Office of the Information and
Privacy Commissioner of Alberta

Strategic Business Plan

2016-2019

Office of the Information and Privacy Commissioner

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

Through the Office of the Information and Privacy Commissioner (OIPC), the Commissioner performs the legislative and regulatory responsibilities set out in the following laws:

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

The Commissioner oversees and enforces the administration of FOIP, HIA and PIPA (the Acts) 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
- 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 freedom of 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

Vision

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

Mission

The OIPC'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

Environmental trends and issues

A number of environmental trends and issues shape and influence the access and privacy landscape that impacts work of the OIPC.

Personal and health information online

One of these trends is the rise of social media and the increasing degree to which **individuals are willing to share information about themselves online**, whether to obtain something tangible (goods and services, shopping discounts), to feel connected to others, or to engage with society. Individuals are sharing vast amounts of personal information through blogs, social networks, e-mail, cell phone GPS signals, call detail records, Internet search indexing, digital photographs, video archives, and through online purchases.

Governments and businesses also value online communication with citizens. This is evidenced by an increased emphasis on **citizen engagement** and consultation strategies, often employing the use of web tools (blogging, Tweeting, online forums, YouTube, Facebook pages etc.) to get messages out and to receive feedback.

Moreover, the public is increasingly willing to use the Internet and social media to advocate or lobby for causes.

Information online knows no boundaries. It flows across borders and around the globe, with technology as the common denominator that connects everything.

The prevalence of mobile devices, including smart phones, laptops, tablet computers and USB keys, means that **information is always on the go**, never stationary, and certainly not confined to any one jurisdiction. Geo-location technologies, such as Radio Frequency Identification Devices (RFIDs) and GPS tracking, are specifically designed to monitor the location of things, such as mobile devices, or vehicles, as well as people.

All of these devices, and many more, are increasingly connected to the Internet and to each other. One of the most significant emerging trends in technology is said to be the Internet of Things. Some projections suggest that up to 100 billion uniquely identifiable objects will be connected to the Internet by 2020.

Information sharing for service delivery

The OIPC is currently seeing an ongoing focus on **multi-agency citizen-centred service delivery**. This global trend seeks to replace the traditional delivery of public services by myriad, disparate government agencies with a network of public, private and non-profit groups that come together to achieve a common mission or program outcome. This service delivery model recognizes that the social and economic challenges facing citizens are complex and require interaction between government and community-based providers. It may also hold some promise for reducing government inefficiencies and bureaucracy. The foundation that underpins multi-agency citizen-centred delivery of government services is **information sharing** beyond the sectoral boundaries of private, public, and health, and, in some cases, across provincial and national borders.

In Alberta's health sector, efforts have been underway for years to encourage and facilitate the implementation of electronic medical records, and to build the **provincial electronic health record** (Alberta Netcare), which enables sharing

of health information among health care providers.

The potential benefits of sharing health information through a provincial electronic health record for patients and society in general are significant, including ensuring that comprehensive and timely patient information is available to provide better care and reduce workplace inefficiencies. A vast electronic repository of health information also holds incredible research potential for improved treatments, quality of care, patient safety and other purposes such as policy development. Patient health information has value.

Governments, businesses and health custodians alike are looking to technology solutions to improve service delivery, maximize efficiencies and reduce costs. Technology solutions provide opportunities to enhance the privacy and security of personal or health information, when reasonable steps are taken to consider and mitigate risks.

Integrating information systems to support shared service delivery, as well as the need to uniquely identify someone in the online environment, requires diligent attention to **identity management.** Biometric technologies, including facial recognition, fingerprinting, palm vein and iris scanning, are under constant development and are being deployed in new and previously unforeseen ways. Reflecting our interconnectedness and borderless society, provincial, national and international initiatives are underway that are focused on standardization and interoperability of identity management systems.

Big data information sharing

Businesses, health information custodians and government have the ability to collect an enormous amount of information about citizens. This, coupled with the development of exceptional technologies that allow vast amounts of data to be stored and analyzed in ways never previously contemplated, has led to a phenomenon that has come to be known as **"Big Data."**

Big Data refers to the ability to track and analyze everything from online purchases to the latest Twitter trending topics. It offers massive opportunities for real-time intelligence about responses to products, services and even political decisions. The advantages for businesses are obvious; companies want to listen to what is being said about them and leverage this information for marketing or reputation management purposes. Big Data enhances a business's ability to meet customer expectations, provide better customer service, and improve consumer products. Consumer information has value.

For governments, Big Data offers opportunities for improved evidence-based decision-making, research, and enhanced program and service delivery. Citizens' information has value.

Transparency and accountability

At the same time as government is re-evaluating how it delivers programs and services, we increasingly hear commitments to **"accountability," "transparency" and "openness."** The principles of government transparency and accountability and the public's right to access information held by public institutions is as current and essential as ever. It is access to information that allows citizens to scrutinize government decisions and actions and, as a result, to more fully and effectively participate in the democratic process.

The emphasis on transparency and accountability goes hand in hand with the rise of global **open government and open data** movements.[1] Internationally,

[1] Open government, as used here, is more generally about the proactive and routine release of

provincially and at municipal levels, governments are committing to initiatives that advance open government and open data agendas.

One of the fundamental principles of the open data movement is that information datasets must be available in standard machine-readable formats, to facilitate analysis and manipulation of the data, as well as linking or data matching with datasets from multiple sources, including governments in other jurisdictions.

Another emerging trend is to facilitate open government and open data by developing protocols to ensure that information systems are designed and built with principles of access in mind.

These initiatives underscore that information about government decision making is essential to democracy. Albertans value information about government.

information to citizens; open data refers to offering government data in a more useful and machine-readable format to enable citizens, the private sector and non-government organizations to leverage it in innovative and value-added ways.

Privacy breach reporting

One trend from 2014-15 that should be noted is the amount of attention privacy breaches received, provincially, nationally and internationally. In Alberta, the OIPC saw a significant increase in the number of self-reported breaches. Public bodies under FOIP reported 41 breaches to the OIPC, which is up from 22 the previous year and represents an increase of 86%. The number of breaches self-reported by custodians under the HIA also increased by 12% (from 68 to 76), and PIPA self-reported breaches increased by 44% (from 96 to 138).

Almost every week saw a new report of another incident, leading to calls for legislative changes to require mandatory breach notification and reporting.

Alberta's PIPA includes **mandatory breach reporting** requirements. Amendments to the HIA to include mandatory breach reporting and notification received Royal Assent in May 2014, but have yet to be proclaimed in force. FOIP does not require mandatory breach reporting or notification.

Federally, the government introduced Bill S-4 in April 2014, which included proposed amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) to include mandatory breach notification provisions similar to those found in Alberta's PIPA[2]. In British Columbia, the Special Committee reviewing PIPA tabled its report in February 2015, which included a recommendation for mandatory breach notification. In Ontario, amendments to the *Personal Health Information Protection Act* were tabled in September 2015 to include mandatory breach reporting. In addition, Newfoundland and Labrador recently enacted breach reporting provisions in their *Access to Information and Protection of Privacy Act*, which is a first for public bodies in a Canadian jurisdiction.

[2] Bill S-4 received royal assent on June 18, 2015. However, provisions related to mandatory breach notification do not come into force until regulations have been enacted.

Implications for access and privacy

Coordinated or integrated cross-sectoral and often highly technical initiatives offer many potential benefits for individuals and society. However, these initiatives also raise a host of access, privacy and data security issues.

For initiatives that involve multiple participating stakeholders, for example, it is imperative to establish **appropriate governance and accountability** structures to ensure that basic responsibilities under access and privacy legislation can be met (e.g. limiting collection, restricting use, responding to access requests, privacy breaches, etc.).

Coordinated or integrated service delivery across sectors may also run into **inconsistent legislative requirements**. For example, health custodians, unlike public bodies or private sector businesses, are legally required to submit a Privacy Impact Assessment (PIA) to the OIPC for review and comment before implementing new information systems. Non-profit participants may or may not be subject to access and privacy legislation. Private sector organizations have a duty to report certain privacy breaches to the OIPC, while other participating stakeholders may not have the same obligation. Inconsistent legislative requirements can result in risks to personal and health information not being identified and reasonably mitigated.

Establishing **legislative authority to share information can be complex**, and is made even more so when participants are subject to more than one of the Acts (for example, a health professional, such as a psychologist or physiotherapist, in independent practice may normally be subject to PIPA but if contracted to the Workers' Compensation Board, he or she may fall under FOIP). When operational staff does not understand the application of the Acts, this creates confusion as to what they can or should do with respect to personal or health information. The OIPC hears about situations where information that could appropriately be shared is not due to this confusion and resulting fear of contravening privacy laws.

Transparency can also be an issue. **Complex, integrated information systems are often not well understood** by sophisticated users, much less the individuals whose personal or health information may be used by them. Given this, it may be a challenge for individuals to exercise their rights under access and privacy laws to complain about the collection, use or disclosure of their information, or to request access or correction of it.

Large databases and advanced analytics provide a **temptation to use information for new purposes** other than those for which the information was collected. There are situations in which individuals would likely not object to their information being used for other purposes, for example, the use of health information for research purposes. Studies have shown that most patients are not concerned that their information will be used for research purposes, and would in fact be surprised if this were *not* the case. What they do expect, however, is that health information that is used for research purposes will be subject to strict protocols and safeguards, including that the information be de-identified. Alberta's HIA was designed to facilitate use of health information for research within such a system of controls.

Individuals are often more concerned with **secondary use of information for public safety purposes**. Massive amounts of information collected, warehoused, and integrated, are sometimes seen as a silver bullet, guaranteeing a safer society. Often, new initiatives will trade off privacy rights in the quest for more security. Any such re-purposing of information for public

safety, or new collections of information, must be scrutinized closely and demonstratively necessary. The risk is that often only a single initiative is considered at any one time, and the slippery slope trend towards a surveillance society goes unnoticed.

Vast databases of information also present a tempting target for identity thieves and hackers. At one time, most **privacy breaches** reported to the OIPC related to human error and mailing and transmission errors (fax and email). Now, we see a concerning shift to targeted large database hacks and phishing attempts to gain access to personal information for nefarious purposes. Many breaches are technology related in that they involve the loss or theft of computer equipment, and particularly unencrypted mobile devices. Technology related breaches are troubling in that the number of affected individuals can be enormous.

A particularly disturbing occurrence is where a trusted user abuses his or her access privileges to "snoop" on others. While most authorized users of information systems are properly trained and respectful of privacy laws, **unauthorized access** by authorized users continues to occur and can be very difficult to identify.

The OIPC continues to consider privacy breaches that are wilfully or knowingly committed as **possible offences** under the Acts. The OIPC will investigate and pursue prosecution of those individuals who choose to abuse their access privileges and the trust placed in them by improperly accessing personal or health information.

Finally, **open government and open data** initiatives, while providing opportunities for citizens to have routine access to information about government decision-making, and reducing the burden on already strained formal access to information processes, can also give rise to privacy risks. Careful thought and planning must go into any decision to publish machine searchable data to ensure privacy is protected. Personal identifiers may be removed, but there are many examples where **seemingly disparate information elements can be combined and linked back to specific individuals**. It can be difficult to determine in advance which seemingly harmless data elements can be combined in such a manner.

Challenges for the OIPC

Meeting public and stakeholder expectations for timely resolution of complaints and requests for review

The OIPC continues to see an increase in the volume and complexity of cases received. In 2014-15, the office reported 1448 new cases opened, a 12% increase over 2011-12.

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

Self-reported breach files are a priority, particularly if there is a real risk of significant harm and affected individuals have not been notified. In 2014-15, the OIPC saw a 37% increase in self-reported breaches to the OIPC. Mandatory breach reporting and notification amendments made to the HIA[3] are expected to significantly increase the number of breaches reported to the OIPC in the future.

The number of wilful privacy breaches that the OIPC considers as possible offence investigations is also rising. Offence investigations are an important compliance activity that require a high level of expertise and significant resourcing to complete.

The Commissioner has authority to open investigations on her own motion to examine compliance with any provision of the Acts. In 2014-15, 58 investigations generated by the Commissioner were opened – a 69% increase over the previous year.

The OIPC prioritizes these types of cases to try to ensure timely resolution. However, as the number and complexity of these cases continues to rise, OIPC staff workloads are increasingly made up of high-priority files.

The Government of Alberta's review of the FOIP Act also has the potential to significantly impact the OIPC's ability to meet expectations for timely resolution of cases. While the results of the review and any proposed amendments are not known at this time, the Commissioner's submission to the review process recommended mandatory breach reporting and notification for public bodies subject to FOIP.

The Commissioner's submission also recommended that Privacy Impact Assessments (PIAs) be mandatory for certain kinds of initiatives. The Office's experience under the HIA (which has a mandatory PIA requirement for health custodians) has demonstrated the value of completing PIAs for new initiatives, particularly those that are focused on implementing new technologies or for information sharing initiatives. Should such amendments be made, however, the OIPC will be challenged to complete reviews in a timely manner with existing staff resources.

Changes to the OIPC's office structure were made in 2013-14 to assist the Office in responding to the challenges identified

[3] Passed in May 2014, and will come into force on proclamation.

above. In particular, the new structure provides an opportunity for the OIPC to review its processes to improve consistency, enhance efficiencies, and ultimately increase timeliness.

A process to triage complaints was implemented in 2014-15, and now resolves over 50% of complaints channeled through this route. The average to resolve cases in this process is 15 business days from the date the triage manager evaluates the file.

Additional process changes introduced in 2014-15 are intended to reduce the time to resolve requests for review, and improve and streamline communicating the results of mediation and investigation. A new case management system was also rolled out, which will further enhance the office's ability to track and report on files, analyze processes, and identify opportunities for improvement.

While these changes have had a positive impact on effectiveness and efficiency, the OIPC expects that anticipated amendments to both the HIA and the FOIP Act will bring new challenges for timely resolution.

Proactive identification and oversight of access and privacy issues

As already described, current stakeholder initiatives are increasingly complex, sophisticated, cross-sectoral, highly technical, interconnected and not always transparent to the individuals whose information is collected, used and disclosed.

The OIPC's traditional, primarily reactive, oversight model (responding to individual complaints and requests for review) is not adequate to provide effective oversight for these initiatives, or to reassure Albertans that their privacy is respected and protected. Because these initiatives are not always transparent to the public, it is not realistic for the OIPC to rely on complaints or requests for review as an indicator of legislative compliance. In fact, complaints submitted to the OIPC generally do not reflect the access and privacy issues and initiatives that stakeholders are primarily engaged with.[4]

Given the above, as part of the OIPC's restructuring in 2013-14, the Office established a Compliance and Special Investigations unit to specifically focus on proactive compliance, including PIA reviews and compliance investigations of systemic issues.

The need to proactively identify and address privacy and access issues has also been reflected in the OIPC's recent education and outreach efforts. Beginning in 2013-14, and continuing in 2014-15, the OIPC has focused resources on providing training workshops and seminars, rather than larger legislation-specific conferences. Workshops this past year focused on PIA training and breach response, with the intention of improving the quality of submissions to the OIPC over time. Demand for this training is expected to continue as the Physician Office System Program has been phased out, and given anticipated and potential amendments to the HIA and FOIP.

The OIPC has also allocated resources towards the Commissioner's mandate to engage in or commission research in order to get ahead of issues and challenges facing stakeholders, and to contribute to increased awareness, understanding and improved compliance. The results of two research studies were made available in 2014 and 2015, to provide guidance on information sharing and the increased

[4] OIPC Stakeholder Survey 2012.

trend towards "deputizing the private sector".

Given the success of these initiatives to date, the OIPC will continue to look for opportunities to provide meaningful education, advice, research and training in advance, or in the absence, of receiving complaints.

Positive collaboration with public bodies

Upholding Albertans' access and privacy rights is a shared responsibility between the public bodies, custodians and organizations who administer the laws and the OIPC who provides oversight. Albertans are assured timely access to information both through the public body processing the request, and, where necessary, the OIPC's oversight of the process.

In 2014-15, the OIPC made a number of internal adjustments to improve the effectiveness and efficiency of processes, and continues to look for further opportunities to improve. At the same time, however, the OIPC is finding: 1) public bodies missing OIPC set deadlines to provide requested information, and 2) public bodies claiming "privilege" as a reason to refuse to provide records to the OIPC.

Resourcing may be a factor affecting a public body's ability to meet deadlines, but every extension of a deadline results in further delays to timely resolution. With respect to claims of privilege, it is currently the case that approximately 80 cases in the office are related to claims of privilege. The resolution of these matters is delayed when the OIPC is unable to obtain information required to exercise its statutory review function.

Despite the above, the OIPC continues to look for opportunities to positively collaborate and provide guidance and support to improve delivery of the shared responsibility the OIPC has with public bodies to uphold Albertans access rights.

OIPC staff has the information, training and expertise required to provide effective oversight and guidance

It is clear from the environmental trends and issues discussed earlier that technology underpins many of the significant initiatives that are underway in the public, private and health sectors.

Ubiquitous 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 privacy and access to information 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.

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.

Particularly with the advent of public/private/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 PIA requirement under the HIA is another model that may have application outside of the health sector.

OIPC staff is required to have deep knowledge of all three Acts, and issues arising in each sector. The OIPC continues to consider 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.

Many OIPC staff members have a long history with the Office. This means they have in-depth knowledge of the development and growth of the OIPC and the many issues that have been considered and resolved over the years.

Given the number, variety and increased complexity of issues before the OIPC, it is not feasible to rely on long-term staff members to be the source of corporate knowledge.

In 2012, the OIPC identified a need to more effectively manage corporate knowledge in order to improve the Office's capabilities and enable better decision-making. A project to modernize the OIPC's case management system was rolled out in January 2015. The new system significantly enhances the OIPC's ability to maintain corporate knowledge, understand and report on the work of the OIPC, and make decisions about process changes and allocation of resources.

Goals and Key Strategies: 2016-2019

The following goals and key strategies have been developed in response to current environmental trends and issues, and to address the challenges described above.

GOAL 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.

GOAL 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.

GOAL 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.

GOAL 4: Staff members are engaged, knowledgeable and expert

4.1 Continue to identify and facilitate opportunities for communication and consultation.

4.2 Develop and implement 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.