Office of the Information and
Privacy Commissioner of Alberta

Strategic Business Plan

2017-2020

Office of the Information and Privacy Commissioner

Vision

A society that values and respects access to information and personal privacy.

Mission

The Office of the Information and Privacy Commissioner's work toward supporting its vision includes:

- Advocating for the privacy and access rights of Albertans
- Ensuring public bodies, health custodians and private sector organizations uphold the access and privacy rights contained in the laws of Alberta
- Providing fair, independent and impartial reviews in a timely and efficient manner

Mandate

The Information and Privacy Commissioner is an independent Officer of the Legislature. The Commissioner reports directly to the Legislative Assembly of Alberta.

Through the OIPC, the Commissioner performs the legislative and regulatory responsibilities set out in the:

- *Freedom of Information and Protection of Privacy Act* (FOIP Act)
- *Health Information Act* (HIA)
- *Personal Information Protection Act* (PIPA)

The Commissioner oversees and enforces the administration of the three access and privacy laws to ensure their purposes are achieved.

The Commissioner's powers, duties and functions include:

- Providing independent review and resolution on requests for review of responses to access to information requests and complaints related to the collection, use and disclosure of personal and health information
- Investigating any matters relating to the application of the Acts, whether or not a review is requested
- Conducting inquiries to decide questions of fact and law and issuing binding orders
- Educating the public about the Acts, their rights under the Acts and access and privacy issues in general
- Receiving comments from the public concerning the administration of the Acts
- Giving advice and recommendations of general application respecting the rights or obligations of stakeholders under the Acts
- Engaging in or commissioning research into any matter affecting the achievement of the purposes of the Acts
- Commenting on the implications for access to information or for protection of personal privacy of proposed legislative schemes and existing or proposed programs
- Commenting on privacy impact assessments submitted to the Commissioner
- Commenting on the implications for access to or protection of health information
- Commenting on the privacy and security implications of using or disclosing personal and health information for record linkages or for the purpose of performing data matching

Goals and Initiatives for 2017-2020

The following goals and initiatives have been developed in response to current trends, issues and challenges.

Goal One: Enhanced access to information and protection of personal and health information by government and other regulated stakeholders

Access to Information

The importance of government transparency and accountability and the public's right to access information held by public institutions cannot be overstated. Access to information allows citizens to more effectively participate in the democratic process.

Governments continuously commit to "accountability," "transparency" and "openness." A common speaking point is that governments strive to be "open by default."

There have been movements globally to enhance open data and open government, such as commitments to disclose expenses and salary information among other data. Sometimes these commitments to openness are coupled with a desire to allow developers to use this information to create apps that will provide services to individuals. These are positive steps.

However, there are equally as many instances of government opaqueness and delays in responding to access requests. In Alberta, the OIPC has experienced an unprecedented number of requests for time extensions over the past few years, topping more than 100 such requests in the last fiscal year.

Meantime, there have been dozens of instances where public bodies, primarily government departments, did not meet the time limit to respond. In these cases, there simply has not been a response to an applicant's request for access.

Big Data and Cybersecurity

A persisting concern for privacy rights and one that continues to increase exponentially centres on the seemingly unbridled ability for governments, health information custodians and businesses to collect, use and disclose limitless amounts of personal and health information about individuals.

The collection of massive amounts of information coupled with the number of connected devices collecting personal information raise concerns about transparency and the loss of individual control over personal and health information, and about the security of the information at issue.

As recent studies have found, approximately 60% of devices do not properly explain to customers how their information is being used[1]. Meantime, half of all websites and apps directed at children and youth share personal information with third parties and 67% collect children's personal information[2].

Information has no borders once collected and shared. This raises numerous complexities in terms of how access and privacy laws apply to personal or health information.

Privacy Breaches and Offences

Alberta remains the only private sector jurisdiction in Canada to have mandatory breach reporting and notification provisions in force. In 2014, the Legislative Assembly of Alberta passed amendments to HIA for mandatory breach reporting and notification, as well as new offence provisions for failing

[1] Global Privacy Enforcement Network's 2016 Privacy Sweep. OIPC News Release: "Alberta Participates in Global Privacy Sweep on 'Internet of Things'".

[2] Global Privacy Enforcement Network's 2015 Privacy Sweep. OIPC News Release: "Global Privacy Sweep Finds Half of Websites, Apps Are Sharing Children's Personal Information".

to report a breach, but these have not come into force.

As the health sector prepares for amendments to come into force and many issues around breaches persist in the private sector, the OIPC is receiving nearly one breach report for every calendar day of the year – more than 300 breach reports in the last fiscal year.

In particular, the issue of employee "snooping" continues in Alberta, most notably in the health sector where in 2015-16 alone four individuals faced charges for unauthorized access to health information under HIA.

Information Sharing

Information sharing initiatives for service delivery continues to be an issue of concern for the OIPC. Although these initiatives are underway in all sectors, new and revised information sharing programs in the health sector highlight the complexities.

The benefits of sharing health information are myriad, particularly in emergency situations and to more efficiently provide care to patients. However, electronic access to health information also raises a number of data security issues.

In addition, inconsistent legislative requirements for government departments, health providers and non-profit organizations adds complexities when trying to provide services to individuals who rely on various sectors to receive the supports and services they need.

These situations create confusion as to what can or should be done with respect to personal or health information. The OIPC is aware of situations where information that could appropriately be shared is not due to this confusion and resulting fear of contravening privacy laws.

Initiatives

- 1.1 Advocate open, transparent and accountable government through legislative reform, compliance reviews and promotion of proactive disclosure of government records.
- 1.2 Develop a strategy to address the increasing number of privacy breaches and offences.
- 1.3 Provide guidance on access and privacy implications of information sharing initiatives.
- 1.4 Provide training, education and guidance.

Goal Two: Increased awareness of access and privacy rights through engagement with Albertans

Children and Youth Education

With the number of new tools, games and gadgets being developed that are coming up with new ways to collect, use and disclose personal information about children without knowing exactly how that information is being collected, shared and monetized, access and privacy education is equally dynamic.

When discussing these issues, most individuals agree; we need to teach children and youth about how to navigate online spaces while respecting personal privacy and recognizing the benefits provided online.

Collaboration with a variety of organizations across Canada is a primary way in which the OIPC participates in education programs and working to develop resources to help educators, among others, teach children and youth about access and privacy issues.

Citizen Knowledge on Access and Privacy

Education and awareness concerns are not limited to children and youth as all age groups need to know how to protect their privacy while understanding their access rights.

When thinking about privacy breaches, for example, anyone is susceptible to any type of breach – from human error to malware and phishing attacks. The harms vary in these instances. Many individuals are affected by health information breaches while others experience financial fraud or identity theft as a result of attacks on ecommerce websites, for example.

Again, leveraging collaboration with other Information and Privacy Commissioners, as well as other organizations, is one way in which the OIPC strives to reach a wider audience through the development of resources and providing training.

Initiatives

- 2.1 Develop a strategy to interact with and engage citizens on navigating access and privacy issues.
- 2.2 Identify and facilitate opportunities to educate youth on access and privacy issues.
- 2.3 Research and consider options to establish an access and privacy advocate role within OIPC.

Goal Three: Efficient, effective, timely processes

Meeting Stakeholder Expectations

The 2015-16 fiscal year saw a 13% increase (1,639) in the number of cases opened by the OIPC over 2014-15 (1,448).

The OIPC's ability to resolve these cases is challenged by the number of parties involved, an increase in the number of represented parties, challenges from regulated stakeholders and more complex issues, such as technology-related or cross-sectoral cases. These factors increase the time required to investigate, assess and resolve cases.

The OIPC continuously analyzes and prioritizes incoming cases to keep up with these pressures, and works to improve processes to ensure cases are resolved as quickly as possible.

For example, the OIPC has been refining early resolution processes. Files are assessed in terms of complexity and the amount of work required to resolve them in order to assign them to an appropriate resolution process. The files selected for early resolution tend to deal with a moderate to minimal number of records (e.g. 300 records or less) with few exceptions to disclosure applied by public bodies, custodians or organizations.

Staff Policies and Procedures

Ensuring internal policies and procedures meet the unique needs of the OIPC's office environment continues through the development of new and updated office policies and procedures that align with the organizational plan.

Technological Advancements

The OIPC continues to search for and analyze various options to reduce its reliance on paper systems and to more efficiently process certain types of case files. However, any new technology must be considered in light of office resources while maintaining the security of information submitted by stakeholders.

Initiatives

- 3.1 Conduct an organizational business process review.
- 3.2 Continue to develop and communicate organizational policies and procedures to support staff.
- 3.3 Research options and consider implementation of a paperless office.

Goal Four: Staff members are engaged and knowledgeable

Ubiquitous Technology

Technology – from biometrics to mobile devices, geo-location tracking software to the interoperability of information systems, social media to open data initiatives – is possibly the most significant factor affecting access to information and privacy today. In particular, the proliferation of electronic devices, the amount of data that can be stored on those devices, their increased portability, and the number of technology-related privacy breaches, give rise to concern.

It is imperative that OIPC staff be positioned to provide comprehensive and informed reviews of information systems and initiatives, and proactive guidance and direction to stakeholders who are grappling with new technologies.

Access and Privacy Law and Policy

In addition to keeping up with new technologies, OIPC staff also need to be aware of access and privacy issues that cross all sectors, as well as jurisdictions. With the advent of public, private and health partnerships, issues are no longer confined to any one sector.

Even more importantly, there are opportunities for each sector to learn from the others. For example, the advanced technical work that is being completed in the health sector related to interoperable systems, self-serve health portals, and the de-identification of health information for research purposes, has the potential to lead and guide in the public and private sectors. The mandatory privacy impact assessment requirement under HIA is another model that may have application outside of the health sector.

OIPC staff are required to have deep knowledge of all three Acts, and issues arising in each sector. The OIPC continues to identify and provide staff with opportunities to further develop expertise working with the three Acts. The OIPC will also actively work to develop technology expertise as well as broad knowledge and understanding of access and privacy issues.

Performance Management and Staff Collaboration

The OIPC established a performance management program to address the unique considerations of the work staff are in engaged in.

In addition, the office continues to explore ways to ensure staff have opportunities to collaborate and share knowledge on a variety of topics.

Changes to the OIPC's office structure were made in 2013-14 to assist the office in responding to issues and trends. In particular, the new structure provides an opportunity for the OIPC to review its processes to improve consistency, enhance efficiencies, and ultimately increase timeliness.

These goals are reflected in the organizational plan to which individual performance plans align.

Initiatives

- 4.1 Continue to identify and facilitate opportunities for communication and consultation.
- 4.2 Continue implementation of a performance measurement program.
- 4.3 Identify and provide training and awareness opportunities to ensure staff members are supported and remain abreast of emerging access and privacy issues and technologies.

Summary of Goals and Initiatives for 2017-2020

1. Enhanced access to information and protection of personal and health information by government and other regulated stakeholders

- 1.1 Advocate open, transparent and accountable government through legislative reform, compliance reviews and promotion of proactive disclosure of government records.
- 1.2 Develop a strategy to address the increasing number of privacy breaches and offences.
- 1.3 Provide guidance on access and privacy implications of information sharing initiatives.
- 1.4 Provide training, education and guidance.

2. Increased awareness of access and privacy rights through engagement with Albertans

- 2.1 Develop a strategy to interact with and engage citizens on navigating access and privacy issues.
- 2.2 Identify and facilitate opportunities to educate youth on access and privacy issues.
- 2.3 Research and consider options to establish an access and privacy advocate role within OIPC.

3. Efficient, effective, timely processes

- 3.1 Conduct an organizational business process review.
- 3.2 Continue to develop and communicate organizational policies and procedures to support staff.
- 3.3 Research options and consider implementation of a paperless office.

4. Staff members are engaged, knowledgeable and expert

- 4.1 Continue to identify and facilitate opportunities for communication and consultation.
- 4.2 Continue implementation of a performance measurement program.
- 4.3 Identify and provide training and awareness opportunities to ensure staff members are supported and remain abreast of emerging access and privacy issues and technologies.