

OBA Privacy Summit

Warren Mar, Assistant Commissioner,
Tribunal and Dispute Resolution Division

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

OBA
Privacy Law Summit
Privacy Regulation: The
Interplay of Federal and
Provincial regulators

October 1, 2024

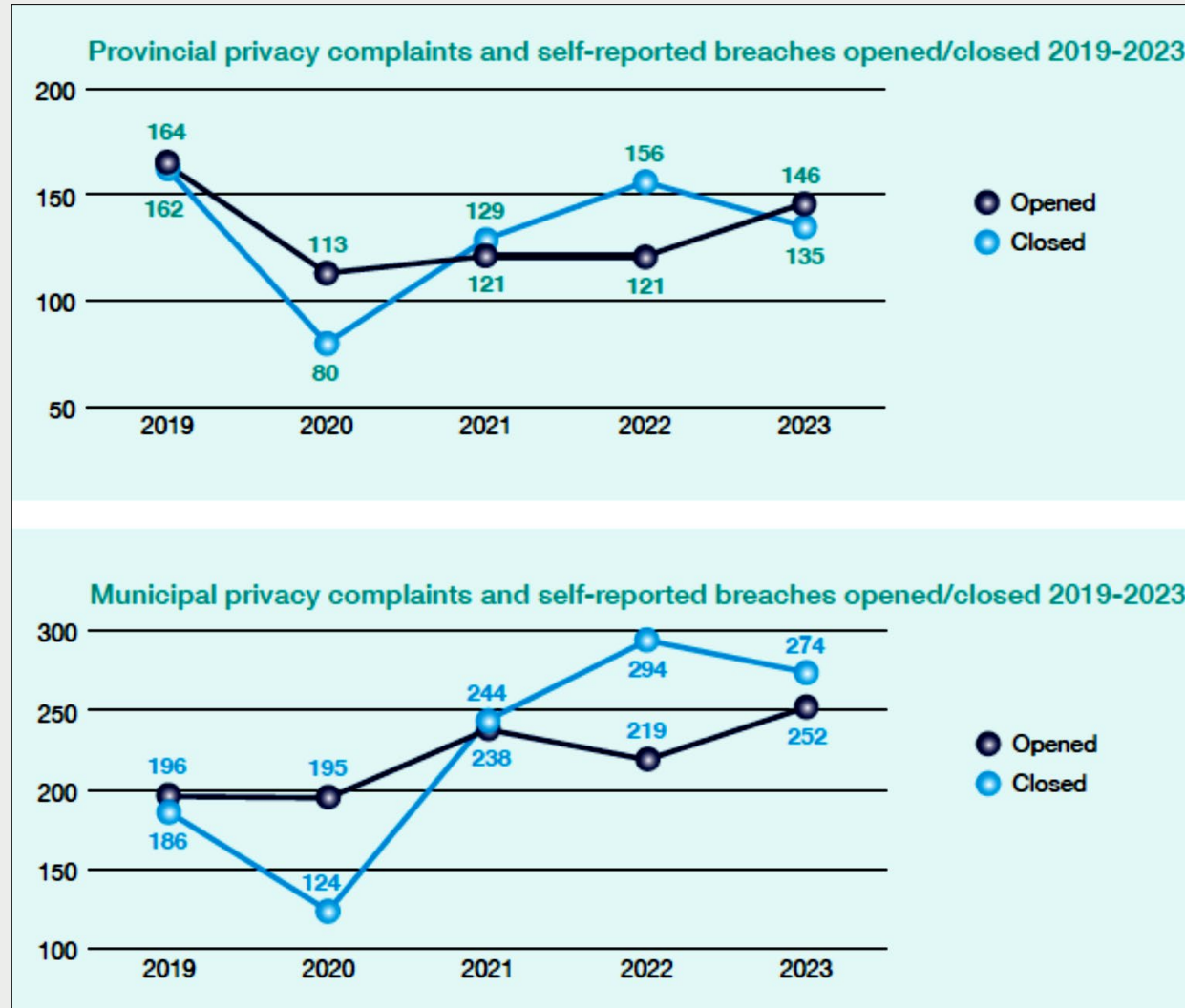
Who We Are

- The Information and Privacy Commissioner of Ontario provides independent review of access and privacy matters
 - Commissioner is not part of government of the day
- Oversees Ontario's access and privacy laws:
 - public's right to access information, have their personal privacy rights protected
 - laws apply to government, police, school boards, universities, hospitals, children's aid societies, etc.
 - outside of personal health information and health information custodians, **no oversight of the private sector** (time for made-in-Ontario solution?)

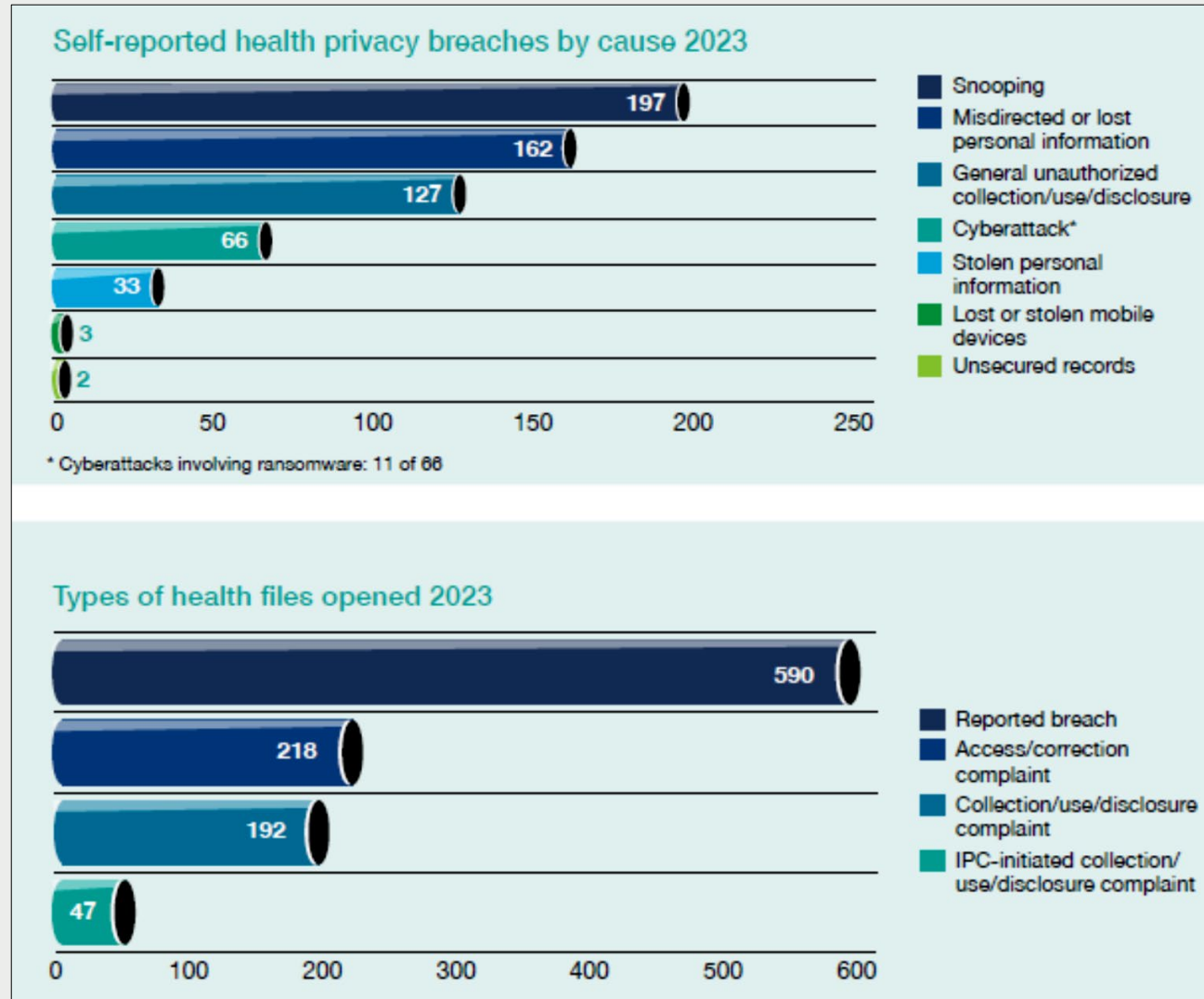
Legislative Framework

Federal public sector	Ontario public sector	Ontario health sector / child services sector	Private sector
<p>Government of Canada federal ministries, agencies, crown corporations</p> <p><i>Privacy Act</i></p>	<p>Government of Ontario ministries, agencies, hospitals, universities, municipalities, police, schools</p> <p><i>Freedom of Information and Protection of Privacy Act (FIPPA)</i></p> <p><i>Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)</i></p>	<p>Health care individuals, organizations ("health information custodians") hospitals, pharmacies, labs, doctors, dentists, nurses</p> <p>Child and family service providers (children's aid societies)</p> <p><i>Personal Health Information Protection Act (PHIPA)</i></p> <p><i>Part X, Child, Youth and Family Services Act (CYFSA)</i></p>	<p>Private sector businesses</p> <p><i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i></p>
OPC oversight	IPC oversight	IPC oversight	OPC oversight

Public Sector Privacy Complaints & Breach Reports



PHIPA Privacy Complaints & Breach Reports – 2023



Managing & Responding to Breaches

Notification to Regulator:

- **Ontario public** (*FIPPA/MFIPPA*): not mandatory, but best practice to notify where breach has a significant or serious impact, such as those that may involve sensitive personal information or large numbers of individuals, or when you are having difficulties containing the breach.
- **Ontario health** (*PHIPA*): mandatory if breach as per s. 12(3), considering factors in s. 6.3 of regulation
- **Ontario child services** (*CYFSA*): mandatory if breach as per s. 308(3), considering factors in s. 9 of regulation
- **Private** (*PIPEDA*): yes, if **RROSH** as per s. 10.1(1)

<https://www.ipc.on.ca/en/privacy-organizations/managing-breaches>

Managing breaches




A privacy breach occurs when personal information is collected, retained, used, disclosed, or disposed of in ways that do not comply with Ontario's privacy laws. All public sector organizations, health information custodians, children's aid societies and other child and family service providers should have a privacy breach response plan.


Under Ontario's access and privacy laws, child and family service providers and health information custodians are required to [report](#) certain privacy breaches to the IPC.


[REPORT A PRIVACY BREACH AT YOUR ORGANIZATION](#)

What to do in case of a breach

Contain the breach and notify affected individuals 

Investigate 

Notify the IPC 

Reduce the risk of future breaches 

Additional Resources

- [Privacy Breaches: Guidelines for Public Sector Organizations](#)
- [Responding to a Health Privacy Breach: Guidelines for the Health Sector](#)
- [Reporting a Privacy Breach to the Information and Privacy Commissioner: Guidelines for Service Providers under Part X of the Child, Youth and Family Services Act](#)
- [Reporting a Privacy Breach to the IPC: Guidelines for the Health Sector](#), types of breaches that need to be reported to the IPC at the first reasonable opportunity
- [A Guide to Privacy and Access in Ontario Schools](#)
- Review our full list of [guidance documents](#).



Real Risk of Significant Harm (RROSH)

- Real risk of significant harm does not apply under Ontario health law (*PHIPA*).
- Under the legislation, the breach doesn't necessarily have to be significant to be reported or for affected parties to be notified.
- For example, if a laptop was lost or stolen and if there were just a few patient memos on it containing PHI, you would be required to report it.

Timing of Breach Reports to Commissioner

- At the first reasonable opportunity.
- Please do not wait until you have all the details — the breach report form will assist you in providing relevant information to the IPC.
- You will have an opportunity to submit an additional report/information later.
- Reasons to report early:
 - individuals impacted by the breach might contact the IPC
 - the media might take an interest in the breach
 - IPC can point you to relevant guidance to assist with remediation.

Content of Breach Report to Commissioner

- Generally, IPC asks organizations/institutions to report:
 - The **circumstances** of the breach (how did info become lost, stolen, used without authority?)
 - Did you **report** breach to **individuals**? If so, how?
 - What is the **exact nature** of the information and how many people were impacted? If you don't know exactly the nature and number of people, do you have an estimate of when you will know?

Ability to Cooperate

General authority and Commissioner's powers:

- Section 59 of *FIPPA* and section 46 of *MFIPPA* (public sector)
- Section 66 of *PHIPA* (health sector) and section 326 of *CYFSA* (child services sector)
- Section 68(3) of *PHIPA* and section 328(3) of the *CYFSA* have explicit statutory provisions that allow the Commissioner to disclose information that comes to their knowledge in the performance of their functions if required for the purpose of exercising those functions.

But limited sharing of information for public sector – other jurisdictions can share freely with us, but limitations on our part regarding what we can share with them:

- *FIPPA* s. 55 (1): The Commissioner or any person acting on behalf of or under the direction of the Commissioner shall not disclose any information that comes to their knowledge in the performance of their powers, duties and functions under this or any other Act.

Bill 194: *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*

Recommendation 20: Amend section 9 of Schedule 2 to remove any ambiguity around the Commissioner's ability to share information necessary to carry out their powers, duties, and functions under the current s. 55(1) of *FIPPA* (**bold** is recommendation, **red** is Bill 194 amendment):

- 55 (1) The Commissioner or any person acting on behalf of or under the direction of the Commissioner shall not disclose any information that comes to their knowledge in the performance of their powers, duties and functions under this or any other Act, **unless** the disclosure is required for the purpose of exercising those powers, duties or functions or **the disclosure is permitted for a prescribed purpose.**

More info on IPC's position on Bill 194 provisions: <https://www.ipc.on.ca/en/resources/ipc-comments-bill-194-strengthening-cyber-security-and-building-trust-public-sector-act>.

PHIPA – Administrative Monetary Penalties

- On March 25, 2020, the Ontario government amended Ontario's health privacy law. Ontario is the first province in Canada to give the Information and Privacy Commissioner the power to levy administrative monetary penalties against individuals and companies that contravene *PHIPA*.
- The IPC's use of this additional enforcement power is governed by section 61.1 of *PHIPA* and an accompanying regulation (O. Reg. 329/04, s. 35) that took effect on January 1, 2024.
- Order requiring a person to pay an administrative penalty shall not be issued more than two years after the day the most recent contravention first came to the knowledge of the Commissioner.

Cooperation Between Federal & Provincial Privacy Regulators

Each regulator will assess the issue and its alignment with their mandate and jurisdiction.

- Regulator's participation in a joint endeavor will occur at varying levels, dependent on legislative limitations, varying levels of authority, regional relevance, and many other considerations.
- FPT privacy regulators in Canada, both large and small, may collaborate, cooperate and exchange information to:
 - a) work together to leverage one another's capacity and resources, to **enhance their collective advocacy and enforcement efforts**:
 - *Yes, You Can* guide released by IPC and adapted by other Canadian offices – children at risk
 - *Sharing Information in Situations Involving Intimate Partner Violence: Guidance for Professionals*

Cooperation Between Federal and Provincial Privacy Regulators (cont.)

b) issue joint statements or resolutions:

- *Principles for responsible, trustworthy and privacy-protective generative AI technologies (2023)*

c) address multi-jurisdictional issues:

- LifeLabs breach
 - Cyberattack involving unauthorized access to its computer systems in 2019; up to 15 million Canadians affected
 - Information included health card numbers, names, email addresses, passwords, date of birth, and test results of some individuals
 - Joint investigation by the Information and Privacy Commissioners of Ontario and BC — see backgrounder from 2019 and findings announced in June 2020 on IPC website
 - LifeLabs agreed to follow orders and implement recommendations, but report not yet public (under judicial review for confidentiality reasons)

Cooperation Between Federal and Provincial Privacy Regulators (cont.)

c) address multi-jurisdictional issues (continued):

- Casino Rama breach
 - Ontario Lottery and Gaming Corporation (*FIPPA* public institution) & Casino Rama private sector company (OPC)
 - 2016: OLG reports a cyberattack on Casino Rama Resort to IPC
 - IPC launched investigation into circumstances of the breach and whether reasonable security measures were in place to protect personal information of Casino Rama customers
 - Investigation revealed weaknesses in cyber-security practices — particularly with response to suspicious activity
 - OLG/Casino Rama have taken steps to address the weaknesses identified — IPC satisfied

Interplay of Other Regulatory Bodies

IPC also works with other regulators on joint statements, resolutions, and advocacy:

- Other Legislative Offices and Commissions in Ontario
 - Joint statement by the Information and Privacy Commissioner of Ontario and the Ontario Human Rights Commission on the use of AI technologies
- International regulators, regulatory bodies and associations such as:
 - International Conference of Information Commissioners (ICIC)
 - International Association of Privacy Professionals (IAPP)
 - Global Privacy Enforcement Network (GPEN)

THANK YOU!

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