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

Navigating Today's Cybersecurity Threat Landscape: An IPC Perspective

17 January 2024

Fred Carter
Senior Policy & Technology Advisor

2nd Annual Update Privacy and Security Law and Practice

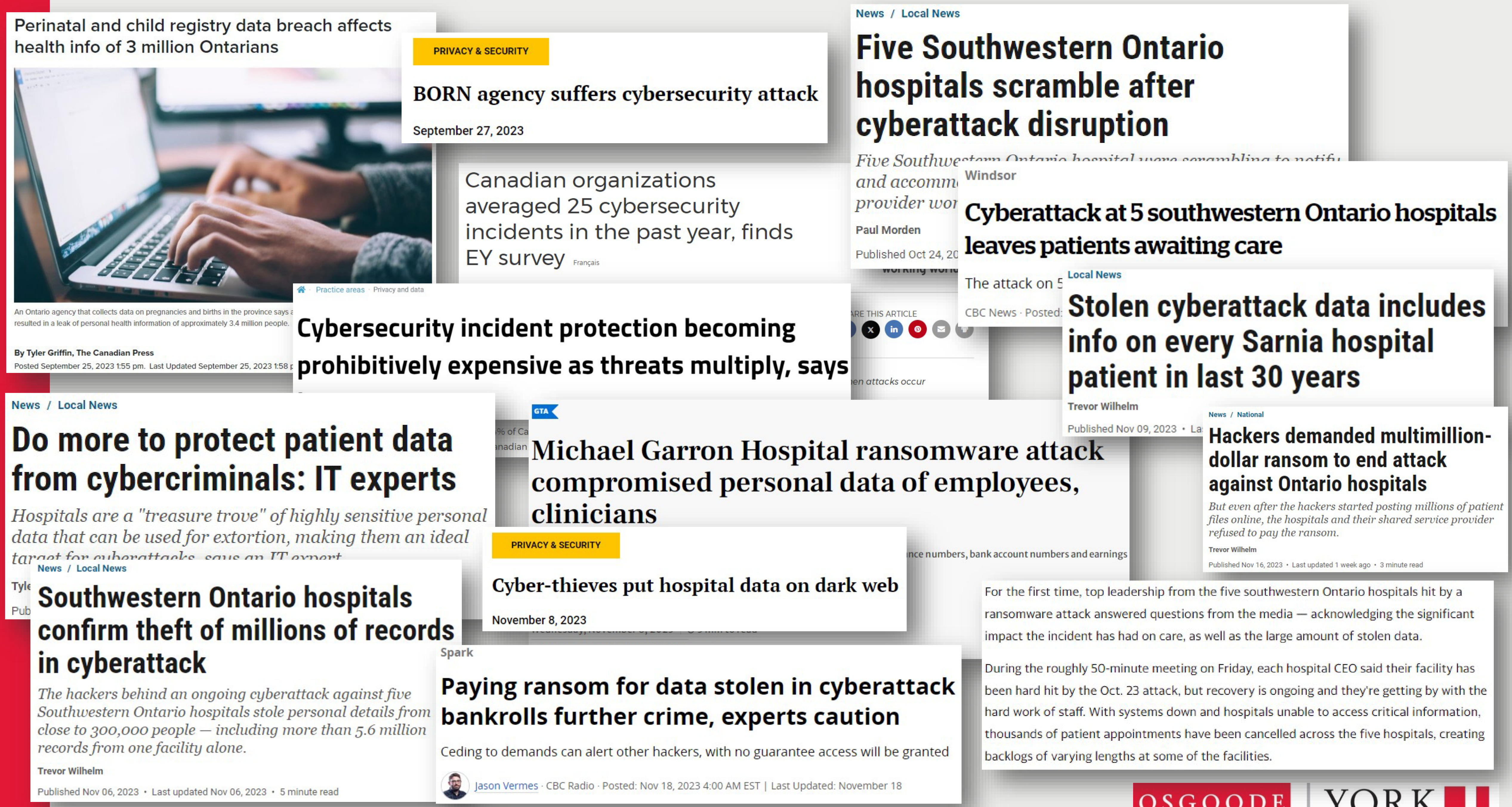
OSGOODE
OSGOODE HALL LAW SCHOOL
PROFESSIONAL DEVELOPMENT

YORK
UNIVERSITÉ
UNIVERSITY

Topics

- Cybersecurity trends
- Recent breach investigations
- IPC guidance
  - Administrative Monetary Penalties (AMPs)
  - IPC outsourcing (forthcoming)
- Discussion

Cybersecurity Trends



Perinatal and child registry data breach affects health info of 3 million Ontarians

An Ontario agency that collects data on pregnancies and births in the province says a
resulted in a leak of personal health information of approximately 3.4 million people.

By Tyler Griffin, The Canadian Press
Posted September 25, 2023 1:55 pm. Last Updated September 25, 2023 1:58 p

PRIVACY & SECURITY

BORN agency suffers cybersecurity attack

September 27, 2023

Canadian organizations averaged 25 cybersecurity incidents in the past year, finds EY survey Français

Practice areas · Privacy and data

Cybersecurity incident protection becoming prohibitively expensive as threats multiply, says

News / Local News

Five Southwestern Ontario hospitals scramble after cyberattack disruption

Five Southwestern Ontario hospital were scrambling to notify and accomm provider wor

Paul Morden

Published Oct 24, 20

Windsor

Cyberattack at 5 southwestern Ontario hospitals leaves patients awaiting care

The attack on 5

CBC News · Posted:

Local News

Stolen cyberattack data includes info on every Sarnia hospital patient in last 30 years

Trevor Wilhelm

Published Nov 09, 2023 • La

News / National

Hackers demanded multimillion-dollar ransom to end attack against Ontario hospitals

But even after the hackers started posting millions of patient files online, the hospitals and their shared service provider refused to pay the ransom.

Trevor Wilhelm

Published Nov 16, 2023 • Last updated 1 week ago • 3 minute read

News / Local News

Do more to protect patient data from cybercriminals: IT experts

Hospitals are a "treasure trove" of highly sensitive personal data that can be used for extortion, making them an ideal target for cyberattacks, says an IT expert

GTA

Michael Garron Hospital ransomware attack compromised personal data of employees, clinicians

nce numbers, bank account numbers and earnings

News / Local News

Southwestern Ontario hospitals confirm theft of millions of records in cyberattack

The hackers behind an ongoing cyberattack against five Southwestern Ontario hospitals stole personal details from close to 300,000 people — including more than 5.6 million records from one facility alone.

Trevor Wilhelm

Published Nov 06, 2023 • Last updated Nov 06, 2023 • 5 minute read

PRIVACY & SECURITY

Cyber-thieves put hospital data on dark web

November 8, 2023

Spark

Paying ransom for data stolen in cyberattack bankrolls further crime, experts caution

Ceding to demands can alert other hackers, with no guarantee access will be granted

Jason Vermes · CBC Radio · Posted: Nov 18, 2023 4:00 AM EST | Last Updated: November 18

For the first time, top leadership from the five southwestern Ontario hospitals hit by a ransomware attack answered questions from the media — acknowledging the significant impact the incident has had on care, as well as the large amount of stolen data.

During the roughly 50-minute meeting on Friday, each hospital CEO said their facility has been hard hit by the Oct. 23 attack, but recovery is ongoing and they're getting by with the hard work of staff. With systems down and hospitals unable to access critical information, thousands of patient appointments have been cancelled across the five hospitals, creating backlogs of varying lengths at some of the facilities.

OSGOODE | YORK

Cybersecurity Attack Trends

- The number and types of attacks are increasing
  - Last year, the Canadian Centre for Cybersecurity blocked up to 5 billion attempts on Government of Canada systems *per day*
  - Tactics are no longer limited to locking down information; now usually include threats to expose sensitive information
- Victims are increasingly including public institutions; hospitals are a common target
- Bigger payouts: the average ransom paid in Canada in 2022 was over $250,000
- Lower bar for entry: it’s easier than ever to be a cyber criminal
- Pandemic and movement to work-from home has expanded the “threat surface”
- “Collective defense” is being explored in the health sector

IPC Breach Investigations: Questions

Incident:

- What happened
- Containment
- Notification

General:

- Prevention
- Incident management
- Remediation

Specific:

- Ransomware
- Malware
- Phishing
- Remote Exploit
- Credential Theft

Vendor:

- Contractual / Vendor Agreement
- Vendor security practices

IPC Breach Investigations: Case Study

Decision 202: Unauthorized access to patient records by employees

- A health centre experienced 28 incidents of unauthorized access to patient records by employees
- Breach incident review revealed systemic issues, including:
  - inconsistencies in staff confidentiality agreements
  - inadequate privacy notices on the Electronic Medical Record (EMR) system
  - absence of a formal privacy breach policy
- The health centre failed to take reasonable steps to protect PHI and to provide notice of the breach to those affected at the first reasonable opportunity, as required by the act.

IPC Breach Investigations: Case Study

Decision 205: Phishing email attack on two health service providers

- Breach involved a home and community care related custodian and one of its agents
- Custodian staff reported a suspicious email from the agent to the organization’s IT department
- Affected PHI included patients’ names, allergies, diagnoses, and more
- The phishing email attack occurred on June 1, 2020, but the Custodian reported the incident as a breach to this office five months later in November 2020.
- Decision discusses notification “at the first reasonable opportunity”

IPC Breach Investigations: Case Study

Decision 210: Cyberattack on a public hospital

- Several hospital systems accessed through a password-spraying attack that compromised a privileged account, affecting PHI of over a million patients.
- Concerns about account privileges, system protections, strength of passwords, and notification timelines
- Takeaways: Reminder of the ever-evolving nature of cybersecurity threats and the importance of strong data protection measures. Institutions must continuously review and enhance their security protocols, particularly in areas of password management, access controls, and firewall security.

IPC Breach Investigations: Case Study

CPIN breach by CAS employee

- An employee of a children's aid society (CAS) accessed the Child Protection Information Network (CPIN) without authorization.
- IPC's Early Resolution team focused on ensuring victim notification, breach containment, and measures to prevent similar future incidents.
- CAS improved its privacy protocols, including enhanced compliance with annual privacy training, regular signing of oaths of confidentiality, introduction of privacy warnings on CAS network logins, and a formal auditing program. CAS also updated its privacy policy to explicitly include disciplinary actions for unauthorized access to personal information.
- Takeaway: importance of proactive measures in safeguarding sensitive information

IPC Breach Investigations: Case Study

Cyberattack on a third-party vendor

- Cyberattack on a vendor providing virtual care platforms compromised the PHI of over 100,000 patients across 32 health care providers.
- The breach, rooted in the vulnerabilities of a third-party service, exposed the crucial need for stringent data protection measures, including strong contractual safeguards.
- This review led to strengthened contractual arrangements and an enhanced understanding of PHI security responsibilities for which health care institutions remain accountable, even when they use third party service providers
- Takeaways: ensure strong cybersecurity measures are in place, especially when entrusting PHI to external service providers

IPC Breach Investigations: Case Study

Cyberattack on laboratory system

- joint investigation found company failed to implement reasonable safeguards
- IPC and BC OIPC ordered the organization to:
  - improve specific practices regarding IT security
  - formally put in place written IT security policies and practices
  - cease collecting specified information and to securely dispose of the records of that information which it has collected
- IPC issued the following additional orders:
  - improve process for notifying individuals
  - clarify and formalize status with respect to the custodians in Ontario with whom it has contracts

IPC Breach Investigations: Case Study

Cyberattack at an Eastern Ontario hospital

- Threat actors accessed the hospital’s electronic network via a compromised VPN account, encrypting back office and legacy health information databases.
- The hospital notified affected individuals and took steps to prevent future breaches, including implementing multi-factor authentication.
- Incident highlights the need for
  - appropriate disposal of redundant data and ensuring that legacy data, if kept, has the same protections as other PHI.
  - ensuring backup data is not connected to the main networks, to safeguard against future breaches.

IPC Cybersecurity Resources

Guidance

- Detecting and Deterring Unauthorized Access to PHI
- Responding to a Health Privacy Breach: Guidelines for the Health Sector (

Technology Fact Sheets

- How to Protect Against Ransomware
- Protect Against Phishing

Podcast

- Unmasking Digital Threats: How to Guard Against Cyber Crime

Notable Cybersecurity Standards

NIST Cybersecurity Framework
Endorsed by the Ontario Cyber Security Expert Panel in 2022 report

Ontario Public Service Data Integration Data Standards (Part III.1 of FIPPA)

IPC Manual for the Review and Approval of Prescribed Persons and Prescribed Entities (Guidance) – note: significant update coming

Administrative Monetary Penalties

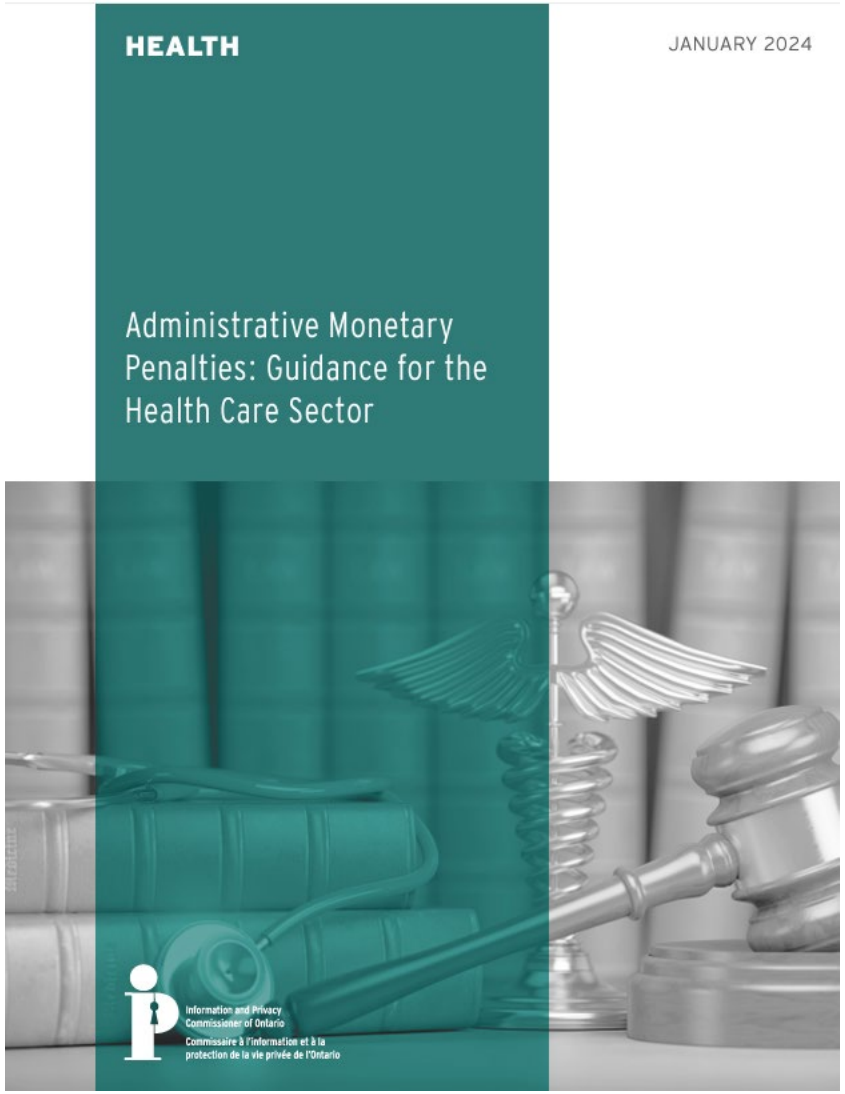
Administrative Monetary Penalties (AMPs)

- Ontario is the first jurisdiction in Canada to have put in place AMPs in the health sector
- As of Jan 1, 2024, the IPC can issue AMPs for serious contraventions of PHIPA
- AMPs are not fines; they are a part of a progressive toolset of regulatory interventions that can be used to address PHIPA contraventions
- AMPs help ensure that no one derives economic benefit from contraventions of PHIPA
- The regulation includes a range of penalties (max. $50,000 for an individual and $500,000 for an organization); specific amounts will depend on the particulars of each case and must not be punitive

New IPC Guidance

Criteria for AMPs and how the IPC will determine penalty amounts.

If you have additional questions about AMPs, email us at **info@ipc.on.ca**.



HEALTH

JANUARY 2024

Administrative Monetary Penalties: Guidance for the Health Care Sector

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

IPC Guidance on Outsourcing to Service Providers (forthcoming)

- Supports IPC Strategic Priority “Privacy and Transparency in a Modern Government”
- Responds to a growing need for due diligence when institutions outsource data processing and records to agents, supporting third-party risk management efforts
- Intended for use by M/FIPPA institutions but may be adapted for use by any organization
- Builds and expands upon the recent “trilogy” of IPC privacy investigation decisions
- Checklist deals with each stage of procurement including planning, tendering, vendor selection, agreement management, and contract termination
- Benefitted from consultations with numerous eternal stakeholders
- Consistent with new OPS/BPS procurement guidance and relevant OPS directives
- Voluntary and does not contain specific legal advice or recommended contract clauses.
- Targeted for early 2024 publication

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

The Office of the Information and Privacy Commissioner of Ontario

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*

OSGOODE | YORK

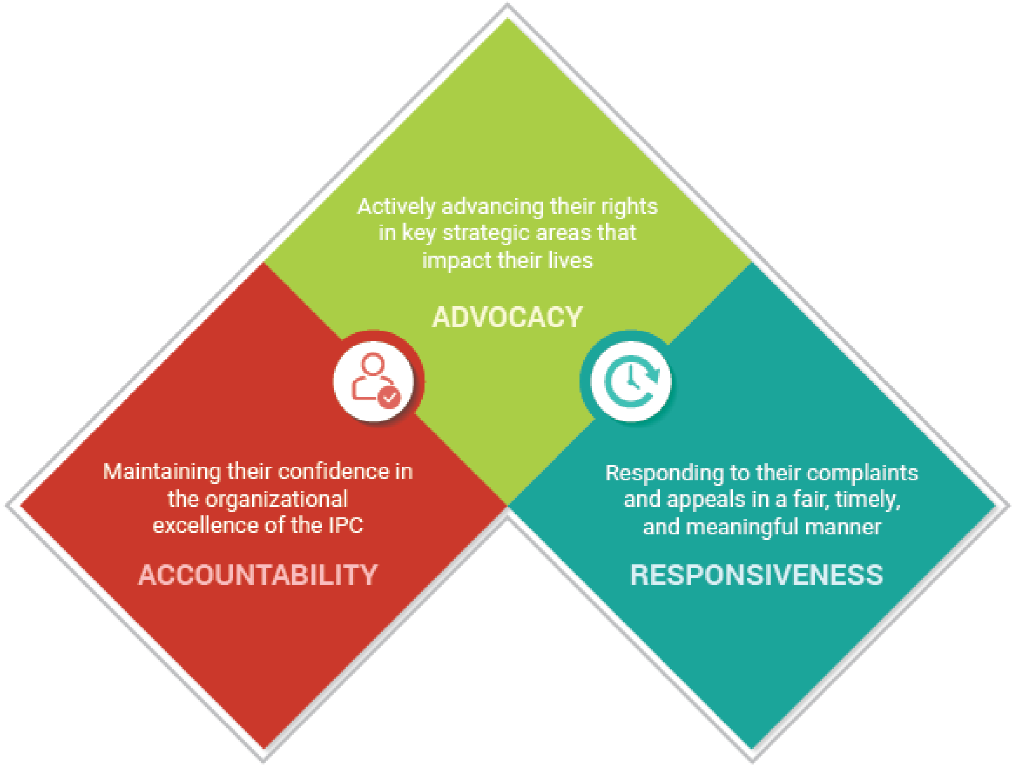
IPC’s Overall Role & Mandate

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’S VISION

Enhance Ontarians’ trust that their access and privacy rights will be respected by ...



Actively advancing their rights in key strategic areas that impact their lives

ADVOCACY

Maintaining their confidence in the organizational excellence of the IPC

ACCOUNTABILITY

Responding to their complaints and appeals in a fair, timely, and meaningful manner

RESPONSIVENESS