PHIPA Year In Review

Sherry Liang

Assistant Commissioner, Tribunal

Information and Privacy Commissioner of Ontario

Information and Privacy Commissioner of Ontario

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

PHIPA Summit

December 3, 2019

Agenda

- Mandatory Breach Reporting under PHIPA
- Annual Statistical Reporting under PHIPA in 2018
- Significant PHIPA Decisions in 2019
- PHIPA Guidance
- What's Ahead for 2020

Mandatory Breach Reporting under PHIPA

Summary of breaches reported to the IPC since January 2018

Mandatory PHIPA Breach Reporting

- As of Oct 1, 2017, custodians must notify the 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 a college or non-college member
  - Significant breaches

When You May Not Need to Report a Breach

You may not need to report a breach if:

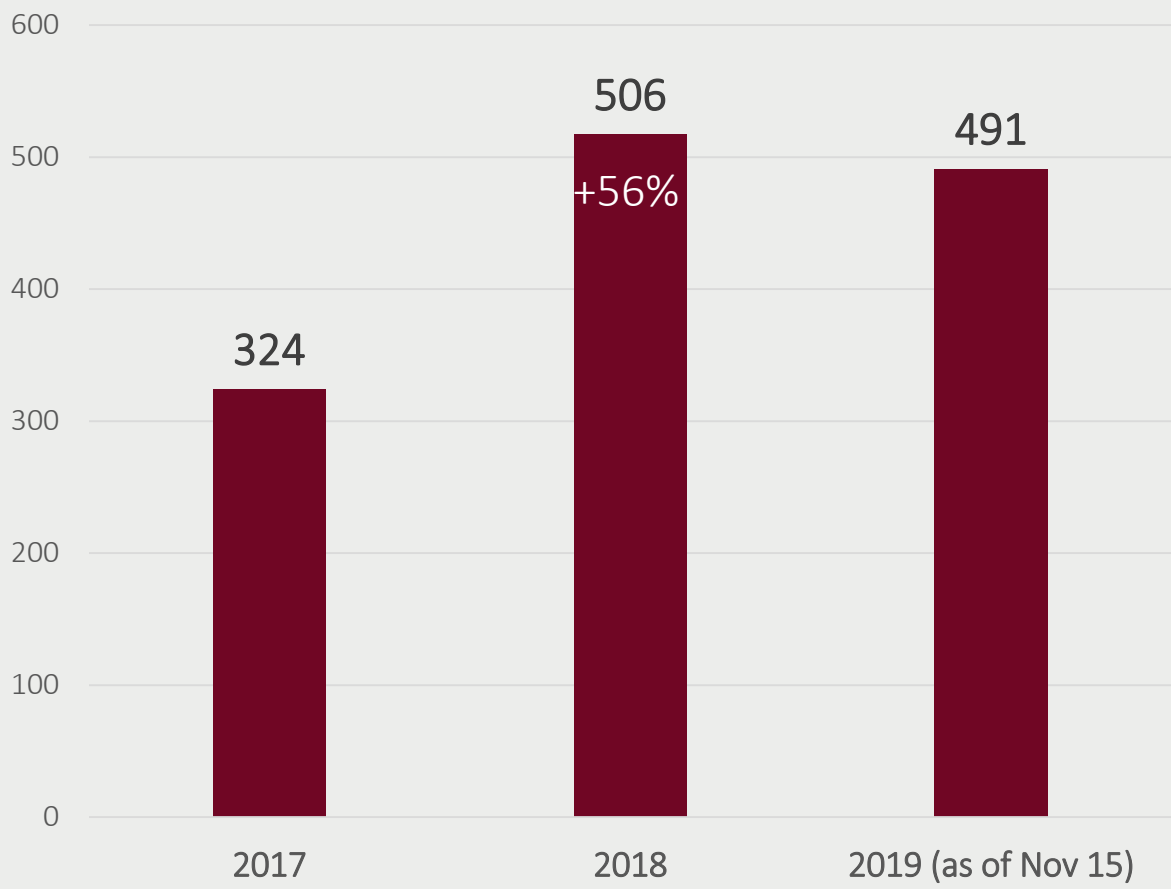
- It is not intentional
- It is a one-off incident
- It is not part of a pattern

When You May Not Need to Report a Breach

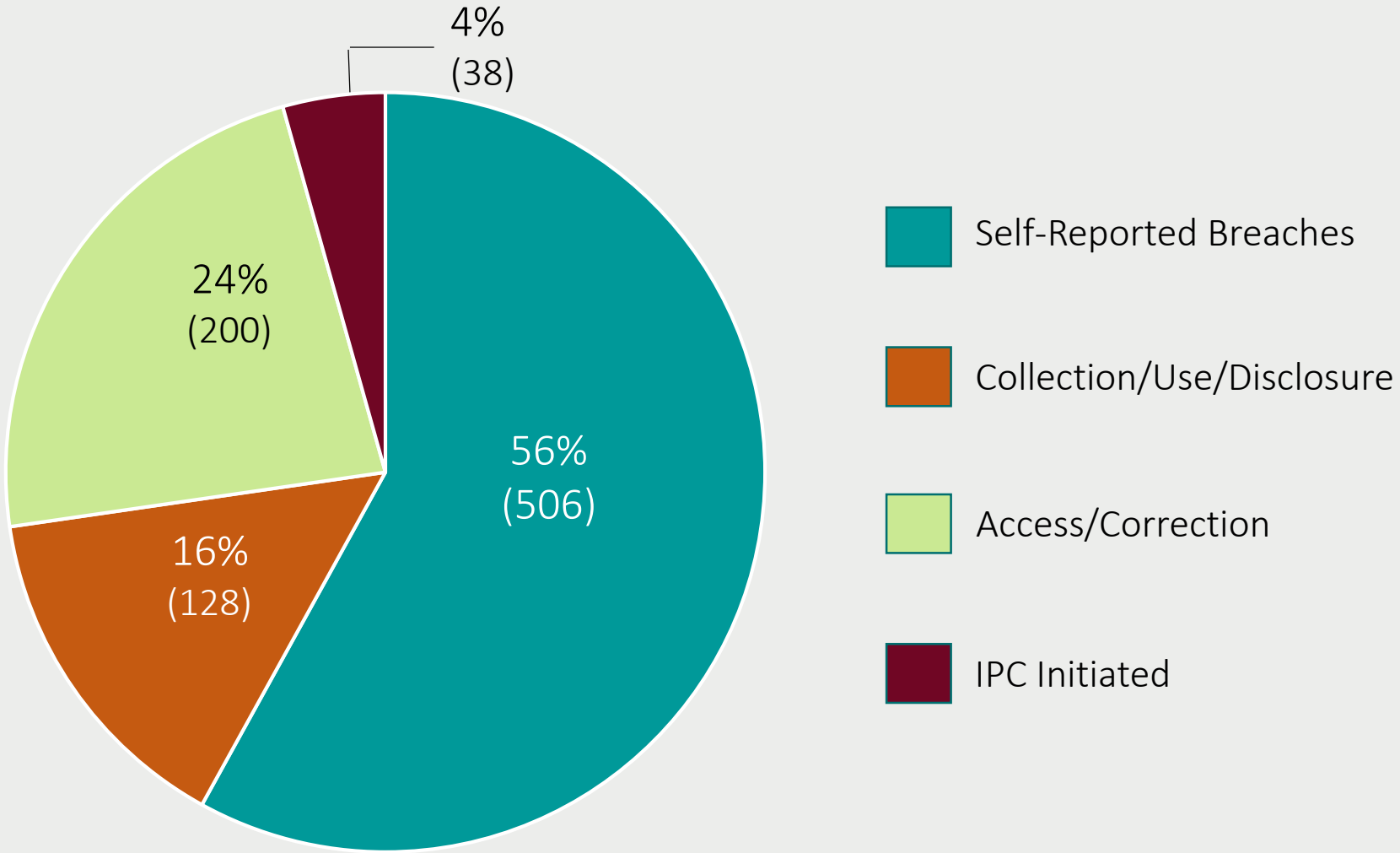
- Not every breach is significant
  - Mailing error
  - Faxing error
- Not every mistake is a breach, for example:
  - Nurse clicks on the wrong patient file
  - Records clerk opens the wrong file folder
  - Doctor walks into the wrong patient room
- BUT if you start to see repeated minor breaches or mistakes, this may indicate a broader and more significant issue that you should investigate

Self-Reported Breaches Before and After Mandatory Breach Reporting

- 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



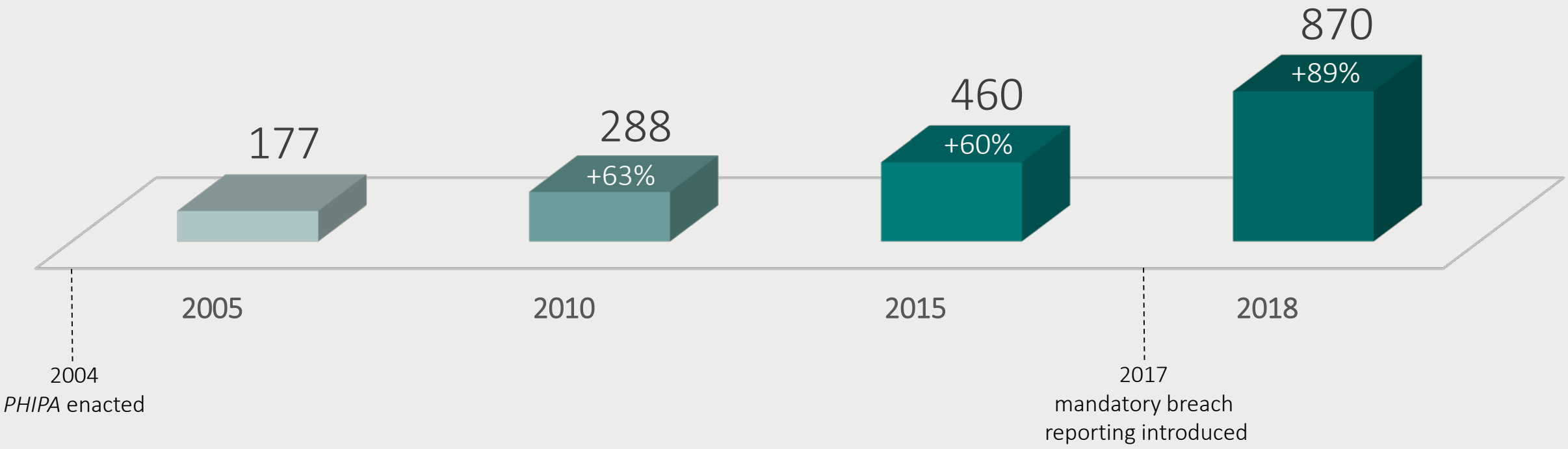
Health Sector Privacy Files in 2018



PHIPA Files Opened by Year

Includes:

- Privacy and access complaints
- Self-reported breaches
- Commissioner initiated files



Annual Statistical Breach Reporting under PHIPA in 2018

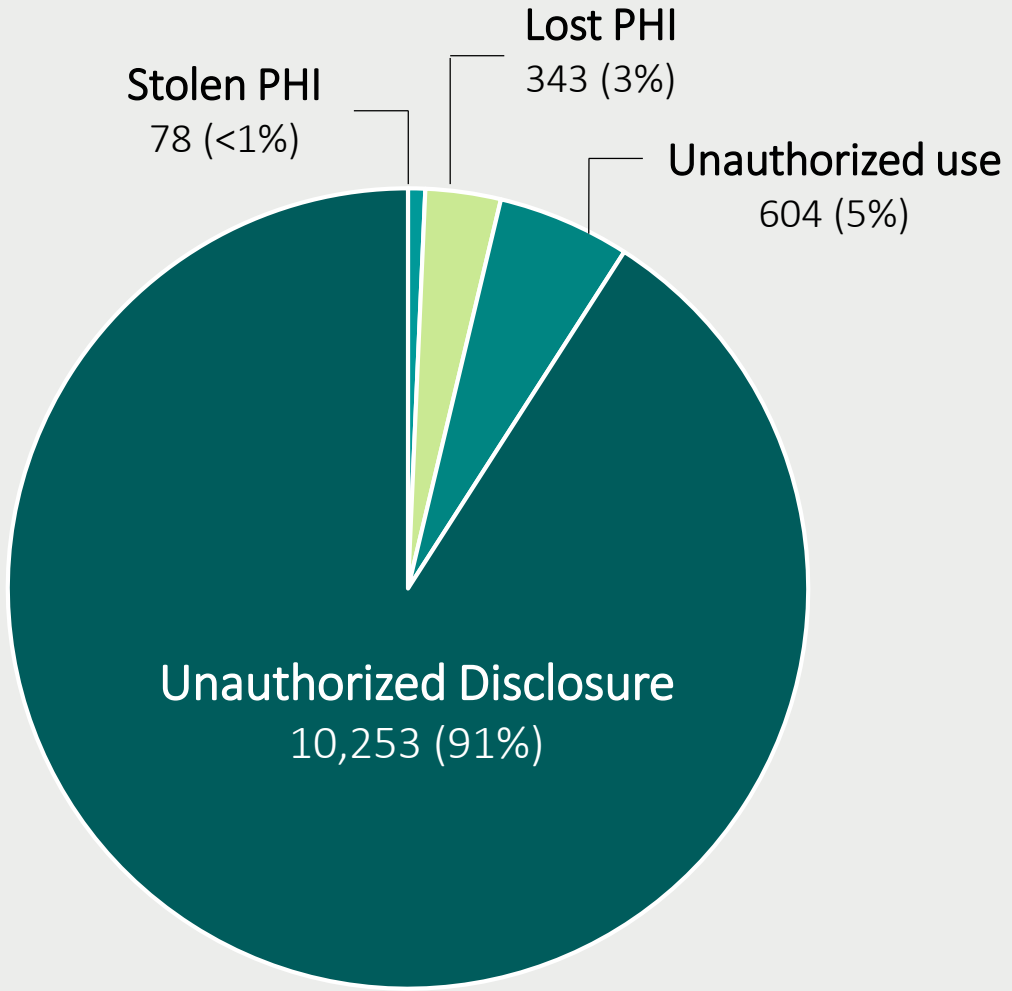
Summary of the first year of annual statistical breach reporting to the IPC

PHIPA Annual Statistical Breach Reporting

- Custodians must submit breach statistics to the IPC every year – the first reports were received in March 2019.
- Annual statistical reports must include breaches where information was:
  - Stolen
  - Lost
  - Used without authority
  - Disclosed without authority
- This includes breaches that did not meet the criteria for mandatory point-in-time reporting to the IPC
  - Rule of thumb – if it met the threshold to notify the patient, the breach should be included in statistical report

2018 Annual Statistical Breach Reporting

- There were 11,278 incidences of health breaches reported to our office in 2018.
- Over half of all reported breaches were misdirected faxes (56.5% or 6,381 in total).



Significant PHIPA Decisions in 2019

Summary of six PHIPA decisions issued by the IPC in 2019

No Review Where Complaint Dealt With Elsewhere

PHIPA Decision 80

- An individual had concerns about the hospital care provided to her husband.
- She believed that during the hospital's investigation, the doctor breached her husband's privacy by speaking to a third party about his care.
- Complaints were made to the hospital and the College of Physicians and Surgeons of Ontario (CPSO).
- The Health Professions Appeal and Review Board (HPARB) affirmed the CPSO's decision.
- Unsatisfied, the individual filed a complaint with the IPC under *PHIPA*.
- The IPC found that 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 HPARB.
- The 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, when taken from the published decision of the HPARB, is not a disclosure under *PHIPA.*
- However, some of the hospital's statements went beyond the board decision and were considered unauthorized disclosures.
- The hospital was directed to amend its policies to include a definition of "personal health information" to include information about unnamed patients if they could be identified by members of the public.

Unintentional Unauthorized Access

PHIPA Decision 84

- An individual believed that a physician and other hospital staff inappropriately accessed her personal health information.
- The hospital conducted a number of audits and communicated the results to the patient – she subsequently requested access to the audit reports.
- The adjudicator found that the accesses were for the purpose of providing or assisting in providing health care to the individual but that the physician inadvertently clicked on more tabs in the electronic medical record than was needed.
- The adjudicator concluded that the physician's access did not constitute an intentional unauthorized access – therefore, no order was issued.

Discretionary Disclosure to Non-Custodial Parent

PHIPA Decision 96

- A non-custodial father appealed a denied request for information about services that his children received.
- Since the father only had a right of access to the children, and was not their substitute decision-maker, he could not exercise a right of access to their records of personal health information.
- The adjudicator found that the custodian had a duty to consider the father's request as a request for disclosure, as well as access, because the father asserted that:
  - he had the mother's consent
  - there was a court order that entitled him to the information
  - provisions of other statutes entitled him to the information
- The adjudicator ordered the custodian to consider the father's request for discretionary disclosure of his children's personal health information.

Surveillance Recordings in Examination Rooms

PHIPA Decision 98

- The IPC was contacted by a media outlet about the use of surveillance cameras in the examination rooms of a cosmetic surgery clinic.
- The clinic operated a network of 24 security cameras that recorded 24 hours a day in examination rooms, the operating room, pre-operative room, as well as in reception and administrative areas of the clinic.
- The central purpose of the camera system was not for health care but for the security of the clinic, staff and patients.
- IPC found that, although the clinic had some valid security concerns, they did not justify such broad-scale, intrusive measures.

Surveillance Recordings in Examination Rooms

Cont'd

PHIPA Decision 98

- The IPC found that the clinic's prior practices contravened *PHIPA* but that the clinic has since addressed these issues by:
  - limiting hours and number of cameras,
  - not recording personal health information,
  - confirming destruction of all footage recorded prior to Jan 2019 (except footage seized by the CPSO),
  - advising of the clinic's intention to securely destroy any footage seized by the CPSO upon conclusion of the CPSO proceeding (subject to any legal obligations), and
  - improving notices and committing to amend its privacy policies and consent forms.

Shared Systems

PHIPA Decision 102

- The IPC received breach reports from three separate custodians about privacy breaches involving a shared electronic patient information system.
- The IPC decided to take a broader look to assess whether the breaches raised common and systemic issues across the shared system.
- The breaches largely involved unauthorized accesses of personal health information of family members, friends, or ex-spouses of an agent or high-profile patients.

Shared Systems

Cont'd

PHIPA Decision 102

- The decision describes the risks of shared systems:
  - Custodians generally do not have sole custody or control of personal health information in a shared system.
  - Shared custody and control can pose unique challenges for *PHIPA* compliance
    - for example, there can be confusion around which custodian is required to notify the individual of a privacy breach.
  - There can be increased risk of unauthorized use and disclosure because, typically, participating custodians and their agents have potential access to all information in the shared system.
  - Shared systems may also attract hackers and others with malicious intent because of the significant amount of information.

Shared Systems

Cont'd

PHIPA Decision 102

- The IPC's investigation found issues with respect to staff training, consistent auditing practices and timely notification of breaches.
- While deficiencies were found, the custodians agreed to address the issues – no further review was warranted.
- One of the custodians is a health information network provider (HINP) responsible for the shared system.
- Decision discusses specific and additional obligations of HINPs.

Shared Systems

Cont'd

PHIPA Decision 102

Lessons Learned for Shared Systems

- All custodians within a shared system should have harmonized policies and procedures that, among other things, address access to the shared system by agents and how breaches will be handled.
- Privacy training of all agents should be tracked and occur before access is provided to the shared system - the training should be consistent across all custodians.
- The signing of confidentiality agreements by all agents should be tracked and occur before access is provided to the shared system.
- Auditing should be consistent among all custodians and include a standard for the type of data displayed.

PHIPA Guidance

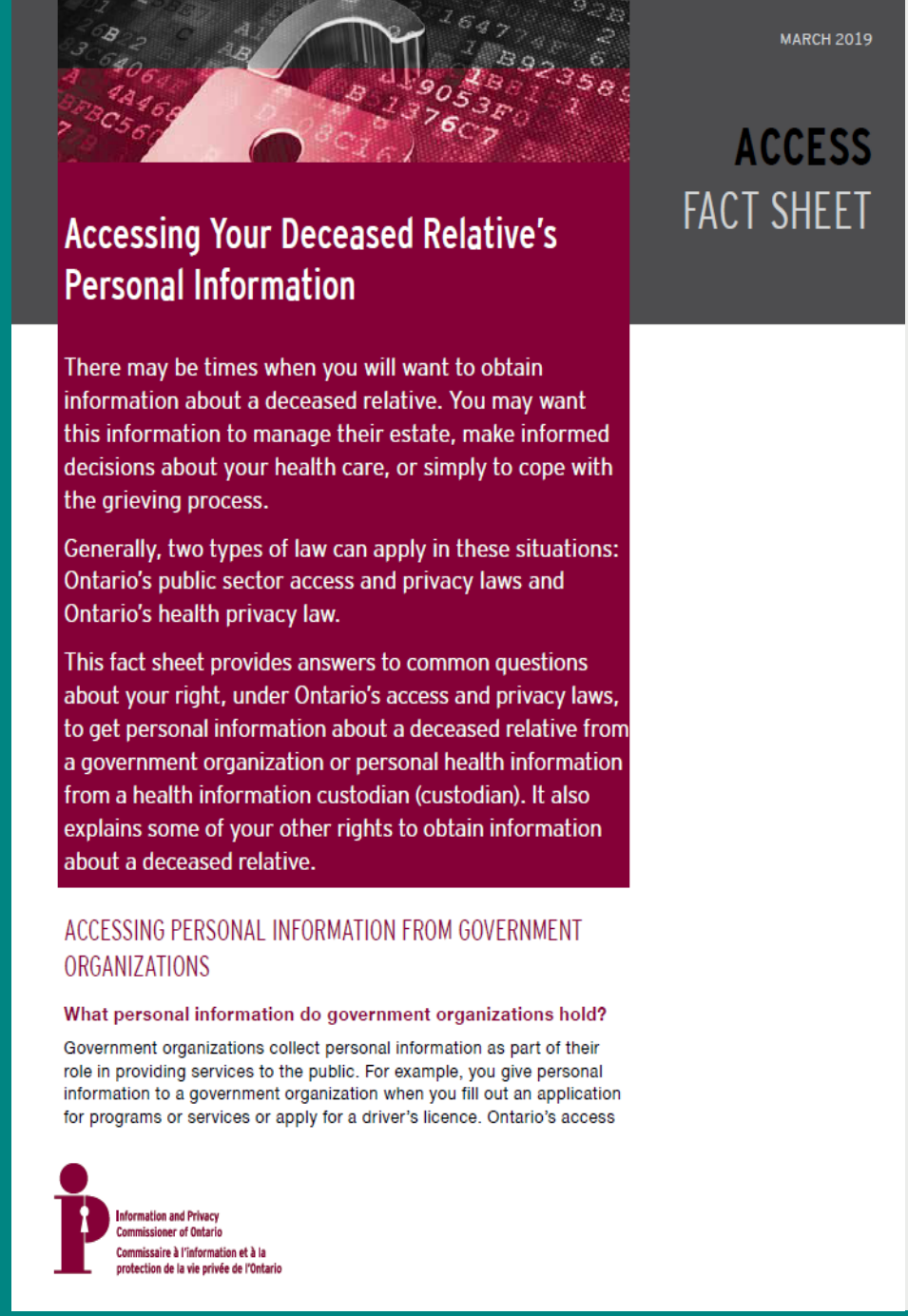
Highlights of guidance issued in 2019

Avoiding Abandoned Records

- **Who is the custodian?**
  - in the event of death, bankruptcy, or transfer
  - in a group practice
- **What obligations do custodian have?**
  - Retain, transfer & dispose of records securely
  - Take reasonable steps to prevent privacy breaches
  - Notify individuals of a transfer
- **How to avoid abandoned records?**
  - succession plans set out roles and responsibilities

Accessing the Personal Information of Deceased Relatives

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



MARCH 2019

ACCESS
FACT SHEET

Accessing Your Deceased Relative's Personal Information

There may be times when you will want to obtain information about a deceased relative. You may want this information to manage their estate, make informed decisions about your health care, or simply to cope with the grieving process.

Generally, two types of law can apply in these situations: Ontario's public sector access and privacy laws and Ontario's health privacy law.

This fact sheet provides answers to common questions about your right, under Ontario's access and privacy laws, to get personal information about a deceased relative from a government organization or personal health information from a health information custodian (custodian). It also explains some of your other rights to obtain information about a deceased relative.

ACCESSING PERSONAL INFORMATION FROM GOVERNMENT ORGANIZATIONS

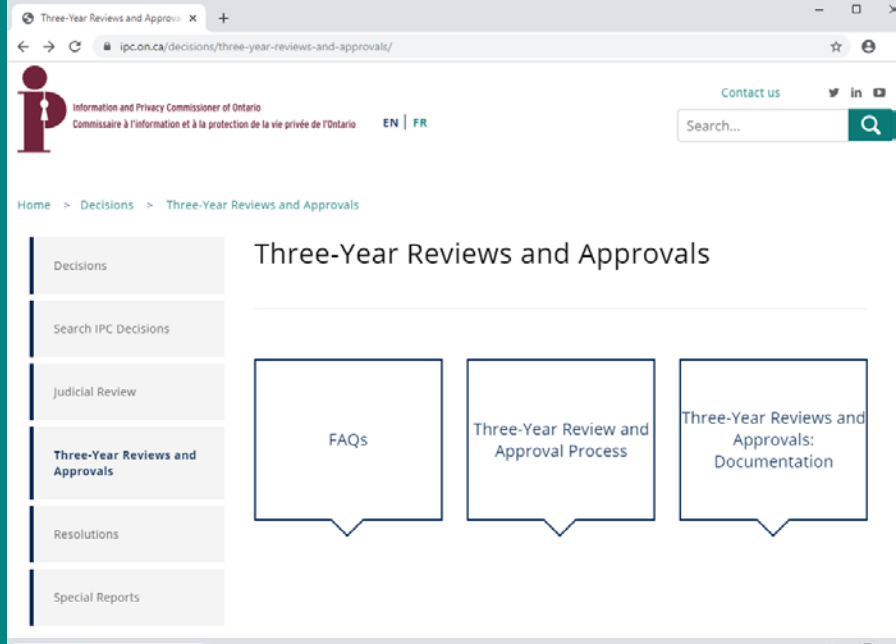
What personal information do government organizations hold?

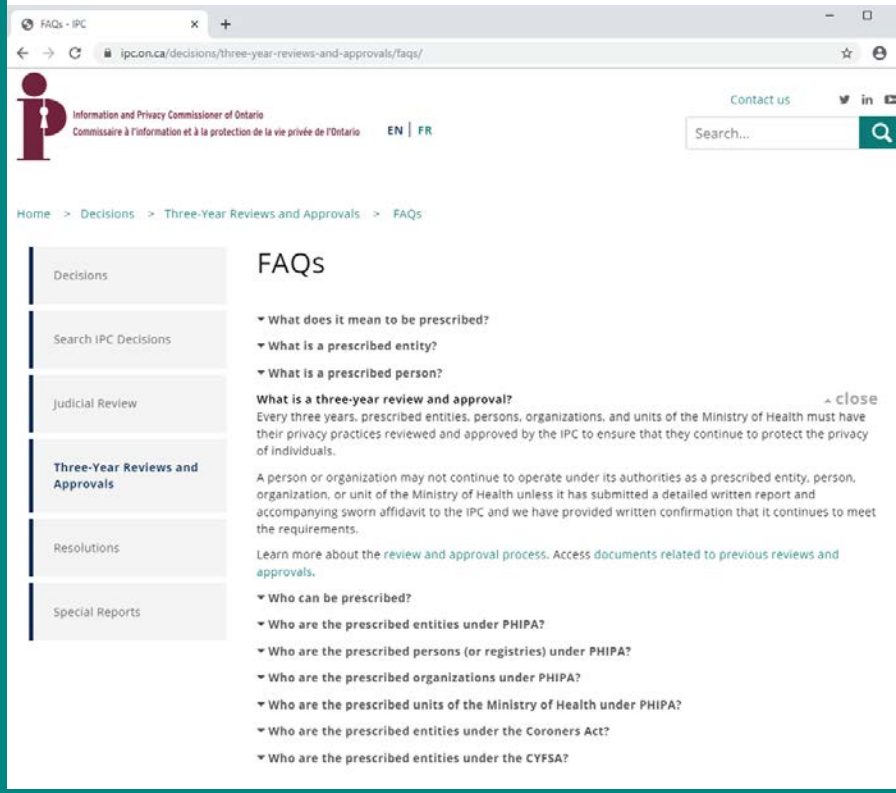
Government organizations collect personal information as part of their role in providing services to the public. For example, you give personal information to a government organization when you fill out an application for programs or services or apply for a driver's licence. Ontario's access

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

Three-Year Review Webpages

- These webpages provide plain language information about the Three-Year Reviews under *PHIPA*, the *Child Youth and Family Services Act (CYFSA),* and the *Coroners Act*.
- Learn about what is means to be prescribed under these laws, who is currently prescribed, the process of becoming prescribed, and documentation related to previous reviews and approvals.
- https://www.ipc.on.ca/decisions/three-year-reviews-and-approvals/





What’s Ahead for 2020?

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
- Core provisions of Part X do not apply to personal health information held by HICs covered by *PHIPA*

What's Ahead for 2020

- **Three-Year Review of Prescribed Entities and Prescribed Persons under *PHIPA* –** Our office is currently conducting reviews of four prescribed entities and six prescribed persons under *PHIPA.*
- ***PHIPA* Poster and Brochure** – updated poster and brochure that may be used to supplement materials offered in custodians' offices.
- **Disclosure of Personal Health Information to Law Enforcement –** guidance that describes situations where custodians can disclose personal health information to a law enforcement agency under *PHIPA.*
- **Updated Fax Guidelines –** our current guidelines will be updated in light of the high number of fax-related breaches reported to our office last year.
- **Guidance for Researchers and Research Ethics Boards** –guidance on complying with *PHIPA* requirements for researchers and research ethics boards.
- **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