Breach Reporting to the IPC under PHIPA

Warren Mar, Assistant Commissioner, Tribunal and Dispute Resolution

Suzanne Brocklehurst, Director of Early Resolution

Office of the 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

CELHIN

May 24, 2024

Overview

- About the IPC
- About the Tribunal
- Early Resolution Department (the first and usually last stop for reported breaches)
- When and how to report a breach
- What to expect from the IPC
- Reporting Significant Breaches, with many Affected Parties
- Administrative Monetary Penalties – what does this mean when reporting a breach?
- Questions?

Information and Privacy Commissioner of Ontario

Patricia Kosseim

Ontario's Information and Privacy Commissioner is an officer of the legislature

- Appointed by and reports to the Legislative Assembly of Ontario
- Independent of the government of the day

The IPC has authority under the following laws:

- *Freedom of Information and Protection of Privacy Act* (FIPPA)
- *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA)
- *Personal Health Information Protection Act, 2004* (PHIPA)
- *Child, Youth and Family Services Act, 2017* (CYFSA)
- *Anti-Racism Act, 2017* (ARA)
- *Coroners Act*

IPC Role and Mandate

In addition to overseeing provincial access and privacy laws, the office of the IPC also serves the government, public institutions and the public through its mandate to:

- Resolve appeals when access to information is refused
- Investigate privacy complaints related to personal information
- Ensure compliance with the province's access and privacy laws
- Review privacy policies and information management practices
- Conduct research on access and privacy issues and provide comment on proposed legislation and government programs
- Educate the public, media and other stakeholders about Ontario's access and privacy laws and current issues affecting access and privacy

IPC Vision of a Modern and Effective Regulator

Statistics for 2021

ACCESS

- In 2021, service providers reported completing almost 72% of access requests within 30 days

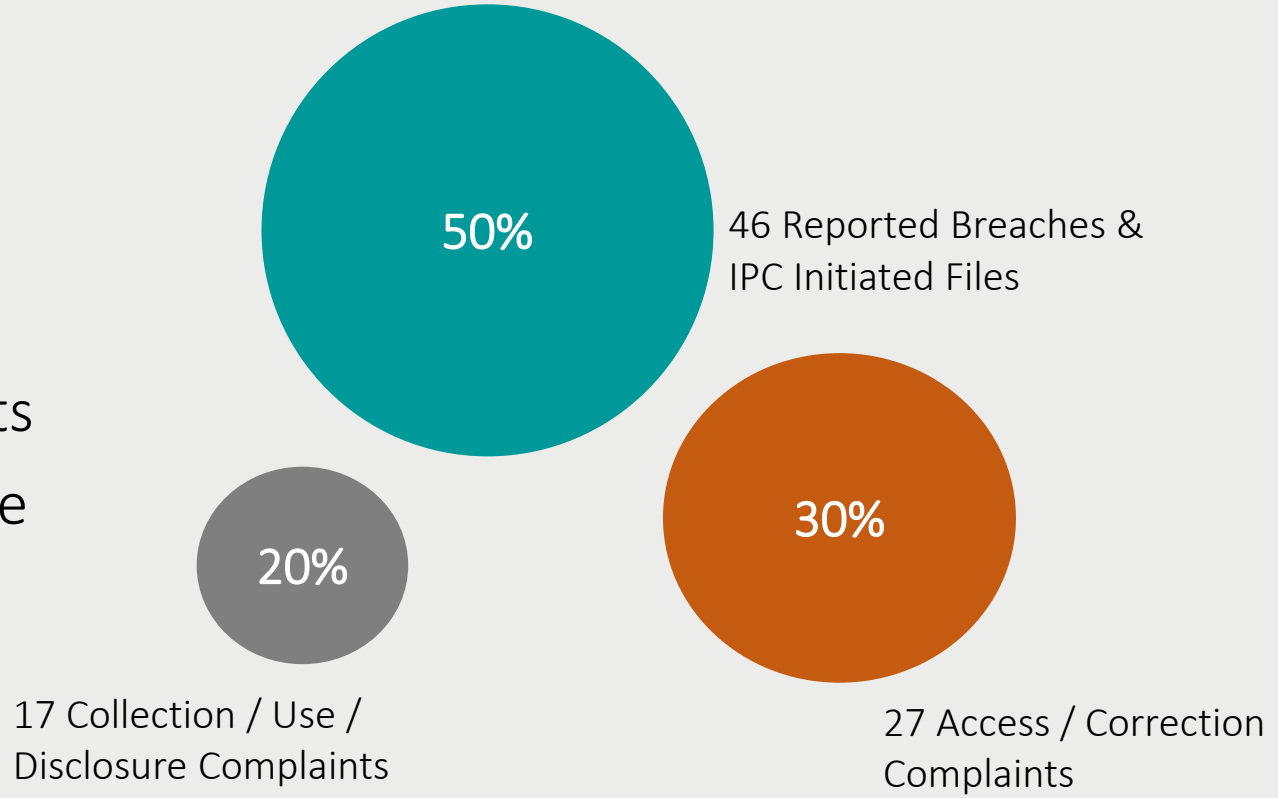
PRIVACY

- Service providers reported experiencing 508 privacy breaches in 2021 (77 of which were reported to IPC)
- Majority of breaches arose out of misdirected emails or mail
- CAS's reported experiencing 348 breaches
- Indigenous well-being societies reported experiencing 103 breaches

Currently 80 open files with IPC: 37 access/correction complaints; 27 privacy complaints; 16 self-reported breaches

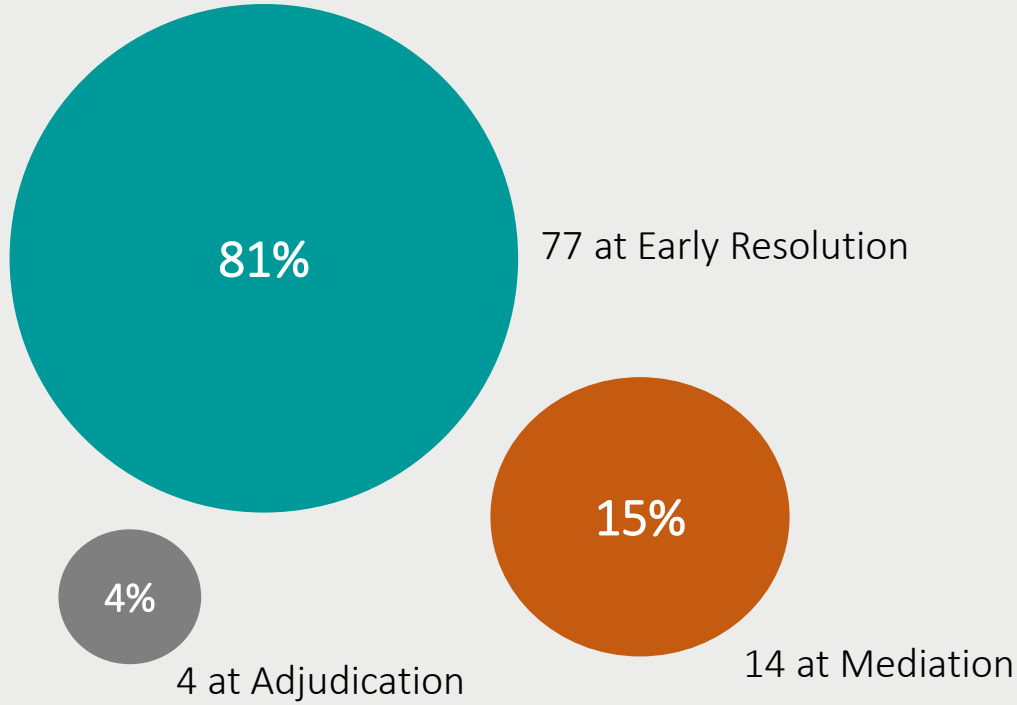
2022 CYFSA Tribunal stats: Files opened

- **92** CYFSA files opened
  - 46 reported breaches
  - 27 access/correction complaints
  - 17 collection/use/disclosure complaints
  - 2 IPC initiated collection/use/disclosure complaints

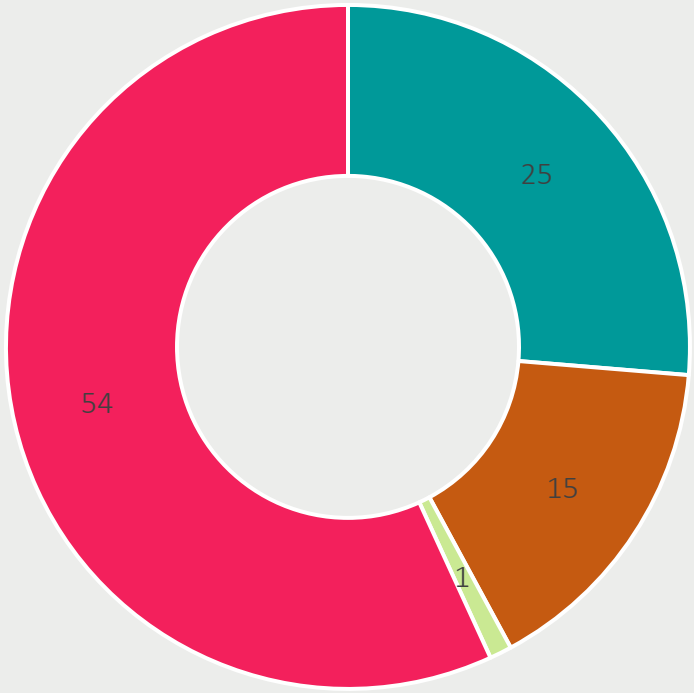


2022 CYFSA Tribunal stats: Files closed

- **95** CYFSA files closed
  - 77 resolved at early resolution
  - 14 resolved at mediation
  - 4 resolved at adjudication



Types of File Closed in 2022



- Access/Correction Complaint
- Collection/Use/Disclosure Complaint
- IPC Initiated Collection/Use/Disclosure Complaint
- Reported Breach

2022 CYFSA Tribunal stats: Breaches

- 46 breaches reported to our office:
  - 16 misdirected or lost personal information
  - 16 general unauthorized collection, use or disclosure
  - 8 snooping
  - 1 cyberattacks
  - 2 ransomware
  - 3 lost or stolen mobile devices

IPC Tribunal complaint process

Early Resolution

- The goal of the early resolution stage is to resolve matters quickly and efficiently to the satisfaction of the IPC

OR

- To consider if the matter should proceed further through the complaint process, or if it should be dismissed

Early Resolution

- A matter may be resolved at the Early Resolution stage in the following circumstances:
  - The analyst is satisfied, based on a review of the information gathered from the parties, that the service provider has responded adequately to the complaint
  - The complainant is in agreement

Early Dismissal

- Analysts have delegated authority to dismiss complaints in certain circumstances. For example:
  - The Service Provider has responded adequately to the complaint (i.e., the collection, use or disclosure was permitted, or the breach occurred and the SP has taken reasonable steps to mitigate)
  - The complaint has been or could be more appropriately dealt with by another means
  - The length of time that has elapsed since the subject-matter of the complaint arose and the date the complaint was made is such that a review would likely result in undue prejudice to any person
  - There is a jurisdictional issue

When early resolution is not possible

What Happens Next?

Investigation or Mediation?

Investigations

- Self reported breaches
- Systemic privacy issues

Mediation

- Privacy complaints from individuals
- Access & correction complaints of individuals

Investigation

- **Self reported breaches or systemic privacy issues** that cannot be resolved at Intake
- Role of investigator:
  - **Requests and reviews documents** and information relevant to privacy issues
  - **Works with service provider** to ensure adequate steps are taken to fully respond to the breach and prevent a reoccurrence
- If satisfied, investigator will close the file with a decision

Role of Mediator

- **Neutral** third party
- **Not a decision-maker/cannot dismiss** complaints
- **Clarifies** and confirms **issues** under appeal
- **Educates parties** about complaint process, legislation, IPC decisions
- **Reality checks** parties based on previous decisions
- **Works with parties** with a **goal of narrowing** and ideally **resolving** the complaint in whole or part

What are the odds?

Excellent!

- Approximately **80%** of access appeals under *FIPPA* & *MFIPPA* **resolve** in whole or part

- In 2022, 96% of CYFSA files were resolved or dismissed at Early Resolution or Mediation

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.

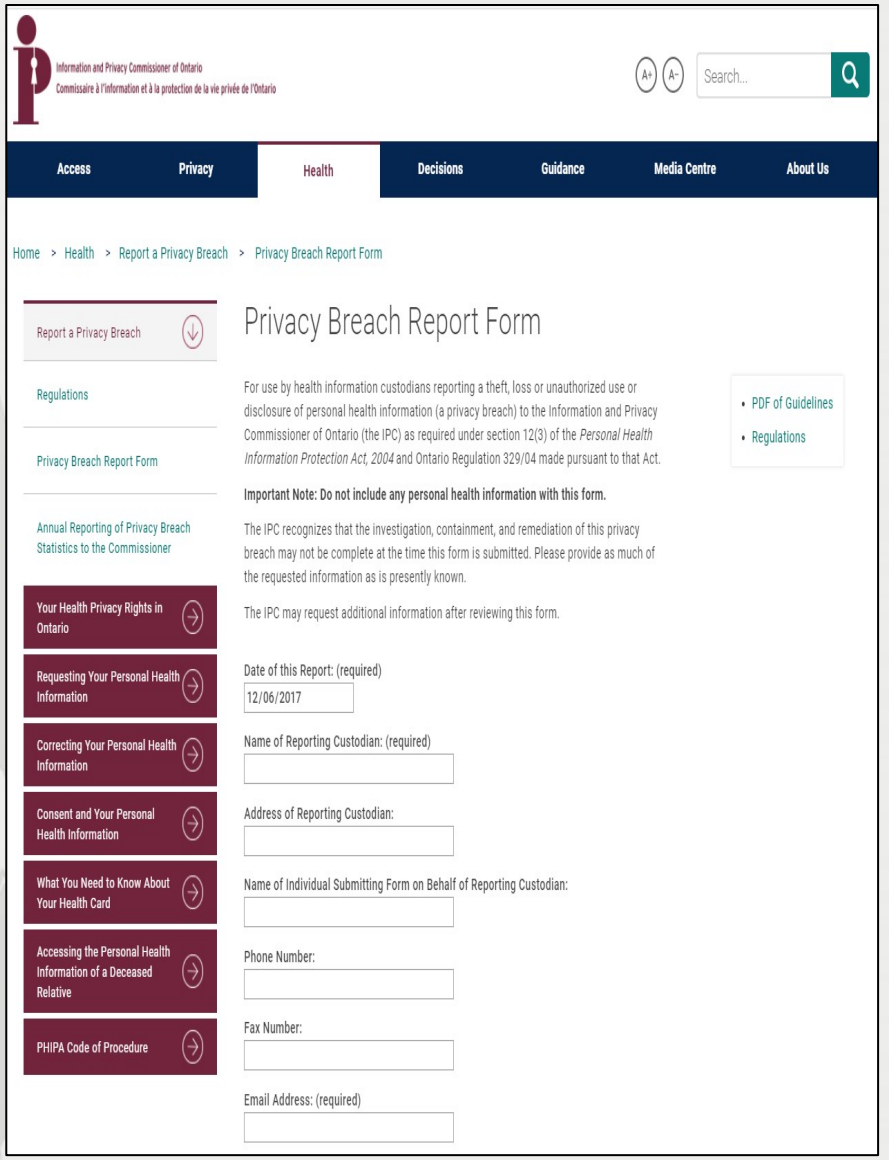
iv. Whether more than one health information custodian or agent was responsible for the loss or unauthorized use or disclosure of the personal health information.

IPC Privacy Breach Online Report Form

Although you can report breaches by mail or fax, we recommend that you use our online report form.

You will be asked to provide:

- a description of the breach
- steps taken to contain the breach
- steps taken to notify affected individuals
- steps taken to investigate and remediate the breach



REACHING OUT TO ONTARIO

You reported a breach to the IPC. What happens next?

- A notice will be sent that reflects the type of breach reported
- A response to the notice will be requested
- Additional information is required for “snooping” breaches
- Most breaches are resolved at the intake stage when the custodian demonstrates it has taken the steps necessary to notify affected parties, contain the breach and prevent future breaches.

Context for introduction of AMPs

- In 2016, 2019 and 2020, the Government made major amendments to PHIPA
- Government had progressively increased punishments for conviction in court of a PHIPA **offense**:
  - 2016: fines doubled to $100,000 (individuals) and $500,000 (organizations)
  - 2020: fines doubled again
  - 2020: imprisonment of up to one year
- However, there have been very few prosecutions under PHIPA
  - Still under 10 prosecutions after 19 years' experience with the legislation
  - Time-consuming, expensive, and very hard to prove in court
- Legislation passed March 2020 allowing AMPs to be administered **by the IPC** as part of the IPC's order-making power
  - Regulation would specify how to determine amount of penalty
  - IPC could not use its authority without that Regulation
- Regulation came into effect on January 1, 2024

Offences vs. AMPs

Offences	AMPs
In PHIPA since 2004	Effective January 1, 2024
Prosecuted by the Attorney General	Imposed **directly by the IPC** as part of an order
For the contraventions listed at s. 72(1)	"if the Commissioner is of the opinion that the person has contravened this Act or its regulations"
Maximums: Individual: $200,000 and/or prison Organization: $1,000,000	Maximums: Individual: $50,000 Organization: $500,000

In the Act – Clause (h.1) was added to the list of order-making powers

Powers of the Commissioner

61 (1) After conducting a review under section 57 or 58, the Commissioner may,

…

(h.1) make an **order** in accordance with section 61.1 requiring any person whose activities the Commissioner reviewed to pay an **administrative penalty** in the amount set out in the order if the Commissioner is of the opinion that the person has contravened this Act or its regulations;

…

In the Act – Section 61.1

Section 61.1 sets out these basic rules for an order under clause 61 (1) (h.1) – that is, an order containing an AMP:

- ***Purpose of AMP:*** an AMP may be issued to
  - encourage compliance with PHIPA; or
  - prevent a person from deriving, directly or indirectly, any economic benefit as a result of contravening PHIPA
- ***Limitation period:*** Within two years of the day that the IPC first learned of the contravention.
- ***Details the order must contain:*** Description of the contravention and instructions on how/when to pay.
- ***Amount:*** The dollar amount of the penalty must "be determined by the Commissioner in accordance with the regulations made under this Act."

The Regulations

- Penalty of up to $50,000 for an individual and $500,000 for an organization
  - May be increased by the amount of the economic benefit received, to avoid treating the penalty as the "cost of doing business" – e.g., an individual making $1M from a large-scale breach could be penalized $1,050,000
- IPC must consider these factors when determining the amount:
  - Extent to which the contravention deviated from PHIPA and its requirements
  - Extent to which steps could have been taken to prevent the contravention
  - Extent of harm or possibility of harm resulting from the contravention
  - Extent to which attempts to mitigate the harm were made
  - Number of individuals and custodians (and other persons) affected by the contravention
  - Whether the person notified the IPC and people affected or not
  - Extent to which the person derived or reasonably could have derived economic benefit from the contravention
  - Whether the person previously contravened PHIPA
- The IPC may also consider any other factors that may be relevant to the case

Journey to AMP "activation"

- Commissioner's recommendation in two successive annual reports
- Extensive back and forth with Ministry of Health re: structure of regulation
- Maximum amounts and decision-making factors determined over time
- Worry about negative impacts on the sector – fear of penalties, reluctance to disclose data even where appropriate, possible "privacy chill"
- IPC publicly supportive of proposed regulation
- IPC agreed to prepare a guidance document
- IPC shared examples of some cases for which monetary penalties may have been appropriate [next slide]

Cases pre-AMPs that likely would have been considered

- Hospital birthing ward: employee shared contact information of new mothers for the purpose of trying to sell RESPs – breach for economic gain
- Doctor identified cases to refer to the doctor's spouse, who was a personal injury lawyer – breach for economic gain
- Individual went snooping in digital medical records thousands of time in one year – egregious, cumulatively large-scale breach of trust

Process considerations

- Identification:
  - Need to spot files that are possible candidates for AMPs early in the Tribunal process, e.g., serious snooping into patient records; contraventions for economic gain; disregard for a patient's right of access.
  - AMPs are **not** the default response to violations of PHIPA – option reserved for severe violations.
  - Just culture approach: apply statutory responsibilities in a way that balances the need for accountability and continuous learning; emphasizes the value of openly reporting and learning from errors that occur in complex systems, while reserving more severe consequences for cases where stronger interventions are necessary to ensure proper accountability.
- Timing:
  - Order requiring payment of AMPs **must** be issued within 2 years from the day the most recent contravention first came to the knowledge of the Commissioner.
  - Need to commence a review under PHIPA prior to making an order.
- Imposition:
  - If an order requires payment of an AMP, determining the quantum requires an analysis of the regulatory factors.
  - Need to be transparent in the order about how the factors are weighed when determining the quantum – procedural fairness / judicial review concerns.
- Enforcement:
  - Order requiring a person to pay an AMP must contain or be accompanied by a description of the contravention and set out the amount of the AMP to be paid and specify the time and manner of the payment – need to clear about when and how the AMP is paid.
  - AMP payment to the Minister of Finance, not the IPC.
  - Need to notify the Ministry of Finance about the imposition of an AMP to ensure payment and collection.
  - Under s. 63(3) of PHIPA, if an AMP is not paid in accordance with the terms of the order, it becomes a debt due to the Crown, and the Crown may recover the debt by action or by any other remedy available by law to the Crown for the collection of debts owed to the Crown – not the IPC's role to do collection or enforcement.

Lessons Learned / Things to be aware of

- Be aware of the extent to which introducing penalties makes things different:
  - For internal processes
  - For the sector itself
  - For the government/IPC relationship
  - For perceptions of the IPC because of this power
- Frequent communication and explanation to all levels of the relevant Ministry
  - Reluctance to hand this substantial power off to an organization outside its control
- Preparing the groundwork
  - Guidance (internal and external)
  - Internal understanding of what the authority will (and will not) be used for
  - Staffing appropriately (doesn't happen in a vacuum, not a simple absorption of a new authority)
    - E.g., two year rule means that Tribunal has to have a system in place to identify possible appropriate cases and "fast-track" them. How will that happen? Who is responsible for doing so? What needs to be done to make this happen? – AMPs project in place within the Tribunal to ensure the proper identification and processing of potential AMPs files.

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

My contact: jesse.campbell@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965