



Office of the
Saskatchewan Information
and Privacy Commissioner

ANNUAL REPORT



2025-2026



June 25, 2026

Honourable Todd Goudy
Speaker of the Legislative Assembly
29 Legislative Building
Regina, Saskatchewan S4S 0B3

Dear Mr. Speaker,

I am pleased to present my second Annual Report as Information and Privacy Commissioner for the province of Saskatchewan. I have prepared this Annual Report in accordance with the provisions of section 62(1) of *The Freedom of Information and Protection of Privacy Act (FOIP)*, section 52(1) of *The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP)*, and section 60(1) of *The Health Information Protection Act (HIPA)*.

I continue to be extremely grateful to the Board of Internal Economy for my appointment, and I look forward to working with the Board to provide our citizens with a continuing high level of service in the coming years.

I also wish to thank the Members of the Legislative Assembly for their support of this office. Going forward, we are committed to this office's mandate – the provision of access to information to the people of Saskatchewan while also working with our stakeholders to ensure that the privacy rights and protections afforded by our legislation prevails.

Finally, I wish to thank the team at the Office of the Information and Privacy Commissioner for their kind assistance in the preparation of this Annual Report.

Respectfully,

Original Signed by
Grace Hession David
Saskatchewan Information and Privacy Commissioner

TABLE OF CONTENTS

Commissioner’s Message	5
About Us	7
Organizational Structure.....	8
Outreach 2025-2026	10
Resources	18
The Strategic Plan 2025-2026.....	20
Summary Advice	31
Types of OIPC Files	34
Files Opened and Closed	34
Reports and Recommendations.....	36
Appeals.....	32
Acknowledgement.....	41
Service and Accessibility Charter	42



Commissioner's Message

Access to Information: We continue with our commitment to access to information for the citizens of Saskatchewan. 433 files were opened last year - the most in our history. 57% of those involved reviews of exemptions applied by heads of government institutions/rural municipalities. 30% involved investigations and reports of privacy breaches across Saskatchewan. This past year we have worked with rural municipalities to educate on the legislation with respect to access to information requests. In November of 2025 I had the honour of presenting at the Saskatchewan Association of Rural Municipalities in Regina. This presentation led to a restructuring of our website to include a special tile entitled “Help for Rural Municipalities”. Our office has always provided assistance with the application of the *LA FOIP* principles. But now we have launched a workshop for rural municipalities. We offer the workshop to those who require ongoing assistance. We understand that rural municipalities face special issues when it comes to staffing, responding to, and processing access to information requests. In order to better serve the public, we are committed to education.

Privacy Breaches: This office announced on December 11, 2025 that Saskatchewan has formally adopted a zero tolerance for the willful violation of privacy. Last month the province of Ontario joined our declaration of zero tolerance for privacy breaches in the wake of the concerning allegations arising from Project South.¹ This office now names those who have intentionally breached the privacy of the people of Saskatchewan. We need to be able to trust that our private information is safe with our government institutions and local authorities. We commend the good corporate citizens who proactively reported these breaches to us. We have named the following individuals for privacy violations this past year:

Fahmida Shipa – [*Investigation Report 104-2025*](#) (proactively reported by the Saskatchewan Health Authority);

Constable Clinton Duquette – [*Investigation Report 123-2025*](#) (proactively reported by the Regina Police Service);

Marianne Mann – [*Investigation Report 155-2025*](#) (proactively reported by the Saskatchewan Health Authority);

¹Ontario privacy watchdog warns “zero tolerance” for police database breaches with new powers. The Globe and Mail. May 25, 2026.

Danniela Morgan – [*Investigation Report 082-2025*](#) (proactively reported by eHealth Saskatchewan).

Of these individuals, we only referred two to the Ministry of Justice for an opinion with respect to prosecution. On May 14, 2026, Constable Duquette was charged pursuant to section 56(6) of *LA FOIP*. As of writing, Constable Duquette’s matter has been remanded in the Saskatchewan Provincial Court to a date in July, 2026. Ms. Morgan is awaiting trial on serious *Criminal Code* charges that preceded the privacy violations.

Artificial Intelligence and Privacy: The growth of artificial intelligence (AI) and public concern over the lack of privacy safeguards became an area of concern this past year. The 2026 edition of the [*Ipsos AI Monitor*](#) published in June 2026 revealed that 67% of Canadians feel nervous with respect to products that offer AI technology and only 25% of the Canadian population are excited to use and adopt this technology. The fears involve speculation with respect to future job loss and the general lack of trust over AI hallucinations and surveillance capability. We know that AI offers time saving options and has presented excellent innovations in policing, education and the health care sector. However, we cannot escape the reality that online commercial tracking, the lack of privacy attached to facial recognition technology, video analytics, deepfakes and voice recognition – are all issues associated with AI technology that can cause anxiety. Our office has also targeted the lack of transparency and accountability of AI services that originate from sources outside our sovereign borders. We are especially concerned with the privacy threat posed to young and vulnerable children who cannot possibly understand the digital footprint they leave online. We are facing a wholesale erosion of personal privacy unless strong regulatory laws can be brought into place.

In the past year, our office has produced two podcasts that explain the intersection of AI and children’s privacy to parents. We have a special tile on our website that assists with the more pressing issues, including a handy checklist for healthcare organizations that are considering the use of an AI Scribe. I had the privilege of presenting an Update of Children’s privacy and proposed privacy legislation in Canada to our Minister of Justice and Attorney General, Mr. Timothy McLeod K.C. on April 27, 2026. On top of the concerns just mentioned, the issues of excessive data collection, data sovereignty and the lack of informed consent with the eventual sharing of personal information are paramount when it comes to AI. This technology is here, and we remain hopeful that it can be harnessed to serve us in our daily lives and at the same time be crafted and regulated to ensure personal privacy and individual safety.

The Honourable Bernadette McIntyre, the Lieutenant Governor of Saskatchewan and Grace Hession David, Information and Privacy Commissioner of Saskatchewan.



About Us



FOIP, LA FOIP and HIPA establish the access to information and protection of privacy rights of the citizens of saskatchewan.

Our Mission

To ensure that access to information and privacy rights in Saskatchewan are protected.

Statutes we Oversee:

The Freedom of Information and Protection of Privacy Act,

S.S 1990-91, c. F-22.01, as amended.

The Local Authority Freedom of Information and Protection of Privacy Act,

S.S. 1999, c. H-0.021, as amended.

The Health Information Protection Act,

S.S. 1999, c. H-0.021, as amended.

Our Mandate

The OIPC ensures that local authorities, government institutions and health trustees respect the privacy and access rights of the citizens of Saskatchewan by:

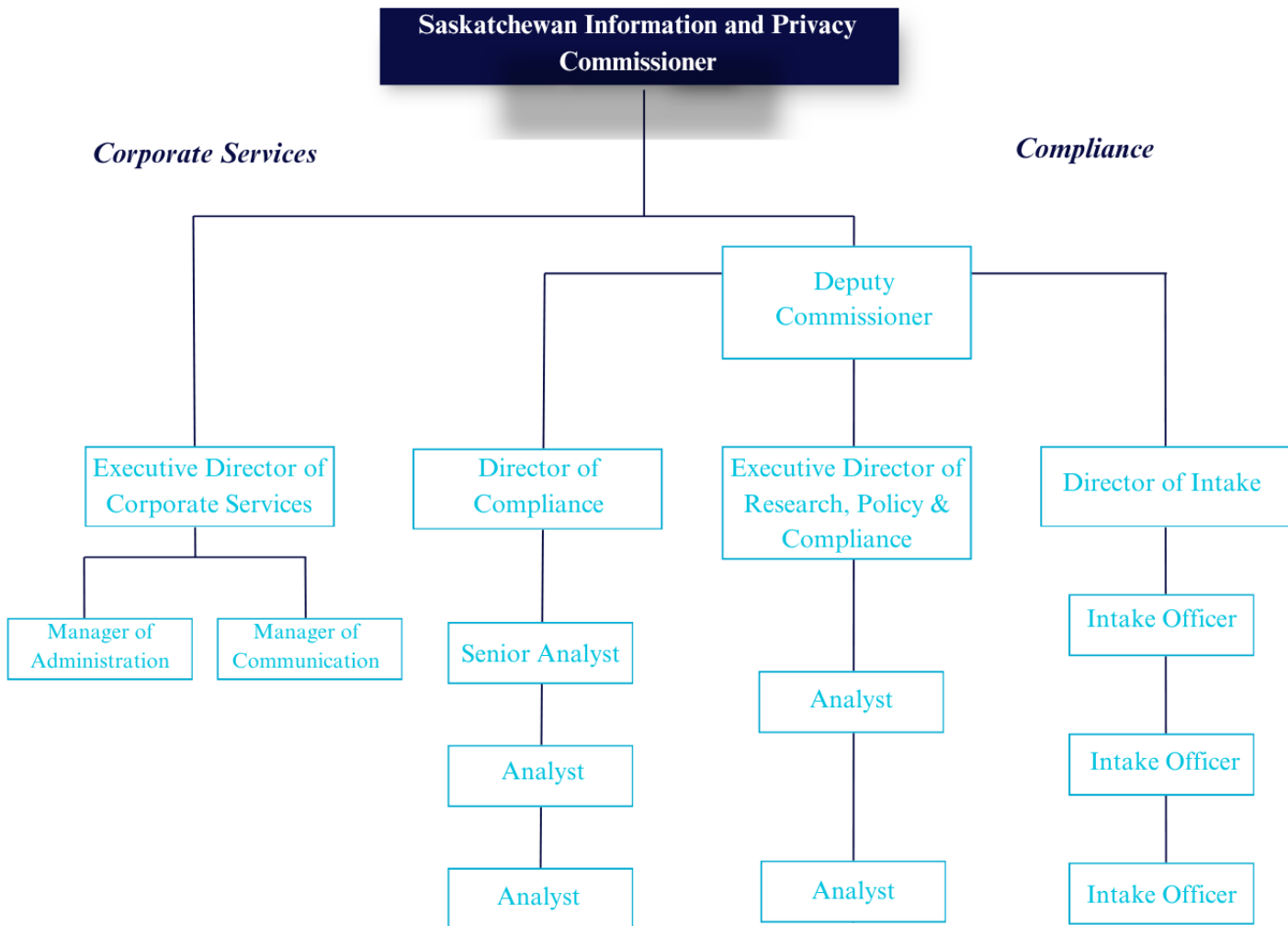
- Informing members of the public of their access to information and privacy rights.
- Resolving access and privacy disputes between individuals and public bodies.
- Making recommendations on appeals from access to information decisions by public bodies.
- Investigating and resolving privacy complaints.
- Issuing recommendations on public bodies' policies and practices.
- Commenting on proposed laws, policies and practices.

Core Values

Excellence Fairness Responsibility & Accountability Integrity Respect

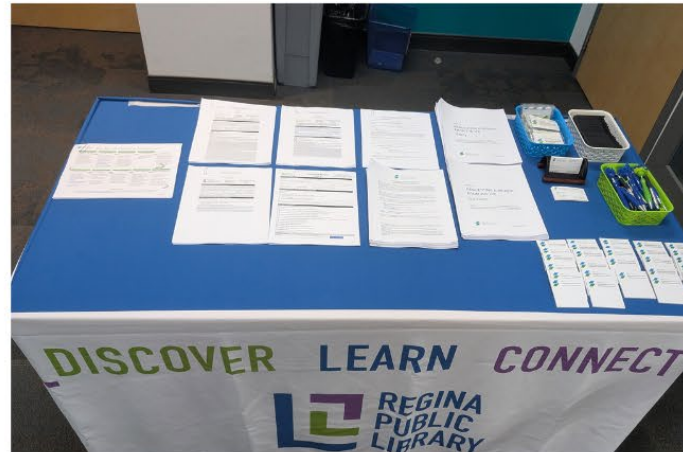
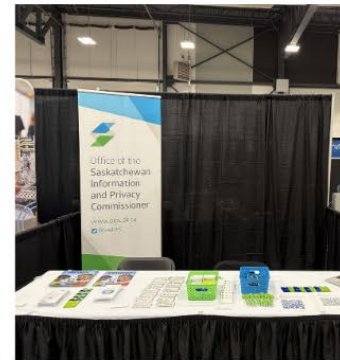
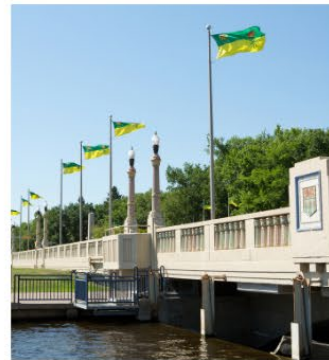


Organizational Structure



HIGHLIGHTS OF COMMUNITY OUTREACH

2025
—
2026



Along with our ongoing investigations and published reports, we have been very busy with our community educational/outreach activities this year.



April 1, 2025-June 30, 2025

**April 1,
2025**

The Deputy Commissioner participated in the Regulated Health Professionals Act “Town Hall”.

**April 10,
2025**

The former Commissioner presented at the Association of Records Managers and Administrators (ARMA) of Saskatchewan Convention on “Privacy: The Changing Landscape”.

**April 22,
2025**

OIPC staff provided feedback to the City of North Battleford on its public video surveillance policy.

**May 12-
13, 2025**

The Commissioner attended the International Association of Privacy Professionals (IAPP) conference in Toronto.

**May 20,
2025**

The OIPC Executive Director of Research, Policy and Compliance virtually attended a Saskatchewan Health Information Leadership Group meeting. This group provides a forum for discussion with respect to best practices as it relates to current trends, opportunities, and issues facing health information professionals in Saskatchewan.

**May 21,
2025**

The Commissioner met with the Saskatchewan Ombudsman, Ms. Pratchler, and Conflict Commissioner, Justice M. Herauf.

Outreach Continued

**May 22,
2025**

The Commissioner met with Mr. Aaron Orban, Executive Director, Audit and Information Management Branch, Ministry of Justice and Attorney General.

**May 28,
2025**

The Deputy Commissioner provided comments to the Ministry of Government Relations on proposed amendments to The Municipalities Act, The Cities Act, and The Northern Municipalities Act, 2010 for introduction in the 2025 Fall Legislative Session.

**June 4,
2025**

The Commissioner met with Manitoba Information and Privacy Commissioner and Ombudsman, Ms. Jill Perron.

**June 6,
2025**

The Commissioner presented to an information session at the Canadian College of Health Information Management (CHIMA) in Regina.

**June 10,
2025**

The Commissioner attended an educational webinar: “Using Artificial Intelligence in your Legal Practice” hosted by the Saskatchewan Trial Lawyers Association.

**June 11,
2025**

OIPC staff provided comments to Health Shared Services Saskatchewan on the transfer of personal health information from Bridges Health Services.

**June 18,
2025**

OIPC staff provided feedback to the rural municipality of Francis on the issue of consent to collect contact information of ratepayers and the sending of e-notices.

The Commissioner attended an educational webinar: “Cybersecurity for Lawyers” hosted by the Saskatchewan Trial Lawyers Association.

Outreach Continued



July 1, 2025-September 30, 2025

**July 1,
2025**

The Commissioner attended an educational webinar: “Chat GPT and Legal Research” hosted by the Saskatchewan Trial Lawyers Association.

**July 4,
2025**

The Commissioner and Deputy Commissioner met with Deputy Minister Denise Macza, Deputy Minister, Ministry of Correction, Policing and Public Policy and Mr. Nathaniel Day, Legal Counsel.

**July 11,
2025**

The Commissioner spoke with Mr. Norman O’Neill, Assistant Deputy Minister, Ministry of Health.

**July 21,
2025**

The Commissioner met virtually with Ms. Caroline Maynard, Information Commissioner of Canada to discuss privacy issues, federal and provincial.

**July 24,
2025**

The Commissioner presented to an information session of the Canadian College of Health Information Management (CHIMA) in Regina.

**July 28,
2025**

OIPC staff provided feedback to Neighbourly Pharmacy Inc. (Queen City Wellness Pharmacy Regina) on its provincial Privacy and Confidentiality Policy and Procedures Manual.

Outreach Continued

July 29, 2025

The Commissioner and Deputy Commissioner met with Ms. Michelle Mula, Vice President of Quality, Safety and Chief Information Officer, Saskatchewan Health Authority and Ms. Pat Stuart, Executive Director, Privacy and Health, Saskatchewan Health Authority.

August 15, 2025

OIPC Public Podcast – “AI and Children’s Privacy” published by the Deputy Commissioner and Commissioner and available on the OIPC website.

August 29, 2025

The Commissioner met with Ms. K. Kaip, Executive Director Regional Prosecutions.

September 9, 2025

The Commissioner presented to the Saskatchewan Health Sector Privacy and Access Forum - representatives from Ministry of Health, Saskatchewan Health Authority, Saskatchewan Cancer Agency, 3sHealth and Health Quality Council.

August 12, 2025

The Executive Director of Research, Policy and Compliance participated in the Federal/Provincial/Territorial Privacy Health Working Group meeting.

August 20, 2025

The Commissioner attended an educational webinar: “Artificial Intelligence – Enhanced Advocacy” hosted by the Saskatchewan Trial Lawyers Association.

September 3, 2025

OIPC staff provided feedback to the Ministry of Health on its Sharing Information to Protect the Health and Safety of Children and Youth, now finalized and available online.

Outreach Continued

September
12, 2025

OIPC staff provided feedback to Tower's Pharmacy Regina (PharmaChoice Canada Inc.) on its Saskatchewan privacy policies and procedures.

September
16, 2025

The Commissioner presented to a U of R Business class on the three privacy statutes in this province.

September
25, 2025

The Executive Director of Research, Policy & Compliance and an OIPC Analyst, presented at the annual "Right to Know" conference held at the Regina Public Library, Regent Branch.

Q3

October 1, 2025-December 31, 2025

October
7-10,
2025

The Commissioner and the Deputy Commissioner attended the annual Federal/Provincial/Territorial meeting of Information and Privacy Commissioners across Canada in Banff, Alberta. The Commissioner meets virtually with this group every month of the year to discuss federal and provincial privacy/information/data security issues.

October
17, 2025

The Commissioner and the Deputy Commissioner met with Ms. Lisa Dietrich, Chief Privacy Officer/Director, Health Information and Privacy, Ministry of Health and formally filed a submission on draft regulations to *The Health Information Protection Regulations*.

Outreach Continued

**October
22, 2025**

The Commissioner attended the Throne Speech of the Lieutenant Governor at the First Session of the 30th Legislature at the Legislative Assembly in Regina.

**October
29, 2025**

The Commissioner presented at the Information Management Community of Practice, Ministry of Justice and the Attorney General meeting.

**November
1, 2025**

OIPC staff participated in the “Law Fair” at the Regina Public Library during “Access to Justice Week”. The OIPC booth provided information to general questions to the citizens of Saskatchewan and supplied resources on privacy and access.

**November
3, 2025**

OIPC staff participated in the Regina Teachers’ Convention. The booth provided information to teachers in Saskatchewan and supplied resources on privacy and access in Saskatchewan. We also supplied the teachers with the Privacy Commissioner of Canada’s curriculum training materials.

**November
6, 2025**

The Commissioner presented at the annual Saskatchewan Association of Rural Municipalities conference in Regina, Saskatchewan.

**November
19, 2025**

The Commissioner presented to the Ministry of Justice and Attorney General Branch Meeting.

**November
21, 2025**

The Commissioner and Deputy Commissioner presented to the Board of Directors, Schizophrenia Society of Saskatchewan on patient privacy.

**December
8, 2025**

OIPC staff provided feedback to the Ministry of Health on its Improving Value of Health Care Initiative.

Outreach Continued



January 1, 2026-March 31, 2026

**January
14, 2026**

The Commissioner attended a virtual webinar: “AI, Deepfakes, and Safeguarding Children Online” hosted by the Saskatchewan Trial Lawyers Association.

**January
15, 2026**

The Commissioner met with the Lieutenant Governor of Saskatchewan, The Honourable Bernadette McIntyre and Executive Director, Ms. Carolyn Speirs to discuss the work being conducted at OIPC.

**January
27, 2026**

The Commissioner attended an educational webinar: “Modernizing Administrative Justice: Judicial Review in 2026”, hosted by Lexis/Nexis Inc. Professor Paul Daly from University of Ottawa and Justice Guy Régimbald of the Federal Court of Canada updated *R v Vavilov*, [2019] 4SCR 653.

**January
28, 2026**

The Commissioner and the Deputy Commissioner participated in a presentation and discussion on AI Governance, hosted by the International Association of Privacy Professionals (IAPP) on “AI Governance”.

**February
3, 2026**

The Commissioner met with Dr. Lisa Broda, Saskatchewan Advocate for Children and Youth, and discussed the upcoming federal Online Harms Bill.

**February
4, 2026**

The Commissioner attended an educational webinar: “AI Laws in Canada”, sponsored by the Law Society of Saskatchewan.

Outreach Continued

**February
12, 2026**

The Commissioner attended an education webinar: “Beyond the Bill: Navigating Online Harms, Intimate Privacy and Reputation in a Changing Legal Landscape”, sponsored by the Canadian Bar Association.

**March 17-
20, 2026**

The Commissioner attended and presented at a weeklong Privacy Access Congress in Ottawa, Ontario. The seminar was hosted by the Privacy and Access Council of Canada. The Commissioner presented with the Commissioners of Alberta, Ontario and the Federal Information Commissioner.

**March 26,
2026**

The Commissioner presented a case law update to the Canadian Bar Association – Saskatchewan Privacy Section.

**March 30,
2026**

The Commissioner and Deputy Commissioner met with Deputy Minister Richelle Bourgoin of Ministry of Social Service.

RESOURCES

[BLOGS](#) [RESOURCES](#) [CHECKLISTS](#) [GUIDES](#) [RESPONSE TEMPLATES](#)

New/Updated OIPC Website Resources

2025-2026

ARTIFICIAL INTELLIGENCE AND PRIVACY

- [Episode 1: AI and Children’s Privacy](#)
- [Episode 2: AI and Child Digital Privacy Part 2](#)
- [Policing Technology and the Citizen’s Reasonable Expectation of Privacy](#)
- [Backgrounder: Summary of joint investigation into OpenAI’s ChatGPT – Office of the Privacy Commissioner of Canada](#)
- [PIPEDA Findings #2026-002: Joint Investigation of OpenAI OpCo, LLC – Office of the Privacy Commissioner of Canada \(full Report\)](#)
- [Update on Children’s Privacy and Proposed Legislation in Canada](#)
- [Joint Statement on AI-Generated Imagery and the Protection of Privacy-](#)
- [Checklist for Healthcare Organizations Considering the use of an AI Scribe](#)
- [AI’s Double-Edged Sword: Balancing Innovation and Privacy of Information](#)
- [When AI Turns Dark](#)

SUGGESTIONS TO PREVENT PRIVACY BREACHES

- [5 Ways to Protect Your Privacy](#)
- [Guide to Faxing](#)
- [Protecting your Personal Information in Today’s Consumer Landscape](#)
- [Ransomware-What Everyone Should Know](#)
- [Snooping in a Police Database](#)
- [Surveillance in Personal Care Homes: A Case Study](#)
- [What Does it Mean if a Proactively Reported Privacy Breach is Informally Resolved?](#)
- [Your Right to Privacy](#)

ACCESS TO INFORMATION TOPICS

- [How do I Request a Correction of my Personal Information or an Amendment of my Personal Health Information?](#)
- [Explaining Cookies in the Internet Age](#)
- [IPC Guide to FOIP \(Chapter 4\)](#)
- [IPC Guide to FOIP Table of Contents](#)
- [Section 45 and 56 Response](#)
- [Work Product vs. Personal Information](#)
- [Your Privacy and Access to Information Rights in Saskatchewan](#)
- [Act on your “Right to Know”](#)
- [Yes, You Can](#) (Disclosure of Children’s Personal and Personal Health Information)

HELP FOR LOCAL AUTHORITIES

- [How to Conduct an Effective Search for Records](#)
- [File Path Frustrations](#)

- [IPC Guide to LA FOIP \(Chapter 4\)](#)
- [IPC Guide to LA FOIP Table of Contents](#)
- [Managing Electronic Records](#)
- [Personal Information for Local Authorities](#)
- [Sample Operational Policy for Municipalities](#)
- [Section 45 and 56 Response](#)
- [School is in Session](#) (Educational Resources Available)
- [Work Product vs. Personal Information](#)

HEALTH CARE PRIVACY TOPICS

- [Health Care Personal Information Snooping: When Will People Learn?](#)
- [Steps to Request a Correction of Personal Information or Amendment of Personal Health Information](#)
- [Avoiding Abandoned Patient Records](#)
- [“Bin” There, Shouldn’t Have Done That: When Medical Records End Up in the Wrong Bin](#)
- [Checklist-for-healthcare-organizations-considering-the-use-of-an-AI-scribe](#)
- [Yes, You Can](#) (Disclosure of Children’s Personal and Personal Health Information)

2025-2026

Strategic Plan



Goal 1: Continue Accessibility to the Public

Goal 2: Prioritizing Youth Privacy

Goal 3: Raising Awareness Around Privacy Breaches

Goal 4: Educating on Privacy Concerns and Artificial Intelligence

Goal 5: Providing Assistance to the Victims of a Cyber Breach



The Strategic Plan 2025-2026

Goal 1: Continued Accessibility to the Public

We aim towards the provision of timely access to information, and we function as the moderating voice in disclosure disputes. We understand our position as an independent and impartial officer of the Saskatchewan legislature. We continue to provide a careful review of the application of exemptions. We have produced a [Service and Accessibility Charter](#) so that the public can clearly understand our responsibilities and what we need from the public in order to meet our mission statement with our core values in mind.

We opened 433 files this past year as opposed to 284 the year before and we successfully closed 307 files which surpasses last year. Our staff is working hard but we value quality work product before quantity. We must ensure that applications for information are motivated by a real need to know. This year, more than any other year, we issued 4 disregard decisions. These decisions are not issued lightly because a citizen's right to access information from a government institution or a local authority is a quasi-constitutional right that is recognized by the highest court in Canada, [Canada \(Information Commissioner\) v Canada \(Minister of National Defence\)](#), 2011 SCC 25, [2011] 2 SCR 306 at paragraphs [40] and [79]. The Commissioner can bring a discontinuance if it is obvious that the access request involves motives that are not in good faith, as in: [Review Report 044-2025](#) (August 26, 2025), or at the request of the local authority when the requests are repetitious, and abusive of the right of access, as in: [Disregard Decision 306-2025](#) (December 12, 2025).

Goal 2: Prioritizing Youth Privacy

Our office has benefitted greatly from the work and example set by our federal Privacy Commissioner, Mr. Philippe Dufresne. We know that children are going online earlier, and they are leaving bigger digital footprints. We have committed to educating parents on the risks of

[unsupervised online access](#) to young children. Australia has banned and now Canada, the UK and Malaysia have proposed to ban, social media for anyone under 16 years of age. Recent statistics indicate that more than 60% of children in Australia are still using the sites because they have easily circumvented the ban.² A ban may serve as nothing other than a false sense of security to parents when the real focus should be with the social media sites that offer dangerous options to young people. We note that the recent *Digital Safety Act*, Bill C-34 introduced in the House of Commons on June 10, 2026 offers exemptions and carve-outs to the ban as long as the proposed Digital Safety Commission is satisfied that the operator of the social media service provides adequate safeguards for the protection of children (see proposed section 29).

At home our office used an international cyber breach as an opportunity to educate on how to contract with an international Information Management Service Provider (ISMP) and protect against cyber breaches. This IMSP was a large US based software provider that over-collected on the sensitive data of its child clients and provided service contracts that omitted any reference to the provisions of *LA FOIP* and the *LA FOIP* regulations. The local authority failed to conduct regular audits of the IMSP, and it also failed to ensure that all records of the local school were properly purged from the IMSP database once the contract was terminated. The resulting cyber breach was disastrous in that the sensitive data of the child clients and adult employees was exfiltrated by cyber criminals. We were the first province in Canada to report and educate on the PowerSchool breach and our report was concise and comprehensive: [Investigation Report 035-2025](#) (August 7, 2025) and a signatory to the FPT joint resolution “[Protecting the Privacy of Children Through the Responsible Use of Technology in the Classroom](#)”.

Goal 3: Raising Awareness Around Privacy Breaches

This office continues to investigate and educate on the dangerous consequences of a privacy/cyber breach and the methods to avoid and contain such breaches- see our two podcasts on this very issue. This past year we have commenced naming offenders who violate the privacy of others and in extreme cases, we utilize the provisions of our legislation to recommend the fact scenarios to the Ministry of Justice for consideration. Without a doubt, the worst consequence of a privacy breach – whether it be by unwarranted snooping on corporate databases or by direct invasions of privacy by cyber criminals – is the loss of trust in governmental institutions, local authorities and health care providers. The public deserves protection. We continue to be committed to maintaining the security of the personal information of the people of this province and we will call out the bad actors who violate that privacy.

Goal 4: Educating on Privacy Concerns and Artificial Intelligence

Last year we only identified Generic AI as a tool that must be used with caution in order to preserve individual security and privacy. This year we have Agentic AI. The difference between these two forms of AI reveals how quickly this technology is advancing and infiltrating into our lives. Generic AI offers a tool for you to generate content or complete your duties – such as sending emails and summarizing documents or even drafting documents. Generic AI can be dangerous if it is trusted and unleashed without supervision to combat hallucinations.

Agentic AI is AI that works autonomously to achieve the user’s goal. Agentic AI can plan, act, observe and adapt to meet your goal. Agentic AI will now manage your task altogether acting as

² <https://mollyrosefoundation.org/more-than-60-of-australian-children-still-using-social-media-despite-ban-for-under-16s-research-shows/>

you: it will formulate a plan for you, search multiple websites and execute duties for you – all without a specific prompting because it operates from your original prompt instruction. But other than your original prompt – there is no human in that loop – which involves unlimited risk and should cause grave concern. Here’s what can happen if you do not choose your agent with care and ensure that the code is trustworthy because:³

- Untrusted code in the AI agent can arbitrarily execute commands by means of direct prompt injection and allow attackers to run your system and execute commands. You are no longer in the driver’s seat, and you suffer a data breach and data leakage;
- Untrusted code can allow attackers access to your passwords opening up the gate for credential and identity theft;
- Untrusted code can engage in indirect prompting that may cause the agent to execute commands that you had never intended;
- Untrusted code can allow the underlying purpose of your agent to drift. This means that the task may start out as you had intended but move into areas by means of the use of other AI tools that you do not even know about or by indirect prompt injection. This can result in data exfiltration and constitutes a huge security breach.

Anything we file into the AI large language model domain is public – with very rare exceptions to date. Lawyers now need to be careful not to inadvertently waive client privilege in the use of legal AI services, and the same caution applied to medical doctors/nurses. Humans need to always be in the loop and Information and Privacy Offices are now finding that this technology is taking up a great deal of time and consideration in our daily duties. Our office is on the forefront of this technology and hopes to continue to educate and lecture on the security risks associated with AI as we have in the past year. AI is here and we need to understand that it must be harnessed and used with governance at all times to ensure privacy and the security of the individual/organizations that have adopted the technology. We take direction from, and fully support, our federal Privacy Commissioner in his efforts to educate and instruct on [Privacy in the age of Artificial Intelligence](#).

Goal 5: Providing Assistance to the Victims of a Cyber Breach

Our office continues to provide support to the victims of a cyber breach. When cyber criminals hack into a system there are two classes of victims. The first class involves the institution that has suffered the security breach. The next class of victims involves the individuals who make up the clientele of the institution. These are the many individuals who have had their personal information stolen without their knowledge. We provide assistance to both groups of victims. In terms of the entity that has been breached, we can help with how to contain the breach and how to properly notify the affected individuals. We also provide education on the proper methods of in-house investigation of the breach. We also provide direct assistance to the individuals who have suffered the exfiltration of their personal information. We accept complaints and initiate our own investigations where we look for the root cause of a cyber breach and assess whether the institution over-collected personal information and whether multi-factored authentication was used along with other desirable security features. We always recommend credit monitoring, and we assist these victims to work with the breached entity so that the matter can be resolved as peacefully and quickly as possible.

³ [“Six Dangers of Autonomous AI Agents”](#), IBM Technology, June 4, 2026.

International Association of Privacy Professionals, Toronto, May 4, 2026



(left to right) Michael Harvey – Information and Privacy Commissioner of British Columbia, Philippe Dufresne – Privacy Commissioner of Canada, Grace Hession David - Information and Privacy Commissioner of Saskatchewan, Patricia Kosseim – Information and Privacy Commissioner of Ontario.

Summary Advice

Outside of undertaking formal reviews and investigations, the OIPC offers advice, such as providing answers to questions posed by the public and stakeholders. It is called summary advice. There are two types:

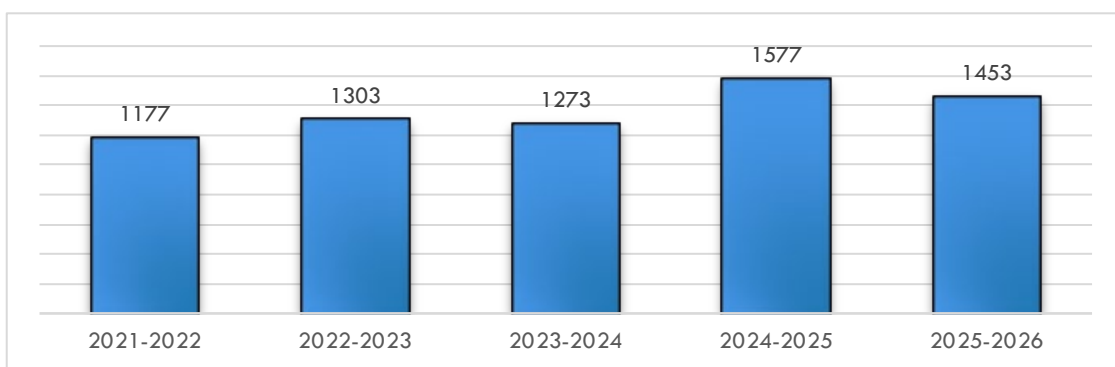
General Summary Advice

- We provide summary advice most often as the result of a question from a member of the public.
- We can effectively assist and respond to questions that involve issues of process involving *FOIP*, *LA FOIP* and *HIPA*.
- We respond with answers that touch on the role, mandate and jurisdiction of the OIPC.
- We can provide the basics to inquiries with respect to simple questions dealing with *FOIP*, *LA FOIP* or *HIPA*.
- We are pleased to assist if we can provide referrals, contacts and we can sometimes offer helpful resources from other sources.

Substantive Summary Advice

- Most often, these requests originate from an organization.
- Without giving an advanced ruling or legal advice, we are happy to offer guidance in interpreting/applying the legislation in particular situations

The chart below demonstrates the demand for both general and substantive summary advice.



Goal of Summary Advice

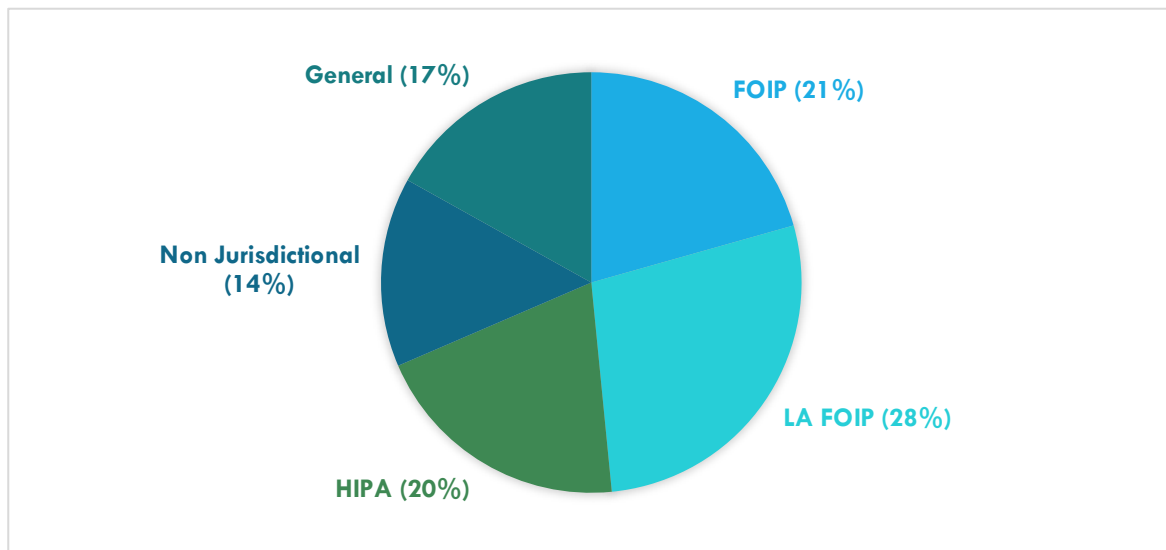
Our goal was to provide summary advice within 3 business days. The OIPC provided summary advice, on average, within **45.12 hours (1.88 days)**, 100% of the time.

Advice offered falls into five different categories.

Summary Advice Categories

FOIP	Anything <i>FOIP</i> related
LA FOIP	Anything <i>LA FOIP</i> related
HIPA	Anything <i>HIPA</i> related
Non-jurisdictional	Access and privacy related, but not the OIPC's jurisdiction
General	Informational Assistance

Percentages of Summary Advice Requests per Category



Types of OIPC Files

The OIPC opens case files to undertake reviews of access and/or correction requests when attempts to effect an informal resolution is unsuccessful. Files are also opened with respect to access-related procedural issues, and investigations into privacy breaches.

A **Review Report** will report on the Commissioner’s opinion with respect to a request for an access to information issue.

An **Investigation Report** will report on the Commissioner’s opinion with respect to a privacy breach investigation and the steps that were taken to contain the breach.

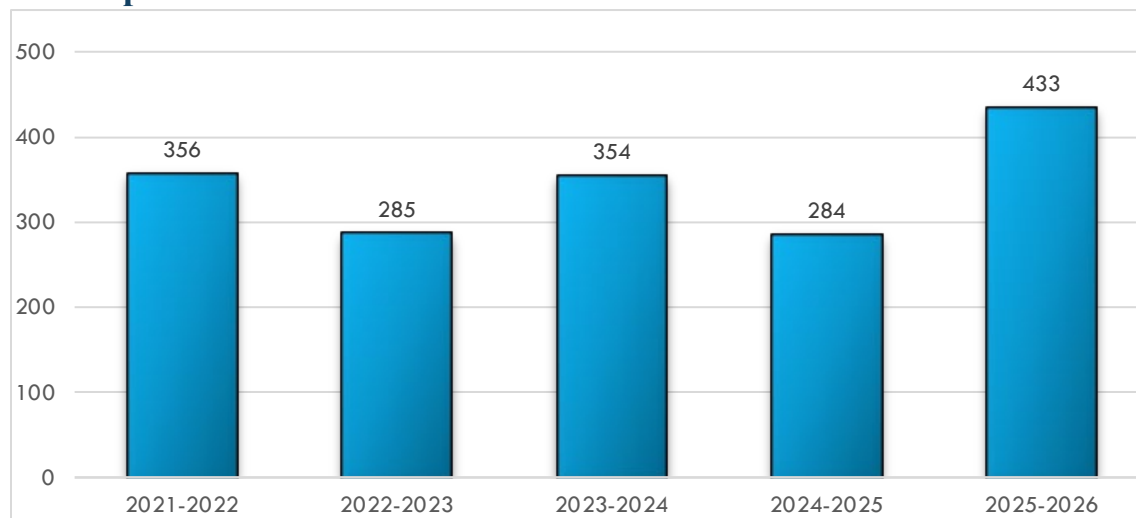
A **Disregard Request** is different from a review or investigation. In this instance, the OIPC informs a government institution or local authority whether it can disregard an access request or correction request before the expiry of the 30-day response period. Instead of a report, a version of a report called a “decision” is issued.

A **Consultation File** is usually opened when the OIPC is approached by a stakeholder and asked to offer commentary on draft work product such as a policy, privacy impact assessment, piece of legislation, a regulatory amendment, etc.

Files Opened and Closed

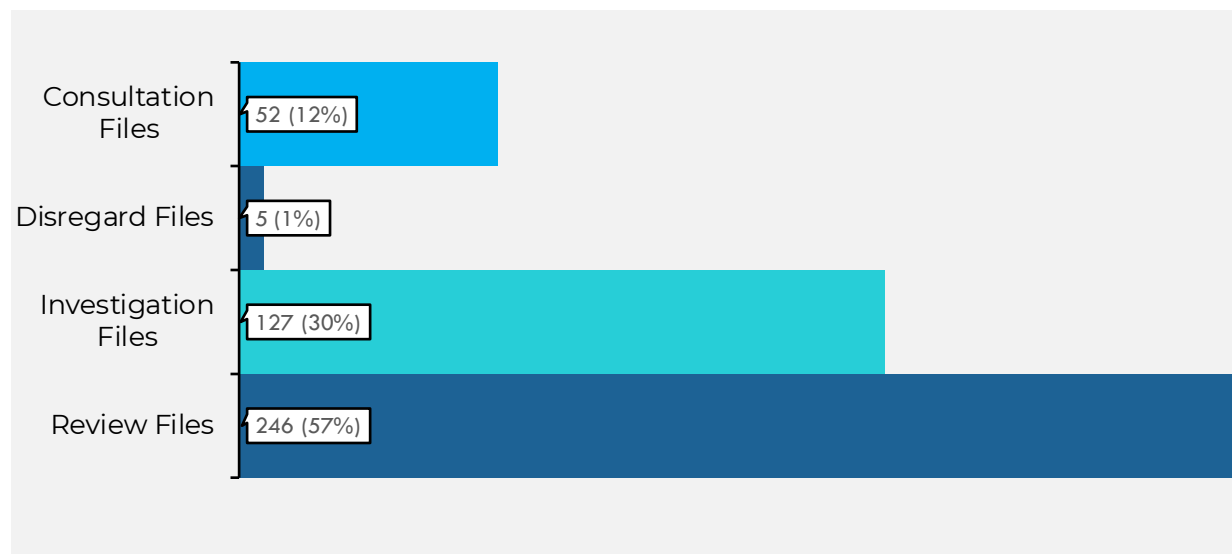
Last fiscal year, the OIPC **opened 433** files, and successfully **closed 307**.

Files Opened



Types of Files Opened

Out of the **433** files opened last fiscal year, the majority were review files. The full breakdown is as follows:



File Closure

A primary goal of the OIPC is to resolve matters through **early resolution** at the intake stage within 30 calendar days, which only can occur with the cooperation of the parties involved. If a matter is resolved by the Intake team, it is closed without moving to the formal process which may result in the issuance of a public report. The Intake team closed **55** files via early resolution this past fiscal year, on average within **48.28** calendar days. Alternatively, a file may be closed via **informal resolution** without the issuance of a report, if after moving to formal notices, an Analyst is able to mediate or otherwise resolve issues to the satisfaction of the parties. **44** case files were closed in the 2025-2026 fiscal year as informal resolution. If informal resolution is not possible, then the file may be closed once the review or investigation report is issued.

Files can also be closed with the issuance of a **disregard decision** which considers a disregard application from a government institution or local authority. In these cases, the Commissioner must make a decision as to whether the processing of one or more access to information/correction requests can proceed.

Files can also be closed by our office under a category called, “**not proceeded with.**” In these cases, the file is not closed by early or informal resolution or by the issuance of a public report, but for a variety of different reasons including the following more common ones:

- Withdrawn/abandoned by applicant or individual
- Frivolous/vexatious/not made in good faith/concerns a trivial matter
- No jurisdiction/grounds
- Matter was subject to a previous report
- Parties have not reached an impasse

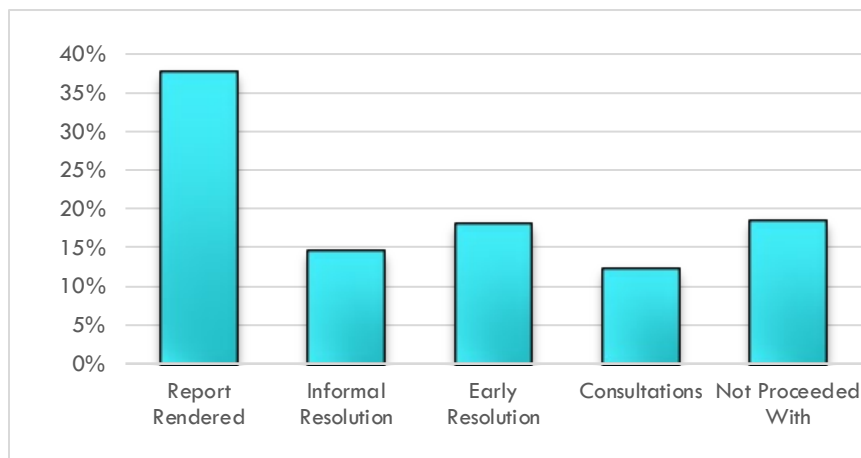
If a review or investigation is underway, a public body or trustee may submit an application to discontinue where some of the above may be raised as preliminary issues. For procedural fairness, the application will be shared with the other party so they may respond before a decision to proceed by the Commissioner is made.

It is still an OIPC priority to issue decisions and reports in a timely fashion without sacrificing accuracy and quality. It must be acknowledged that we approach each matter on a case-by-case basis. Some cyber breaches involve massive investigations, and we work in conjunction with the stakeholder. This focus can occur over the course of many months. The resulting Investigation Report will be complicated and lengthy. Putting a timeline on this kind of work is impossible. All the same, the usual access request is something that can be investigated and reported on within the efficient timelines as established by this office.

The following is a breakdown of how the **307** files closed were resolved by the OIPC.

2025-2026 Resolution	#of Files
Went to Report	115 ⁴
Informally Resolved	44
Early Resolution	55
Consultations	37
Not Proceeded With	56
Total	307

Only 38% of files resulted in the **issuance of a public Review or Investigation Report.** This demonstrates the commitment of the OIPC to work with government institutions, local authorities and trustees to resolve matters informally instead of making the matter public.



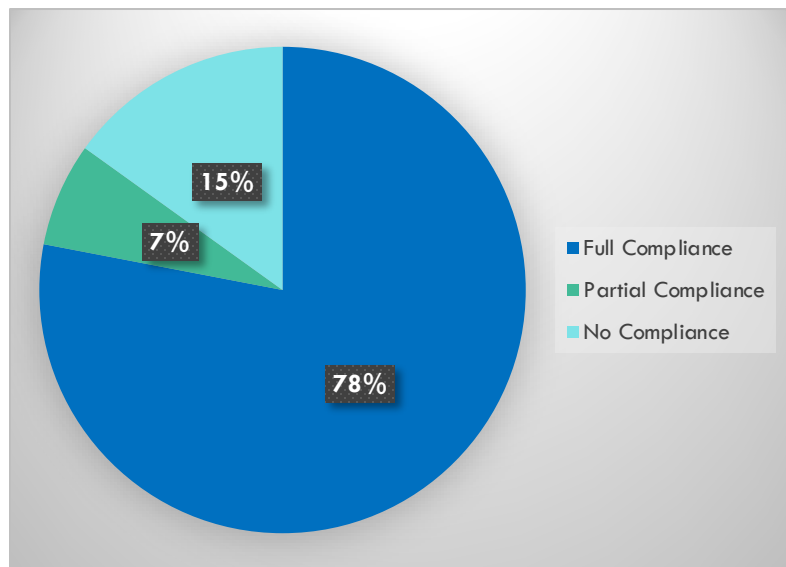
⁴ This number includes 74 review files, 37 investigation files and 4 disregard decisions. On the previous page we noted 5 disregard 5 files were opened, we had one abandoned.

Reports and Recommendations

When the OIPC issues a Review or Investigation Report, the Commissioner makes formal findings and recommendations. In terms of compliance with individual recommendations made, as indicated in the pie chart below, only **15%** of the time there was no compliance. Conversely, in almost all other cases (**85%**), there was compliance and/or partial compliance.

The office issued **115** Review and Investigation Reports in the 2025-2026 fiscal year. A public body or trustee is required to respond to the recommendations within 30 days of receiving the report.

This chart shows the percentage of individual recommendations made to public bodies (government institutions and local authorities) and health trustees where there is full compliance, partial compliance and no compliance. Of the 232 recommendations made, 181 were full compliance, 16 were partial compliance and 35 were not complied with.



The OIPC is obligated to report on the recommendations that were not complied with - see *FOIP*, section 62(2); *LA FOIP*, section 52(2); and *HIPA*, section 60(2). Failure to respond to a report is considered to be non-compliance. On the following pages are three tables; the first table lists those public bodies and trustees that responded to a report with no compliance, the second table lists those public bodies and trustees that responded to a report with partial compliance.

NO COMPLIANCE

Government Institution	Report #	Recommendation(s) not complied with
Ministry of Corrections and Public Safety	Review Report 005-2025	[46]
Water Security Agency	Review Report 002-2025	[59] , [60]
Local Authority	Report #	Recommendation not complied with
City of Regina	Review Report 231-2025	[34]
RM of Prairie Rose	Review Report 242-2024	[66] , [67]
Village of Mortlach	Investigation Report 178-2025	[33]

PARTIAL COMPLIANCE

Government Institution	Report #	Recommendation(s) not or partially complied with
Executive Council	Review Report 264-2024	[51] , [52] , [53]
Farm Land Security Board	Review Report 076-2025, 195-2025	[66] , [67]
Ministry of Education	Review Report 008-2025	[26]
Ministry of Education	Review Report 114-2025	[92]

Ministry of Immigration and Career Training	Review Report 109-2025	[52] , [53]
Ministry of Labour Relations and Workplace Safety	Review Report 265-2024	[43]
Saskatchewan Human Rights Commission	Review Report 255-2024	[51]
Saskatchewan Marshals Service	Review Report 199-2025	[85] , [87]
Saskatchewan Municipal Board	Review Report 214-2024	[70]
Local Authority	Report #	Recommendation not or partially complied with
Prince Albert Police Service	Review Report 154-2025	[52]
Regina Police Service	Review Report 090-2025	[87] , [89] , [91] , [96]
Regina Police Service (Constable Clinton Duquette)	Investigation Report 123-2025	[70]
RM of Buchanan	Review Report 220-2024	[38]
RM of Reford	Review Report 198-2024	[86]
Saskatoon Police Service	Review Report 078-2025	[73]
Saskatoon School Division #13 St. Paul's Roman Catholic Separate School Division #20	Investigation Report 095-2025	[75]
Town of Eatonia	Investigation Report 105-2025	[52]
Town of Lafleche	Review Report 048-2025	[54] , [57]

University of Saskatchewan	Review Report 013-2025	[27]
Trustee	Report #	Recommendation not or partially complied with
Saskatchewan Health Authority	Investigation Report 193-2024, 043-2025	[166] , [167] , [168] , [169] , [170] , [171] , [173] , [174] , [175] , [176]
Saskatchewan Health Authority	Investigation Report 266-2024, 031-2025	[107] , [108] , [110] , [111] , [112] , [113] , [114]
Saskatchewan Health Authority (Fahmida Shipa)	Investigation Report 103-2025, 104-2025	[94]
Saskatchewan Health Authority (Marianne Mann)	Investigation Report 155-2025	[96]



APPEALS

We are extremely grateful for the continuing guidance given by the Saskatchewan Court of Appeal and the Saskatchewan Kings' Bench Court in assisting with the proper interpretation of the provisions of the three statutes we are tasked to administer. This past year there were only three appeals of our matters, but all three contained very helpful instruction. Our summaries follow.

**KASPRICK V SASKATCHEWAN
POWER CORPORATION, 2025
SKKB 139 (AUGUST 15, 2025)
JUSTICE A. DAVIS**



At A Glance

Exemptions

- Section 16(1)(a) of *FOIP* - Cabinet Confidences
- Section 17 of *FOIP* and the “could reasonably be expected” standard
- Section 17(1)(a) of *FOIP* - Advice, Proposals, Recommendations, Analyses or Policy Options
- Section 17(1)(b) of *FOIP* - Consultations, Deliberations, Positions, Plans, Procedures, Criteria or Instructions
- Section 17(1)(g) of *FOIP* - Confidential Information re: Policy/Budgetary Decisions
- Section 18(1)(b), (d) and (f) of *FOIP* - Sensitive Commercial Information
- Section 19 of *FOIP* - Third Party Information

The applicant was interested in the government of Saskatchewan’s future use of small nuclear reactors to provide clean, sustainable power to the people of Saskatchewan. The Applicant filed an access to information request with the Saskatchewan Power Corporation (SaskPower) for records relating to:

(1) Plans to build nuclear reactors in Estevan SK including cost, name of company supplying/building the reactors and timeline.

(2) Compensation to be paid to Estevan coal miners and coal plant workers when coal mining/electricity stops.

SaskPower initially withheld all responsive records. The Commissioner recommended that most of the withheld documents be released and over 200 pages were released but some pages still contained redactions. Davis J. ruled that some records be released but others were still subject to exemptions. The ruling is expansive and assists by providing important guidance on the following privacy issues:

Purpose of the Exemptions: Freedom of information legislation is not just about enhancing the public’s access to government records. It is the government’s chosen means of balancing competing interests: the (statutory) right to access information and society’s interest in maintaining the confidentiality of certain information, *SGI v Giesbrecht*, 2025 SKCA 10. [at paragraph 18]

Discretionary Exemptions: We are not to read the discretionary exemptions formally or narrowly such that the purpose of the exemption is defeated. A government body’s application of an exemption is to be given full latitude. If a document is found to fall within the application of a discretionary exemption, a reviewing court may not replace the government body’s exercise of discretion with that of the court. *FOIP* is to be seen as a means of providing transparency while also ensuring that the government benefits from the confidentiality it requires to carry out its duties. This was a case where the government was anticipating a project, and the plans and documents reflected a very early stage in its development. The government should not be impeded in its “sober consideration of a particular project or policy”. [at paragraphs 19 and 20].

Section 16(1)(a) of *FOIP* - Cabinet Confidences: Access should be prohibited when a record discloses the confidences of Executive Counsel. This includes “records created to present advice, proposals, recommendations, analyses or policy options” to Council or its committees. This is because the executive arm of the government must be able to receive advice, consider proposals and deliberate its options with the candour that comes from knowing what it reviews in confidence will remain confidential. [at paragraph 28]

Section 17 of *FOIP* and the “could reasonably be expected” standard: A “could” standard generally invokes reasonable possibilities – not probabilities. When combined with the word “expectation” the Legislature appears to be instituting a lower standard than probability but at least somewhat higher than mere possibility. *SGI v Giesbrecht*, 2025 SKCA 10 cited an “objective possibility” threshold. [at paragraph 30]

The Burden Pursuant to s.61 *FOIP*: The burden is upon the government institution to justify the application of the exemption. This burden does not mean that the government institution has to prove a fact, there must just be proof that a reasonable possibility existed – this is a very low standard which the Legislature chose to create. The possibility must be more than theoretical, and it must give rise to an expectation. The burden under section 61 is a very low one and Davis J. cautions against a “dogmatic and overly formalistic” approach when reviewing the decision to withhold. [at paragraphs 31 to 33]

Drafts vs Final Documents: Common sense must be applied to the core material in a document. It does not matter what stage the document appears. A draft document that contains recommendations or advice from an official, budgetary information or other protected class of information does not need to consolidate into its final form for the exemption to properly apply. “It would be illusory if only final documents, rather than drafts or constituent pieces of information were actually protected, see *John Doe v Ontario (Finance)*, 2014 SCC 36 , [2014] 2 SCR 3. [at paragraph 35]

Section 17(1)(a) of FOIP - Advice, Proposals, Recommendations, Analyses or Policy Options: The Executive Council or its members/committees must be permitted to consult public servants and others with a reasonable degree of confidentiality. A record-holder has the discretion to withhold records that contain advice from officials. Advice is not limited to directive statements or the clear expression of an opinion. It can involve information setting out considerations related to different policy options: John Doe at paras 26-27. [at paragraph 37]

The exemptions under section 17 cannot be used to prevent the disclosure of purely factual information but caution is urged when the advice takes the form of facts, information or consultations on which it is predicated and which may not be easily extracted. In those cases, the document should be treated as a whole and allow the exemption. [at paragraph 38]

The exemptions afforded by section 17 are not limited to communications that are immediately obvious as “advice” or “recommendations” but include analysis and policy options and in some cases, the raw data underlying them. This is especially the case where the raw data provides the basis for an official’s analysis, advice, recommendation or proposal. [at paragraph 38]

Documents that contain analysis, advice, recommendation or proposal include those that could facilitate the making of a decision at a much later date in time. [at paragraph 39]

Section 17(1)(b) of FOIP - Consultations, Deliberations, Positions, Plans, Procedures, Criteria or Instructions: In some cases, it is important to permit an institution to conclude significant consultation with First Nations bodies before the information is opened up to greater transparency or public scrutiny. [at paragraph 42]

In a similar vein, documents that show the government body is weighing various options, and establishing criteria, plans or procedures for different phases of a project may be subject to the s.17 exemptions if it forms part of the advice ultimately given to the Executive Council. [at paragraph 43]

Section 17(1)(g) of FOIP - Confidential Information re: Policy/Budgetary Decisions: This section is not intended to shield the government from scrutiny on how it spends the taxpayer’s money. The records in this case do not provide a clear indication of what this project cost to the date of the request and they do not indicate what the costs would be to bring the project to completion. Many of the documents in this tranche are unresponsive. [at paragraphs 46 to 48]

Section 18(1)(b), (d) and (f) of FOIP - Sensitive Commercial Information: The standard to be applied here is a “reasonable expectation”. The disclosure of proprietary information from a third party could reasonably be expected to have a negative impact on Saskatchewan’s economic interests. Similarly, the disclosure could reasonably be expected to negatively affect the province’s interests in ongoing negotiations or reveal valuable information that the province paid a third party for and for which it has every right to use on its own terms. [at paragraphs 50 to 52]

Section 19 of FOIP - Third Party Information: Even though the government or the third party did not argue s.19 in this matter, the exemption was still properly applied pursuant to s.18(1)(b), (d) and (f). The documents would reveal proprietary information with respect to the third party’s methodology in selecting a suitable site for the small nuclear reactor. Were these documents to be released, sensitive commercial information would be released. The data and methodology in the documents also had a monetary value. [at paragraphs 57 and 58]

Non-Responsive Documents: Government institutions should no longer release non-responsive documents. This is a developing approach with respect to disclosure. There is no logic in the release of irrelevant material. Tangential and non-responsive records really should not be identified by the document holder and they should not be ordered to be released. [at paragraphs 62 to 64]

Duplicate Documents: “This [ordering the release and printing of duplicate documents] creates mindless busy work for a taxpayer-funded employee without moving the needle toward promoting transparency. I do not think it matters that the applicant is not paying. If he is not paying that just means everyone else is.” The burden is still upon the record holder to clearly identify a duplicate when it alleges it will not release a document. A record holder may only decline to disclose duplicates when the documents are actually identical in all material respects. [at paragraphs 65 and 66]

Line by Line Analysis of Redactions: The rule here is whether the item that is urged to be unredacted actually promotes transparency. “The line-by-line assessment which the OIPC referred to is not intended to go through a document and identify all the meaningless headings, pictures and the like for disclosure. At the hearing of this matter, Mr. Kasprick himself highlighted the absurdity of receiving disclosure of a photograph of an onion.” [at paragraph 72]

**SCHILLER V SASKATCHEWAN
(MINISTRY OF EDUCATION), 2025
SKKB 146 (SEPTEMBER 11, 2025)
JUSTICE G. MITCHELL**



At A Glance

Two issues before the court

- The first was whether the Court should examine the unredacted records in camera.
- The second issue allowed for guidance on sections 24(1) and 29 of *FOIP*.

The Applicant filed an access to information request with the Ministry of Education for:

“All communication (electronic, digital, facsimile, verbal) with respect to SARS-Covid2, Covid 19, Sars COVID-2, other related terminology such as the Wuhan Virus and all related variants between Holy Family RCSSD #140 and its representatives and the Minister of Education and its representatives.”

On July 13, 2023 the Commissioner recommended that virtually all the information that the Ministry had redacted in its initial response be disclosed. The Ministry complied with most of the Commissioner’s recommendations but continued to refuse to disclose personal information relating to public servants in the matter. The Ministry withheld the personal information of its employees that was not publicly available. The types of information properly withheld included: names, email addresses, and phone numbers. The Applicant brought the appeal to the Saskatchewan King’s Bench.

There were two issues before the Court. The first was whether the Court should examine the unredacted records in camera. Justice Mitchell noted that often an appellate court will want to review records in camera because an appeal pursuant to the provisions of *The Freedom of Information and Protection of Privacy Act*, SS 1990-91, c. F-22.01, as amended (*FOIP*), is an appeal de novo where particulars of the documents and detailed reasons for the application of exemptions are not always available. But in this case, the Ministry’s submissions with respect to the reason for the personal information redactions were persuasive. It was clear the Applicant’s appeal was devoid of merit. The second issue allowed for guidance on sections 24(1) and 29 of *FOIP*. There was a finding that the personal information of government employees falls subject to the mandatory exemption in section 29(1) of *FOIP* unless the information is publicly available as set out in section 29(2)(p). [at paragraphs 30-34]

**SCHILLER V SASKATCHEWAN
(MINISTRY OF HEALTH), 2025
SKKB 85 (APRIL 22, 2026)
JUSTICE B. KLATT**



At A Glance

Exemptions

- Section 29 of *HIPA* – Use and Disclosure for Research

Other Issues at Play

- Purpose of the Legislation
- The Concept of Severance
- The Concept of De-Identification
- The Concept of Record Creation Does Not Exist in Saskatchewan

The Applicant sought information relating to the adverse effects of COVID-19 vaccine that the Ministry of Health began to compile in 2021. The information came directly from individuals who self-reported.

The Ministry then compiled the information onto a spreadsheet that had 18 columns. The Ministry disclosed certain columns but refused to disclose others.

The Commissioner recommended the disclosure of more information, but the Ministry refused to follow the Commissioner's recommendation. Since filing his appeal of the Ministry's decision to refuse disclosure, Mr. Schiller learned that the data used to create the spreadsheet came from information collected on Adverse Events Following Immunization forms (AEFI forms) that had been filled out by health care practitioners across the province once individuals began to report adverse effects. Mr. Schiller petitioned the court that he now required the data from these forms since his main interest is statistical information. He submitted that *The Health Information Protection Act*, SS 1999, c. H-0.021, as amended (*HIPA*) does not apply to a request for statistical information. He also brought his application pursuant to FOIP. He petitioned the court for an order that the Ministry de-identify the data so there would be no possibility of identification of the individuals who alleged adverse effects and release the data to him.

Purpose of the Legislation: *HIPA* contains a broad set of principles that apply to the rights of persons to access their own personal health information. The overarching goal of *HIPA* is the protection of personal health information. The trustees who hold that information have a duty to the persons to whom the information relates. By contrast, *FOIP* governs the public's right of access to records, excluding personal health information, in the possession of a government institution. [at paragraphs 38 and 39]

Section 29 of *HIPA* – Use and Disclosure for Research: This section of *HIPA* requires that the research project for which the statistical information is required be one that is approved by a research ethics committee approved by the Minister. Mr. Schiller provided no evidence of prior Ministerial approval. [at paragraph 51]

The Concept of Severance: Section 8 of *FOIP* mandates a head to provide access to as much of a record as can be reasonably severed without disclosing the information that is subject to an exemption. There is no corresponding duty under the *HIPA* regime, save for section 38 of *HIPA* that requires severance for an individual who seeks access to their own health record. [at paragraph 54]

The Concept of De-Identification: There is currently no duty upon the Ministry to de-identify the AEFI forms to facilitate access. Even if there was such a duty, any efforts to de-identify the AEFI forms would be impossible because they contain such a high degree of detailed medical and personal health information. [at paragraph 58]

The Concept of Record Creation Does Not Exist in Saskatchewan: Mr. Schiller asked for an order that the Ministry add new columns to the spreadsheet to contain information such as gender, race, age, prior health concerns. The court refused to compel the Ministry noting that there is no duty under *HIPA* or *FOIP* such that the Ministry should have to create a new record to suit the Applicant's request. [at paragraphs 59 and 67]

The appeal was dismissed.

Land Acknowledgement

We acknowledge our office operates on the lands of the First Nations who signed treaties 2, 4, 5, 6, 8, 10 and on the lands of the Metis.



Service and Accessibility Charter



✓ **Out Commitement to Service** ⁵

The Office of the Saskatchewan Information and Privacy Commissioner (OIPC) is an independent office of the Saskatchewan Legislative Assembly. We have a mandate to oversee compliance with the three following pieces of legislation:

- The Freedom of Information and Protection of Privacy Act (FOIP)
- The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP)
- The Health Information Protection Act (HIPA)

As part of our mandate, we:

- review access and correction decisions made by government institutions (FOIP), local authorities (LA FOIP) and trustees (HIPA) in their administration of the applicable laws; and
- conduct investigations when there is evidence of a privacy breach committed by those bound by the legislation.

Our office is an appeal body. Your first step is to work with the government institution, local authority or trustee to address your concerns and only to bring your concerns to the OIPC when they cannot be resolved within a reasonable period of time. ⁶

There is no charge for our services.

✓ **Our Values and Guiding Principles** ⁷

<i>Excellence</i>	<ul style="list-style-type: none">• To apply the highest standards of personal and business excellence, which includes high quality, and consistent and accurate work product.
<i>Fairness</i>	<ul style="list-style-type: none">• To provide an opportunity to be heard and to provide adequate information about our processes.• Communication is clear and suitable.• Decisions are free from personal interest or bias.
<i>Responsibility & Accountability</i>	<ul style="list-style-type: none">• We take responsibility for our actions and are accountable to each other and team objectives.• Externally, we are responsible and accountable to the Legislative Assembly and to those provide services to including Saskatchewan citizens.

⁵ OIPC acknowledges that this resource is adapted from resources by the Office of the Ontario Information and Privacy Commissioner (IPC Service Charter | Information and Privacy Commissioner of Ontario) and Office of the Privacy Commissioner of New Zealand (Office of the Privacy Commissioner | Our service charter).

⁶ See How do I resolve a complaint? and How do I get access to information?

⁷ Taken from OIPC's Annual Report.

<i>Integrity</i>	<ul style="list-style-type: none"> • We conduct ourselves internally and externally in an honest, trustworthy and reliable manner.
<i>Respect</i>	<ul style="list-style-type: none"> • We recognize and appreciate individuality and treat Citizens, public bodies/trustees and each other with respect, dignity and equality.

Our Service Approach with Citizens

How you can expect us to work with you	How we expect you to work with us
<ul style="list-style-type: none"> • We administer <i>FOIP, LA FOIP and HIPA</i> for the province of Saskatchewan. • Treat you with dignity and respect. • Clearly explain our role and an estimated timeline for our office to undertake a review or investigation. If we cannot become involved, we will tell you why and direct you, when able, to where you may get help. • We will need to discuss your request for review or your complaint with the applicable public body or trustee. • Consider both sides of the story. • Strive to be timely, but we cannot guarantee our timelines. • Treat all applicants and complainants fairly and without prejudice. • Be transparent about the progress of your file. • Welcome your feedback on how our office can improve. 	<ul style="list-style-type: none"> • Treat our staff with dignity and respect. • Prior to contacting our office, try to resolve your concern with the government institution, local authority or trustee. • Provide us with all important facts, information and required materials regarding your request for review or privacy complaint. • Be open, honest and truthful when communicating with our office or providing us with information. • Do not record us without our knowledge and consent. • Cooperate with our office and respond in the time periods set by our office. • Comply with OIPC's rules and procedures for conducting reviews and investigations. • Recognize that our office is impartial and unbiased. We seek representations from all sides. • Contact us with any concerns questions you may have and let us know how our office can improve.

Our Service Approach with Public Bodies & Trustees

How you can expect us to work with you	How we expect you to work with us
<ul style="list-style-type: none"> • We administer FOIP, LA FOIP and HIPA for the province of Saskatchewan. • Treat government institutions, local authorities and trustees’ representatives with respect. • Clearly explain our role and how our office can be involved in a review or investigation. • Advise you when our office has the authority or mandate to undertake a review or investigation and when it does not. • Clearly advise on our established, but reasonable timelines for you to provide our office with materials (e.g., records, submissions) and to respond to our questions. • Be thorough, fair and impartial in our conduct. • Consider both sides of the story. • Advise what documentation our office requires in a review or investigation, which can include, but is not limited to, records, submissions, evidence and organizational policies/procedures. • Be transparent about the progress of a review or investigation. • Welcome your feedback on how our office can improve. 	<ul style="list-style-type: none"> • Treat our staff with respect • Be open, honest and forthcoming when explaining your internal processes for decision making. • Cooperate with our office and respond in the time periods set by our office. Provide reasonable explanations when a timeline cannot be met or when requesting an extension. • Comply with OIPC’s rules and procedures for conducting reviews and investigations. • Comply with timelines set out by FOIP, LA FOIP or HIPA. • Be open to early resolution or mediation to informally resolve a review or privacy complaint that will be in the best interest of citizens. • Contact us with any concerns or questions and let us know how our office can improve.

Well-being of Our Staff

We have a duty to ensure the safety and wellbeing of our staff when they interact with anyone including members of the public. We have zero tolerance for threats or violence towards our staff. Threats include, but are not limited to:

- Using abusive, defamatory or offensive comments and language with OIPC staff.
- Intimidating or harassing OIPC staff by phone, email or in person.
- Asking OIPC staff inappropriate questions, including questions of a personal nature.
- Posting information about OIPC staff online.

When threats are perceived to have been made, we will respond by first issuing a warning.

If threats continue, including threats of violence, we will limit access to services.

If necessary, we will report a matter of concern to the police. We may disclose your personal information to the police to report threats of violence.

Our Commitment to Accessibility

- We are committed to building a workplace and organization that is accessible and inclusive for everyone.
- Our goal is to identify and work towards removing barriers so that all employees and members of the public can fully participate and access our programs, services and information. ⁸
- At intake we work with citizens to explore options for removing barriers that may exist, keeping in mind that many disabilities are invisible. Our Intake Officers gather relevant information to determine accommodation requirements on a case-by-case basis.
- We are prepared to work with individuals who require the use of Assistive Devices, Accessible Formats and Communication Supports (ASL interpreters, Braille, Audio, Large print), Service Animals, and Support Persons. ⁹

⁸ 2026 to 2028 Accessibility Plan, Office of the Privacy Commissioner of Canada, March 2, 2026, https://www.priv.gc.ca/en/accessibility/accessibility_2026-2028/.

⁹ Accessibility Standards, Ombudsman Ontario, March 2, 2026, <https://www.ombudsman.on.ca/en/about-us/policies/accessibility-standards>.

Definitions

The following definitions apply throughout this accessibility plan:¹⁰

Disability: Any impairment, or difference in physical, mental, intellectual, cognitive, learning, or communication ability. Disabilities can be permanent, temporary or can change over time.

Barrier: Anything that might hinder people with disabilities’ full and equal participation. Barriers can be architectural, technological, attitudinal, based on information or communications or can be the result of a policy or procedure.

Accessibility: The design of products, devices, services, environments, technologies, policies and rules in a way that allows all people with a variety of disabilities to access them.

How are we accessible?

Our Physical Space	Our Information/Communication Space
<ul style="list-style-type: none"> • We are accessible by elevator. • We have accessible washrooms. • Our office has wide hallways. • Our door handles are easily used by people with limited strength and dexterity. • Our office has counter service Appointments or meetings can be arranged in advance. 	<ul style="list-style-type: none"> • We will communicate by mail, email, telephone, videoconference or meet in office if pre-arranged. • We encourage individuals to contact our office by phone or through our intake email rather than by fax. • We strive to use clear, everyday language in our blogs and resources for our readers. • We work with applicants and complainants and adapt to their needs on a case-by-case basis as determined at intake. • We try to remove barriers by modifying how we accept submissions from clients to meet their individual needs basis. • We work with representatives, who with consent, can act on behalf of the applicant or complainant.

¹⁰ 2026 to 2028 Accessibility Plan, Office of the Privacy Commissioner of Canada, March 2, 2026, https://www.priv.gc.ca/en/accessibility/accessibility_2026-2028/. OR supra at footnote 1.