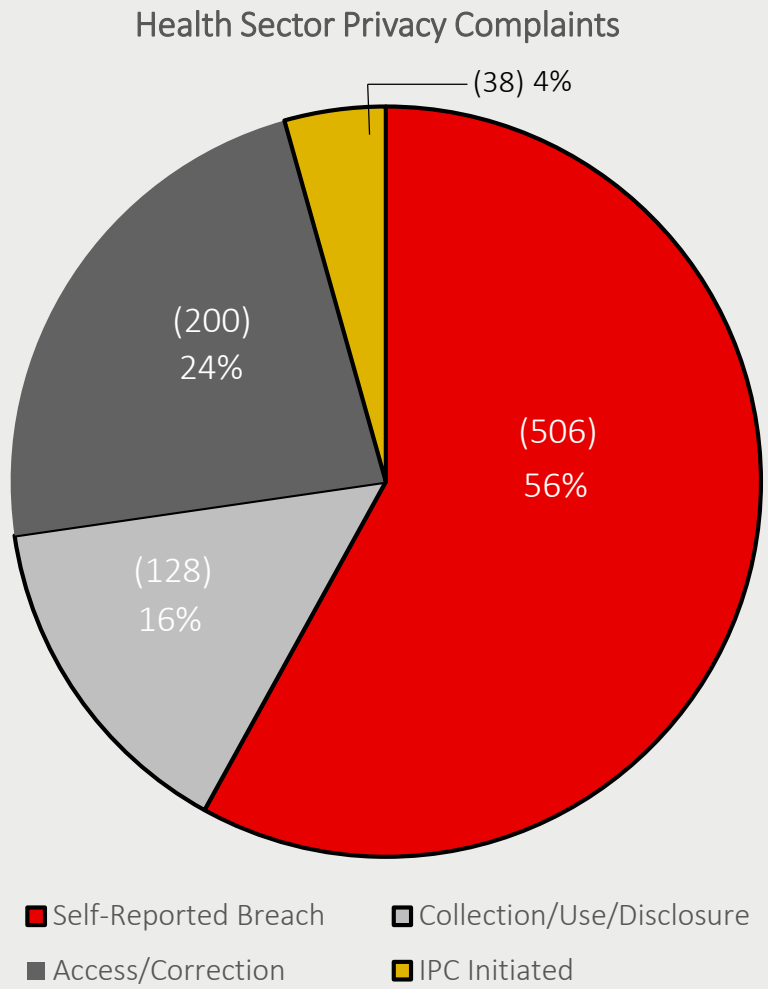
- You may not need to report a breach if:
  - it is not intentional
  - it is a one-off incident
  - it is not part of a pattern
- Not every breach is significant
  - nurse clicks on the wrong patient file
  - records clerk opens the wrong file folder
  - doctor walks into the wrong patient room

Self-Reported Breaches Before and After Mandatory Breach Reporting

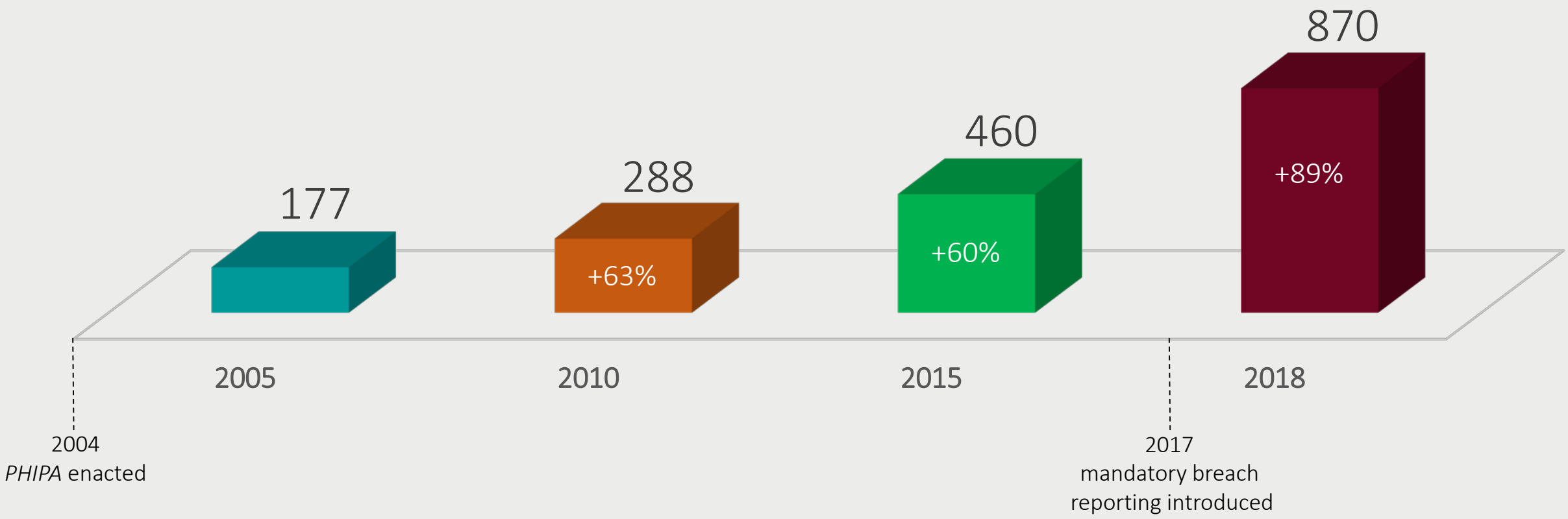


Health Sector Privacy Complaints 2018

- Of the 506 self-reported breaches in 2018:
  - 120 were snooping incidents
  - 15 were ransomware/cyberattack
- Remaining 371 were related to:
  - lost or stolen PHI
  - misdirected information
  - records not properly secured
  - other collection, use and disclosure issues



PHIPA Complaints Opened per Year



Fighting “Snooping” – Innovative Audit Solution

- Project to address the challenge of auditing transactions
- Use data analytics and AI
- IPC was approached by Mackenzie Health to participate in the project steering committee and provide a regulatory perspective
- Other partners included Michael Garron Hospital, Markham Stouffville Hospital and vendor, KI design
- Our office provided input throughout the pilot, particularly on the project objectives and assessment criteria

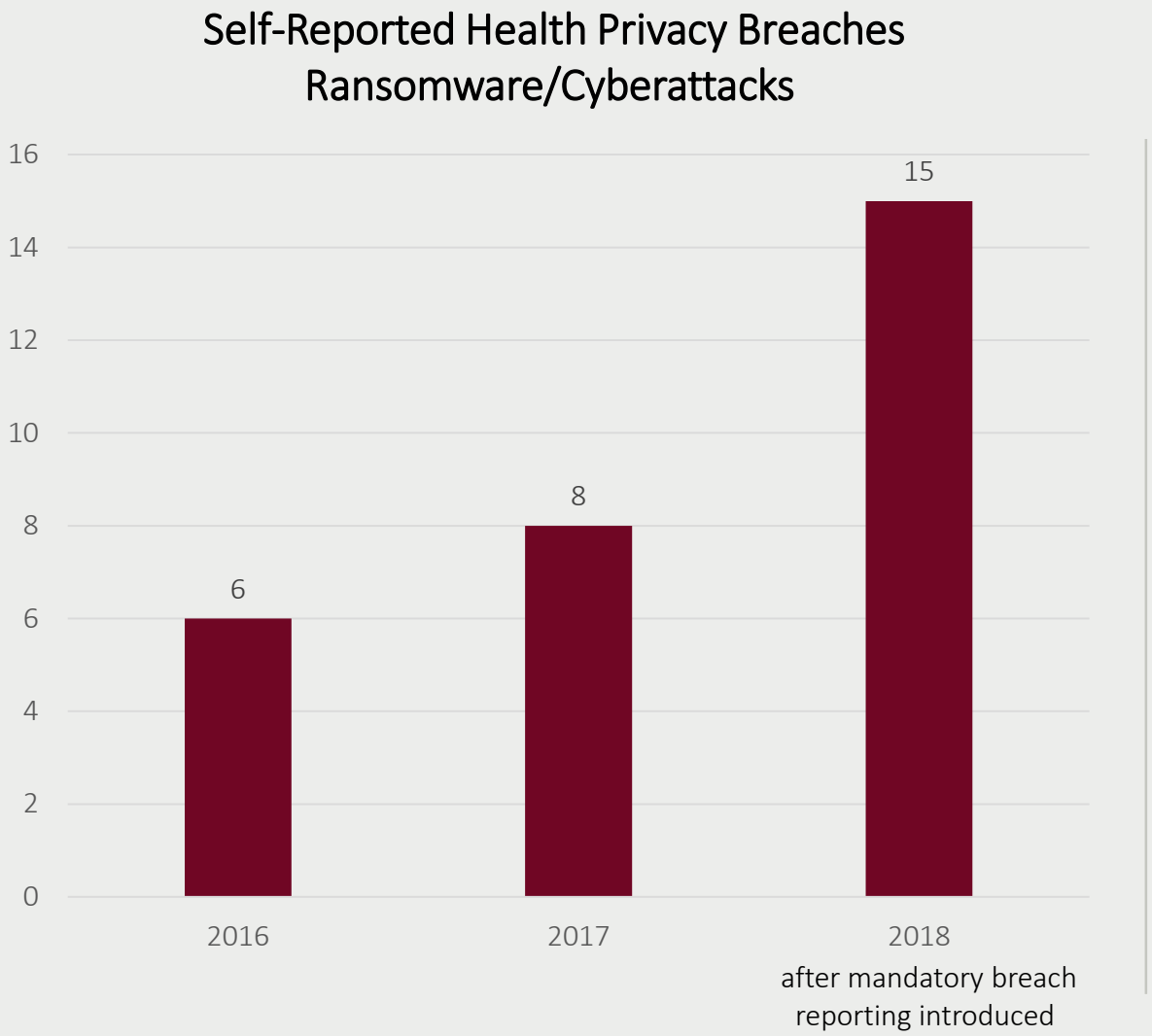
Results of the Pilot

- Initially, many privacy breaches were detected during the six month pilot
- The auditing solution used data analytics and AI to determine what accesses could be explained
- Breaches decreased significantly as the solution was fine tuned and missing information from various information systems (e.g., scheduling) was added
- The number of breaches is expected to decrease further with staff awareness and increased ability for solution to explain accesses

Privacy Breach Reporting

- The more effective the auditing and monitoring, the more privacy breaches that will be detect
- Those using innovative audit solutions will likely have more breaches to report, but over time the number of breaches is expected to decline
- IPC will **NOT** be identifying any health care organizations in our first annual report of privacy breaches

Cyberattacks and Ransomware



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

Technology Fact Sheet

Protecting Against Ransomware

July 2016

Ransomware has become an increasingly common and dangerous threat to the security of electronic records. This fact sheet provides information on how public institutions and healthcare organizations in Ontario can protect themselves against it.

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software, or "malware," that encrypts files on your device or computer, including any mapped or network drives, and then demands payment in exchange for the key needed to decrypt the files. It essentially locks you out of your data and holds the means of regaining access for ransom.

HOW DO COMPUTERS GET INFECTED?

Hackers use different techniques to install ransomware on computers. In general, these fall into two categories: "phishing" attacks and software exploits.

Phishing Attacks

Phishing is a type of online attack in which a hacker sends one or more individuals an unsolicited electronic communication—email, social media post or instant messenger chat—designed to trick or deceive a recipient into revealing sensitive information or downloading malware.

In the case of ransomware, the hacker will often try to impersonate an "official" correspondence relating to a common business transaction, such as a shipping notice or invoice from a delivery company. The hacker may also try to fake an "urgent matter," such as an unpaid invoice or notice of audit. More advanced versions (also known as "spear phishing") target specific individuals or places of business.

Ransomware may be installed if the recipient opens a file attachment or clicks on a link in the body of the message.

Protect your organization

- train employees
- limit user privileges
- use software protections and back-ups
- have an incident response plan in place

Casino Rama Investigation

- In November 2016, OLG reported to the IPC that Casino Rama Resort was subjected to a cyberattack
- IPC launched investigated the circumstances of the breach and whether reasonable security measures were in place to protect personal information of Rama customers
- The investigation revealed weaknesses in the cyber security practices – particularly with response to suspicious activity
- OLG/Casino Rama have taken steps to address the weaknesses identified – IPC satisfied
- Institutions should plan for cyberattacks by having appropriate measures in place to secure their systems, ensure early detection and action, and train staff

Avoiding Abandoned Records

- **Who is the custodian?**
  - in the event of death? bankruptcy? transfer?
  - in a group practice?
- **What obligations do custodian have?**
  - must retain, transfer and disposed of records in a secure manner
  - must take reasonable steps to prevent privacy breaches
  - must notify individuals of a transfer
- **How to avoid abandoned records?**
  - succession plan setting out roles and responsibilities

Personal Health Information on Social Media

FierceHealthcare

A Division of QUESTEX

Healthcare

WI nurses fired over cell photos of X-ray

Feb 27, 2009 12:42am

A pair of nurses accused of taking a picture of patient X-rays have been fired, with one also charged with posting the pictures on a Facebook page. While the nurses apparently didn't violate Wisconsin state laws, hospital and local officials said that they're investigating whether the nurses violated HIPAA.

The incident began when a patient was admitted to the emergency room with an object lodged in his rectum. According to the police, the two nurses took pictures of the patient's X-ray when they learned that the object was a sexual device. One of the two allegedly posted a discussion about the incident on her Facebook page, though police haven't found anyone who saw the pictures, they said.

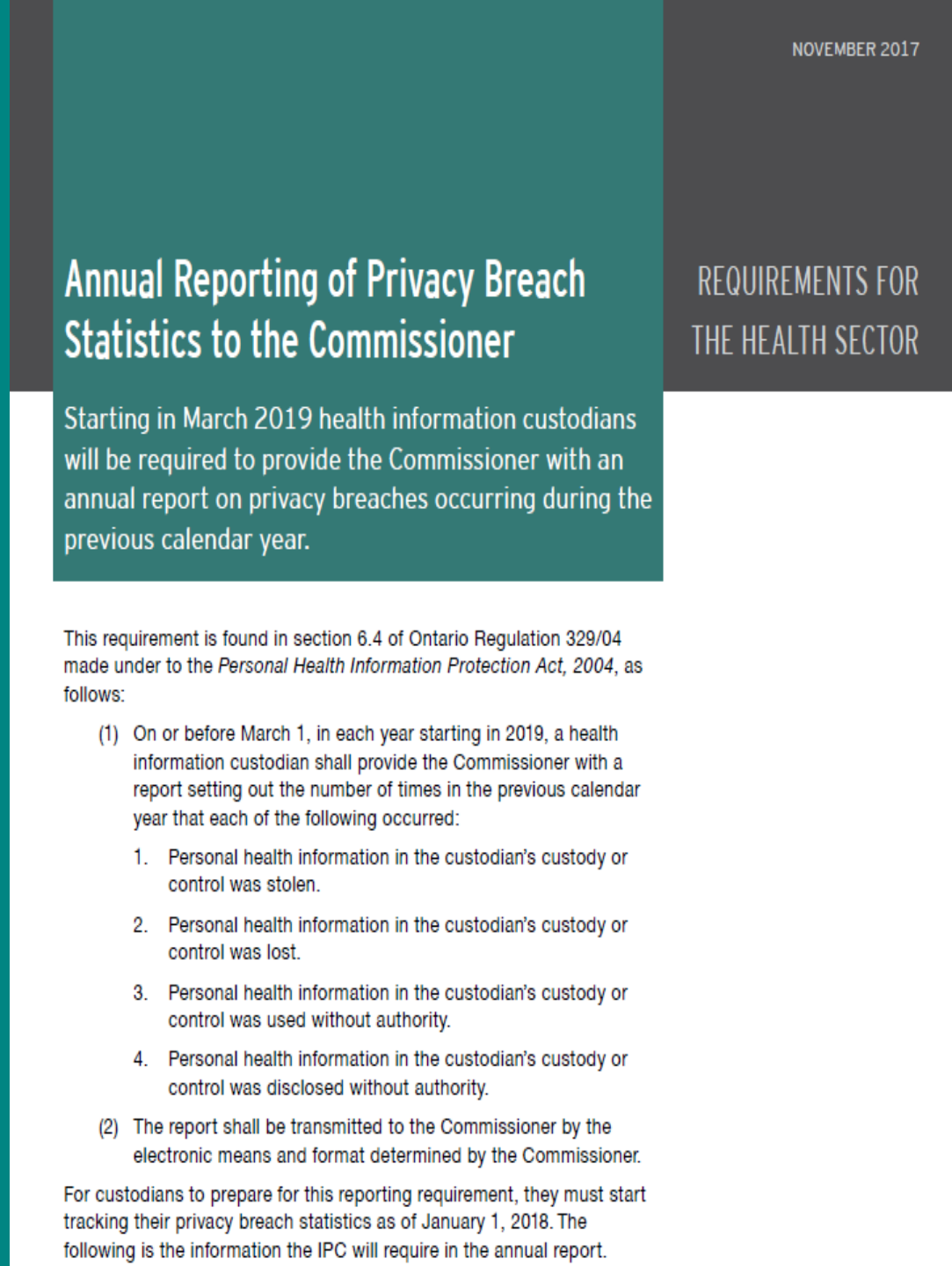
The hospital has referred the case to the FBI for further investigation.

Health Information Custodians must submit breach statistics every year.

They must submit statistics on breaches where information was:

- stolen
- lost
- used without authority
- disclosed without authority

This includes breaches that did not meet the criteria for 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:

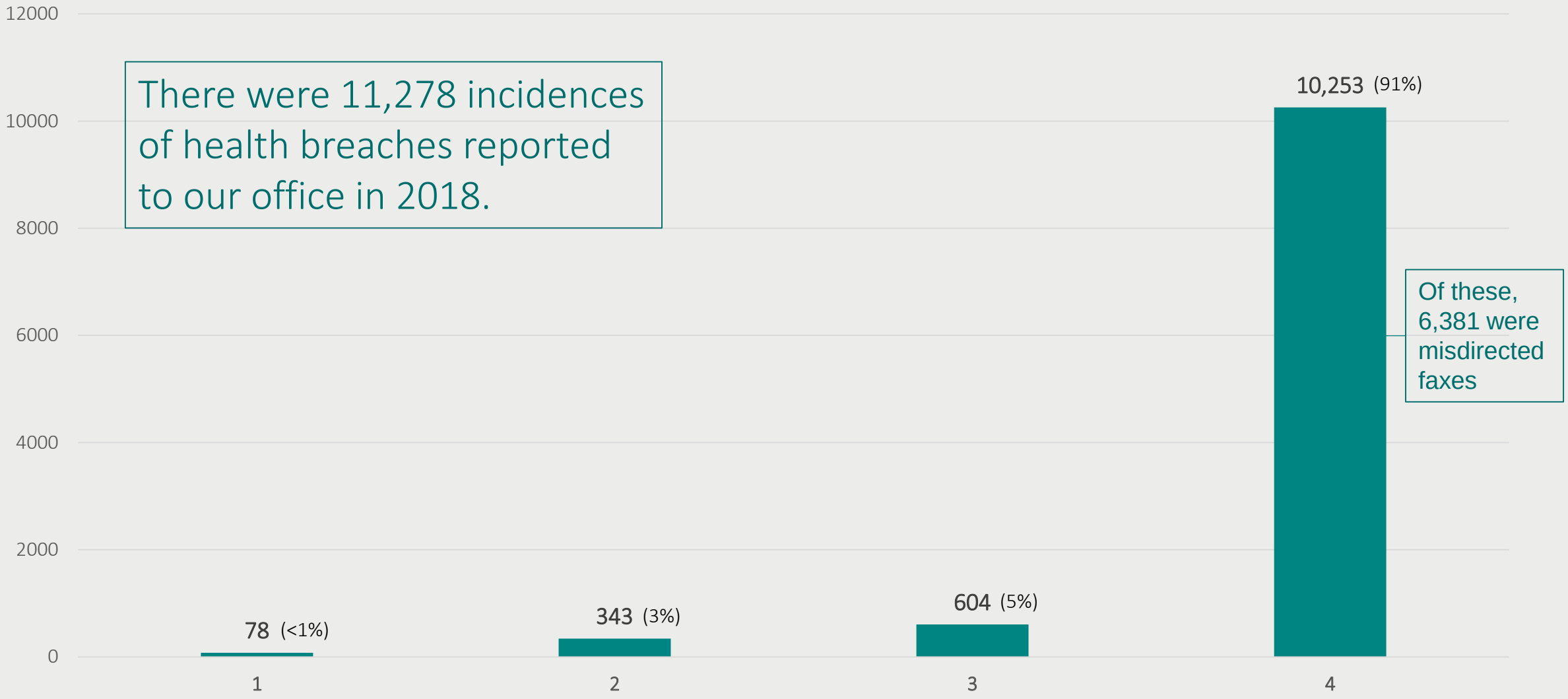
(1) On or before March 1, in each year starting in 2019, a health information custodian shall provide the Commissioner with a report setting out the number of times in the previous calendar year that each of the following occurred:

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.

Annual Reporting Breach Statistics, 2018



IPC Webinar

https://youtu.be/KjitJ74wn4A

Investigations

Limits to Correction

PHIPA Decision 67

- Complainant submitted a 62-part request to correct her health records, to the Toronto Central Local Health Integration Network
- TCLHIN agreed to make two corrections but denied the remainder
- IPC agreed that TCLHIN was not required to make the corrections
- Most were about differences of opinion - information was not inaccurate or incomplete
- Also, consisted of good faith professional opinions
- Decision provides guidance on dealing with complicated correction requests

No Review Where Complaint Dealt With Elsewhere

PHIPA Decision 80

- An individual had concerns about the care provided to her husband at a public hospital
- Also believed that during the hospital's investigation, the doctor breached husband's privacy by speaking to a third party about his care
- Concerns raised in complaints to the hospital and the CPSO
- Health Professions Appeal and Review Board affirmed the CPSO's decision
- Unsatisfied, the individual filed a complaint with the IPC under *PHIPA*
- IPC found there was no need for a review as the matter had already been appropriately dealt with by CPSO/HPARB

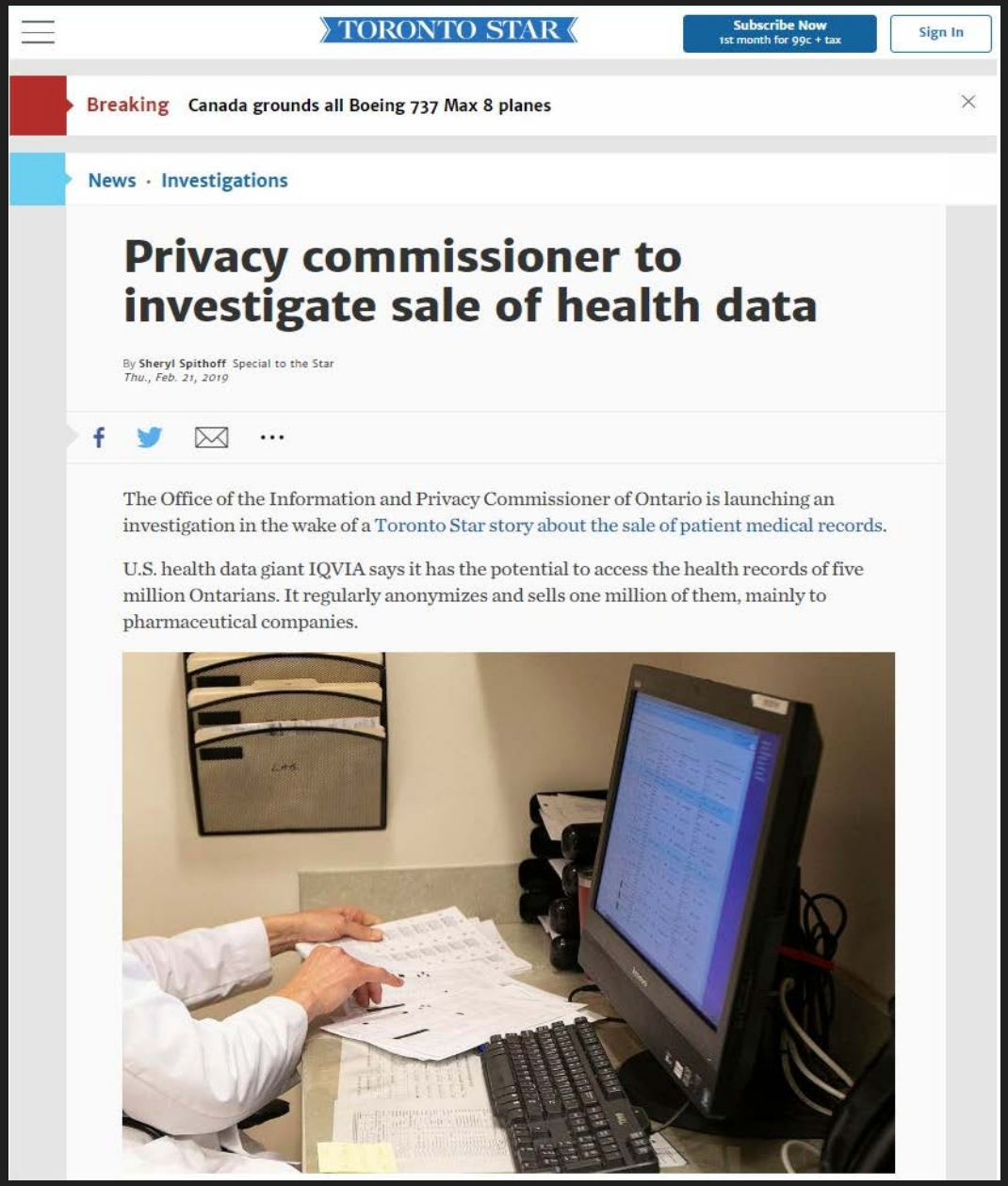
Comments to the Media – Authorized or not?

PHIPA Decision 82

- A hospital responded to media requests for information about a deceased patient who had been the subject of a decision by the Health Professions Appeal and Review Board
- Patient's family complained that the hospital's statements contravened *PHIPA* by disclosing the patient's health information without consent.
- IPC found that repetition of facts about the patient, when taken from the published decision of the HPARB, is not a disclosure under *PHIPA*
- We also found that some of the hospital's statements went beyond the board decision and were considered unauthorized disclosures

"The article indicates that information from patient records is being provided to private sector organizations. We have reason to believe that these arrangements may be contrary to the law."

— IPC statement to the Star



TORONTO STAR

Subscribe Now
1st month for 99¢ + tax

Sign In

Breaking Canada grounds all Boeing 737 Max 8 planes

News · Investigations

Privacy commissioner to investigate sale of health data

By **Sheryl Spithoff** Special to the Star
Thu., Feb. 21, 2019

The Office of the Information and Privacy Commissioner of Ontario is launching an investigation in the wake of a Toronto Star story about the sale of patient medical records.

U.S. health data giant IQVIA says it has the potential to access the health records of five million Ontarians. It regularly anonymizes and sells one million of them, mainly to pharmaceutical companies.

- A CBC Marketplace investigation revealed that a Toronto plastic surgeon, Dr. 6ix, may have been filming patients in states of undress without their consent
- A surveillance camera was discovered in one of the consultation rooms
- He is now under investigation by both the College of Physicians and Surgeons of Ontario and our office

MARKETPLACE

'It's creepy': Security cameras spotted in plastic surgeon's consult room

Marketplace investigation sparks probes by Ontario privacy commissioner and College of Physicians and Surgeons

Caitlin Taylor, Makda Ghebreslassie · CBC News ·
Posted: Dec 14, 2018 4:00 AM ET | Last Updated: December 14, 2018

What’s Coming

Bill 74, *The People's Health Care Act, 2019*

- Bill 74 will fundamentally change the way health care is delivered in Ontario
- The Ministry will have authority to integrate the health system in Ontario, including
  - power to dissolve certain organizations, including LHINs, eHealth Ontario and Cancer Care Ontario, and order the transfer of their functions to Ontario Health
  - designate integrated care delivery systems (also known as Ontario Health Teams) responsible for administration of integrated and coordinated health care in defined geographic populations or patient segments
- Creation of Ontario Health, a provincial agency responsible for implementing health system strategies and managing health service needs
- Bill 74 will have significant implications for privacy and access rights of Ontarians, but generally does not address those implications (e.g., no *FIPPA* or *PHIPA* designations)

Bill 74, *The People's Health Care Act, 2019*

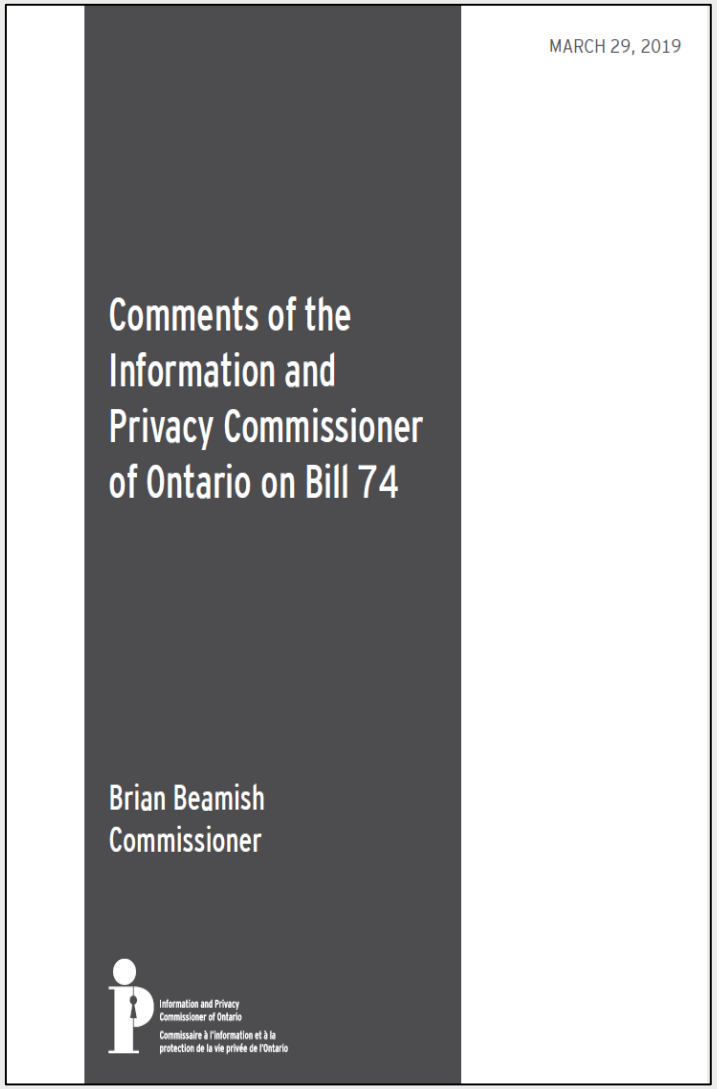
Cont'd

- Ontario Health will perform functions of a government institution
  - including functions of organizations that could be transferred to Ontario Health, who currently operate as government institutions within the meaning of *FIPPA*
- Ontario Health will also be involved in the delivery of health care, including the collection, use and disclosure of PHI to perform its functions
  - organizations that could be transferred to Ontario Health currently have various designations under *PHIPA*
    - prescribed entities
    - prescribed persons
    - health information custodians
    - electronic service providers
    - agents of health information custodians
    - health information network providers
- Ontario Health Teams will be involved in providing coordinated and integrated care to patients, including sharing of PHI for care, planning and quality improvement, and shared electronic systems and interoperable digital technologies

Bill 74, *The People's Health Care Act, 2019*

Cont'd

- Need a privacy and access rights framework that also addresses accountability and transparency of Ontario Health and Health Teams
  - make appropriate designations under *FIPPA* and *PHIPA*
  - ensure that PHI Ontario Health collects, uses or discloses for different purposes is retained separately, keeping its multiple functions logically separate
  - require secure transfer as transitions are carried out
  - provide notice to affected individuals where appropriate
  - ensure that *FIPPA* applies to records transferred to an institution, since Ontario Health will be relying on all transferred records to perform its functions



Child, Youth and Family Services Act

- The *CYFSA* received Royal Assent on June 1, 2017
- Part X of the *CYFSA* was proclaimed along with the rest of the CYFSA on April 30, 2018, but will come into effect on January 1, 2020
- Part X of the *CYFSA* represents a big step forward for Ontario's child and youth sectors:
  - closes a legislative gap for access and privacy
  - promotes transparency and accountability

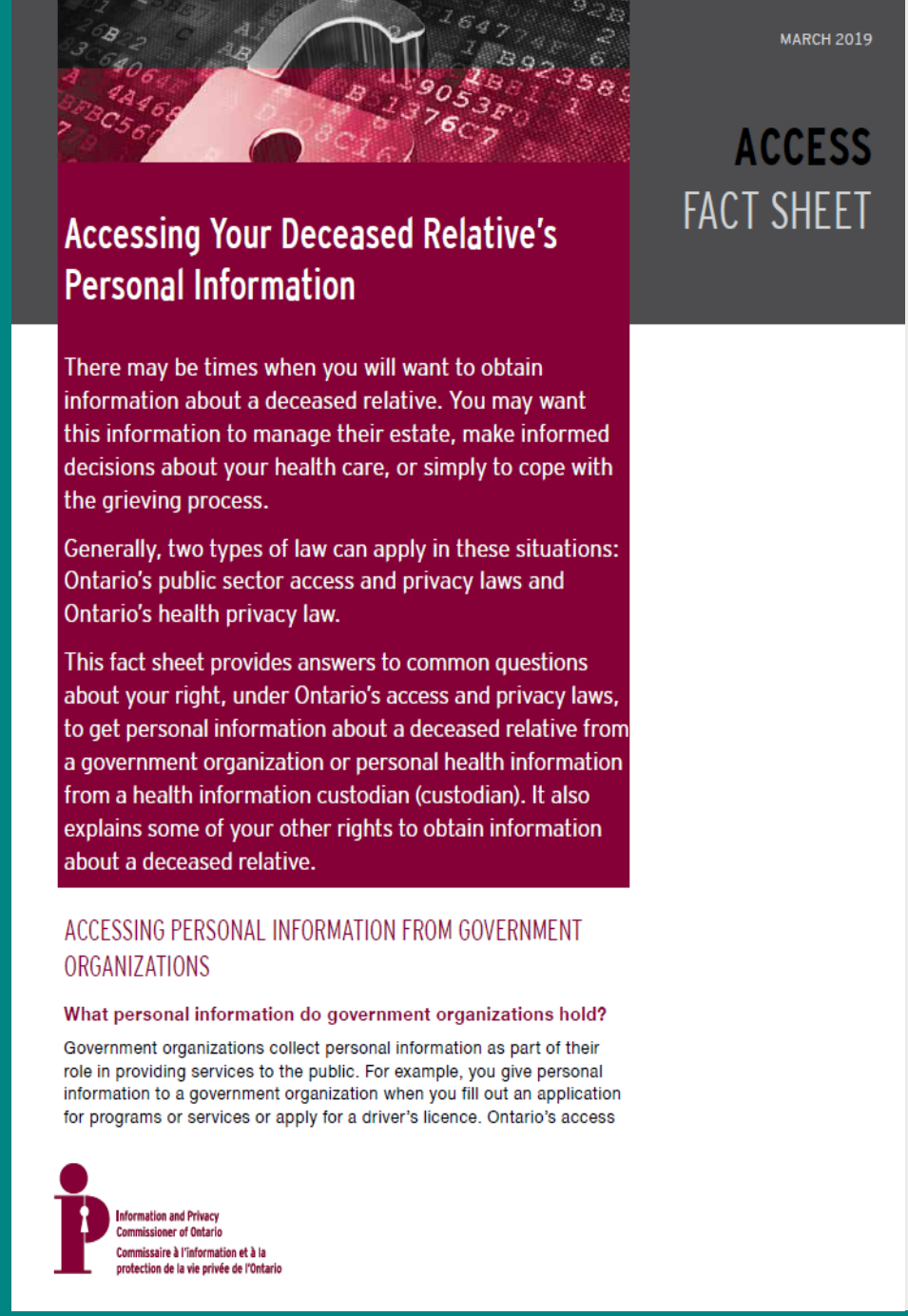
Guidance from the IPC on the *CYFSA*

- Current:
  - Frequently Asked Questions: Part X (Personal Information)
- Upcoming:
  - Guidance document – early May
  - Webinar – June 6
  - Two fact sheets – Fall 2019
    - Access: Process
    - Access: Rights and Exceptions

All the above can be accessed on our website: www.ipc.on.ca

Accessing the Personal Information of Deceased Relatives

- This fact sheet provides answers to common questions about accessing personal information about a deceased relative from a government organization or a health information custodian in Ontario.
- Generally, two types of law can apply in these situations:
  - Ontario's public sector access and privacy laws
  - Ontario's health privacy law.



What We are Working On

- **Genetic information** – factors to consider before increasing its availability through shared electronic systems
- **Abandoned records** – reducing the risk through succession planning prior to planned or unforeseen changes in practice
- **Consumer health apps** – what to consider before asking patients to use apps to manage their health care and access their personal health information
- **Updating *PHIPA* documents** – we are updating our *PHIPA* documents to reflect IPC decisions, legislative amendments, and evolving best practices

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