Office of the Information and
Privacy Commissioner of Alberta

ANNUAL REPORT
2018-19

Office of the Information and
Privacy Commissioner of Alberta

Office of the Information and
Privacy Commissioner of Alberta
410, 9925 - 109 Street, NW
Edmonton, AB T5K 2J8

Phone: 780.422.6860
Toll Free: 1.888.878.4044
Fax: 780.422.5682
Email: generalinfo@oipc.ab.ca
Twitter: @ABoipc

www.oipc.ab.ca

NOVEMBER 2019

Office of the Information and
Privacy Commissioner of Alberta

November 2019

Honourable Nathan Cooper
Speaker of the Legislative Assembly
325 Legislature Building
10800 - 97 Avenue
Edmonton, AB T5K 2B6

Dear Mr. Speaker:

I am honoured to present to the Legislative Assembly the Annual Report of the Office of the Information and Privacy Commissioner for the period April 1, 2018 to March 31, 2019.

This report is provided in accordance with section 63(1) of the *Freedom of Information and Protection of Privacy Act*, section 95(1) of the *Health Information Act* and section 44(1) of the *Personal Information Protection Act*.

Sincerely,

Original signed by
Jill Clayton
Information and Privacy Commissioner

Table of Contents

Commissioner's Message

When I appeared before the Standing Committee on Legislative Offices at the end of November last year I reported that my office had officially reached a breaking point in terms of our ability to keep up with the ever increasing volume of cases. Despite the success of a number of initiatives that improved our efficiency and streamlined our processes, we were losing the battle to provide timely reviews and investigations.

Amendments to the *Health Information Act* that came into force on August 31, 2018 significantly impacted what was already a strained situation.

At the time I appeared before the Standing Committee, we were anticipating that these amendments would increase our workload by approximately 500 net new case files – for a total of approximately 624 HIA breach reports a year, instead of the 130 we had routinely received for the last few years.

As a result, our 2019-2020 budget estimate included a request for five new staff to address the additional workload we expected to see. In my comments to the Standing Committee, I said:

> These new positions will be used to tackle the backlog in the office and maintain our current timelines in reviewing matters that Albertans bring before the office. Our new normal is to anticipate well over 2,000 cases a year, and with our current staffing levels this just is not sustainable.

I was gratified that the all-party Committee approved our budget estimate.[1]

[1] In May 2019, the Commissioner was notified by the Government of Alberta that because the legislation required to make the budgets of the Legislative Officers and government a reality was being delayed to the fall of 2019, the OIPC's funding for 2019-20 (from April 1, 2019 to November 30, 2019) was being held to the 2018-19 budget forecast, not the amount approved by the Standing Committee.

As it turns out, our estimate of the additional cases was far too conservative. We ultimately received 674 breach reports under HIA in 2018-2019, including only seven months of mandatory breach reporting. We are, in fact, consistently receiving approximately 90 HIA breach reports each month, putting us on target to receive well over 1,000 in the first full year (from August 31, 2018 to August 30, 2019).

Many of these breaches are relatively easy to address, requiring only some follow-up by OIPC staff to ensure health custodians have contained the breach, responded appropriately (i.e. notified affected individuals), and taken steps to prevent similar events from re-occurring in the future.

A significant number of these cases, however, are much more serious, involving wilful disregard for the law and affecting, in some cases, hundreds if not thousands of Albertans. These cases often become offence investigations, and can result in significant court-imposed fines for offending individuals. Offence investigations are time sensitive and resource-intensive but, in my view, are among the most important investigations my office takes on. Unfortunately, we have gone from having 5-6 active offence investigations open at any one time to over 20 as of September 30, 2019, with approximately 70 flagged as potential offences.

The number of self-reported breaches under HIA is just the most obvious factor contributing to the OIPC's increased workload. In addition to the 407% increase in HIA breaches last year, we also saw a 112% increase in public sector breaches voluntarily reported under the *Freedom of Information and Protection of Privacy Act*, and a 26% increase in private sector breaches under the *Personal Information Protection Act*.

The number of privacy impact assessments (PIAs) submitted to the OIPC also increased to 1,090, from 792 the previous year. Many of these PIAs related to complex province-wide information system projects, which take significant time and resources to review.

Overall, my office opened 3,273 cases in 2018-19, representing a 33% increase over the 2,467 cases we opened in 2017-2018. The 2,467 opened cases in 2017-18 led me to tell the Standing Committee that we had reached our "breaking point".

With yet another substantial increase in caseload, while maintaining a status quo budget for salaries, wages and benefits since 2013-14, the situation is now dire. It is impossible for the OIPC to provide timely and effective independent oversight of access and privacy matters in Alberta without additional resources.

At the same time, society has developed an enhanced awareness of our digital age, which has increased individuals' expectations of information delivery and thrust information and privacy rights into the spotlight. Privacy and access issues – breaches, GDPR, open government, smart cities, artificial intelligence, wearable health devices – routinely make front page news. Citizens expect to have information at their fingertips and enjoy the numerous potential benefits of technology and innovation, but they also expect that their personal information will be protected and handled with respect and in accordance with the law.

Albertans' increased awareness and understanding of information and privacy rights is extremely positive and should be encouraged – it is, in fact, essential for a healthy democracy and engaged citizenry. However, these rights cannot be protected without effective and timely independent oversight. And without adequate resourcing, this oversight is currently at risk.

Thank you, as always, to my colleagues in the office, for their dedication to upholding the access and privacy rights of Albertans.

Jill Clayton
Information and Privacy Commissioner

ABOUT THE OFFICE

Mandate

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

Through the Office of the Information and Privacy Commissioner (OIPC), the Commissioner performs the legislative and regulatory responsibilities set out in Alberta's three access and privacy laws.

Freedom of Information and Protection of Privacy Act

The *Freedom of Information and Protection of Privacy Act* (FOIP Act) applies to more than 1,100 public bodies, including provincial government departments, agencies, boards and commissions, municipalities, Métis settlements, drainage districts, irrigation districts, housing management bodies, school boards, post-secondary institutions, public libraries, police services, police commissions and health authorities.

The FOIP Act provides a right of access to any record in the custody or under the control of a public body, subject to limited and specific exceptions. The Act also gives individuals the right to access their own personal information held by public bodies and to request corrections to their own personal information. The Act protects privacy by setting out the circumstances in which a public body may collect, use or disclose personal information.

Health Information Act

The *Health Information Act* (HIA) applies to more than 54,900 health custodians, including Alberta Health, Alberta Health Services, Covenant Health, nursing homes, physicians, registered nurses, pharmacists, optometrists, opticians, chiropractors, podiatrists, midwives, dentists, denturists and dental hygienists.

HIA also applies to "affiliates" who perform a service for custodians, such as employees, contractors, students and volunteers. Custodians are responsible for the information collected, used and disclosed by their affiliates.

HIA allows health services providers to exchange health information to provide care and to manage the health system.

HIA protects patients' privacy by regulating how health information may be collected, used and disclosed, and by establishing the duty for custodians to take reasonable steps to protect the confidentiality and security of health information. The Act also gives individuals the right to access their own health information, to request corrections, and to have custodians consider their wishes regarding how much of their health information is disclosed or made accessible through the provincial electronic health record information system (i.e. Alberta Netcare).

Personal Information Protection Act

The *Personal Information Protection Act* (PIPA) applies to provincially-regulated private sector organizations, including businesses, corporations, associations, trade unions, private schools, private colleges, partnerships, professional regulatory organizations and any individual acting in a commercial capacity.

PIPA protects the privacy of clients, customers, employees and volunteers by establishing the rules for the collection, use and disclosure of personal information by organizations.

PIPA seeks to balance the right of the individual to have their personal information protected with the need of organizations to collect, use or disclose personal information for reasonable

purposes. PIPA also gives individuals the right to access their own personal information held by organizations and to request corrections.

Commissioner's Powers, Duties and Functions

The Commissioner oversees and enforces the administration of 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
- Reviewing privacy breach reports submitted by private sector organizations and health custodians as required under PIPA and HIA, and when voluntarily submitted by public bodies
- Reviewing and commenting on privacy impact assessments submitted to the Commissioner
- Receiving comments from the public concerning the administration of the Acts
- Educating the public about the Acts, their rights under the Acts, and access and privacy issues in general
- Engaging in or commissioning research into any matter affecting the achievement of the purposes of the Acts
- Commenting on the access and privacy implications of existing or proposed legislative schemes and programs
- Giving advice and recommendations of general application respecting the rights or obligations of stakeholders under the Acts
- 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

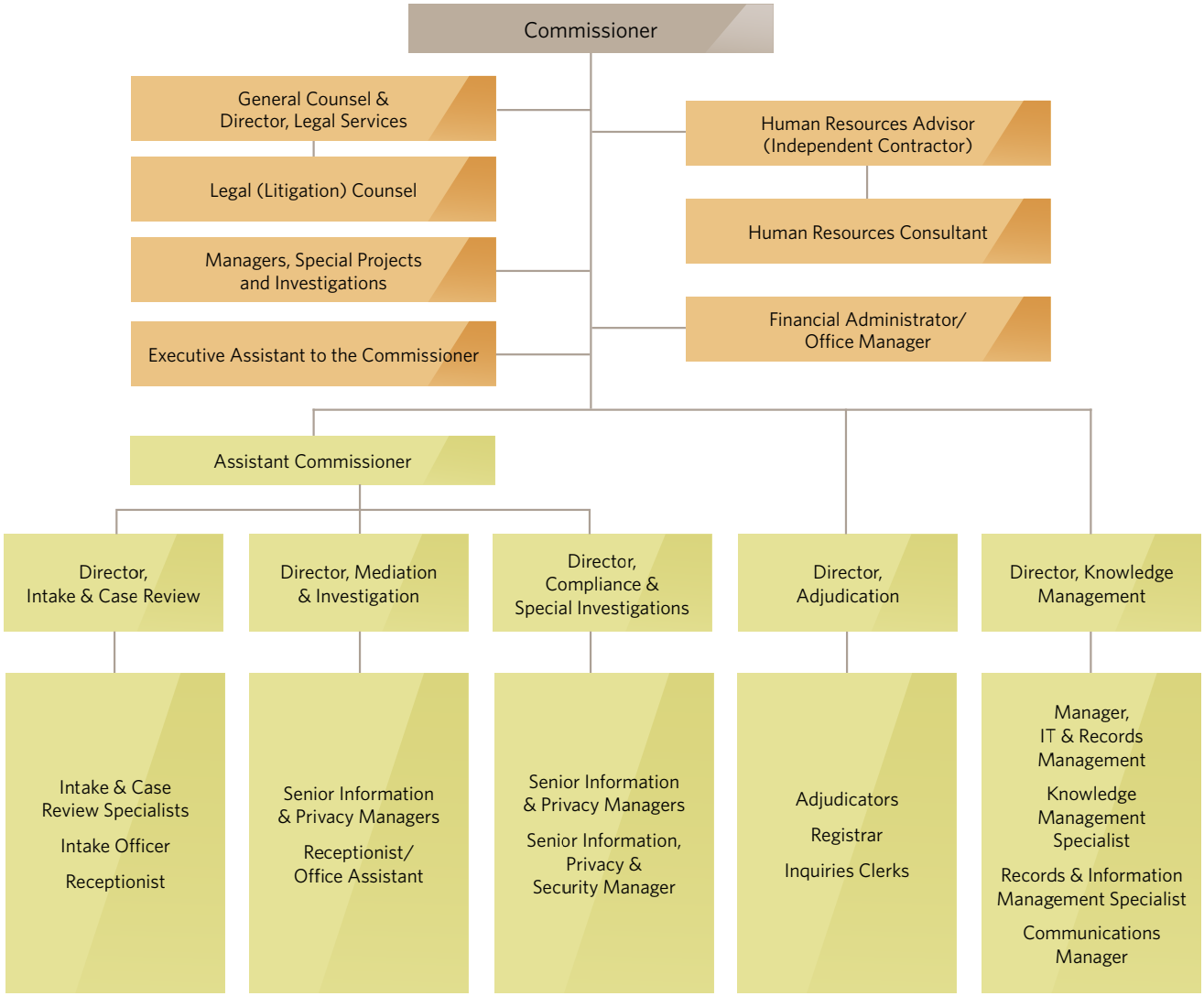
A society that values and respects access to information and personal privacy.

MISSION

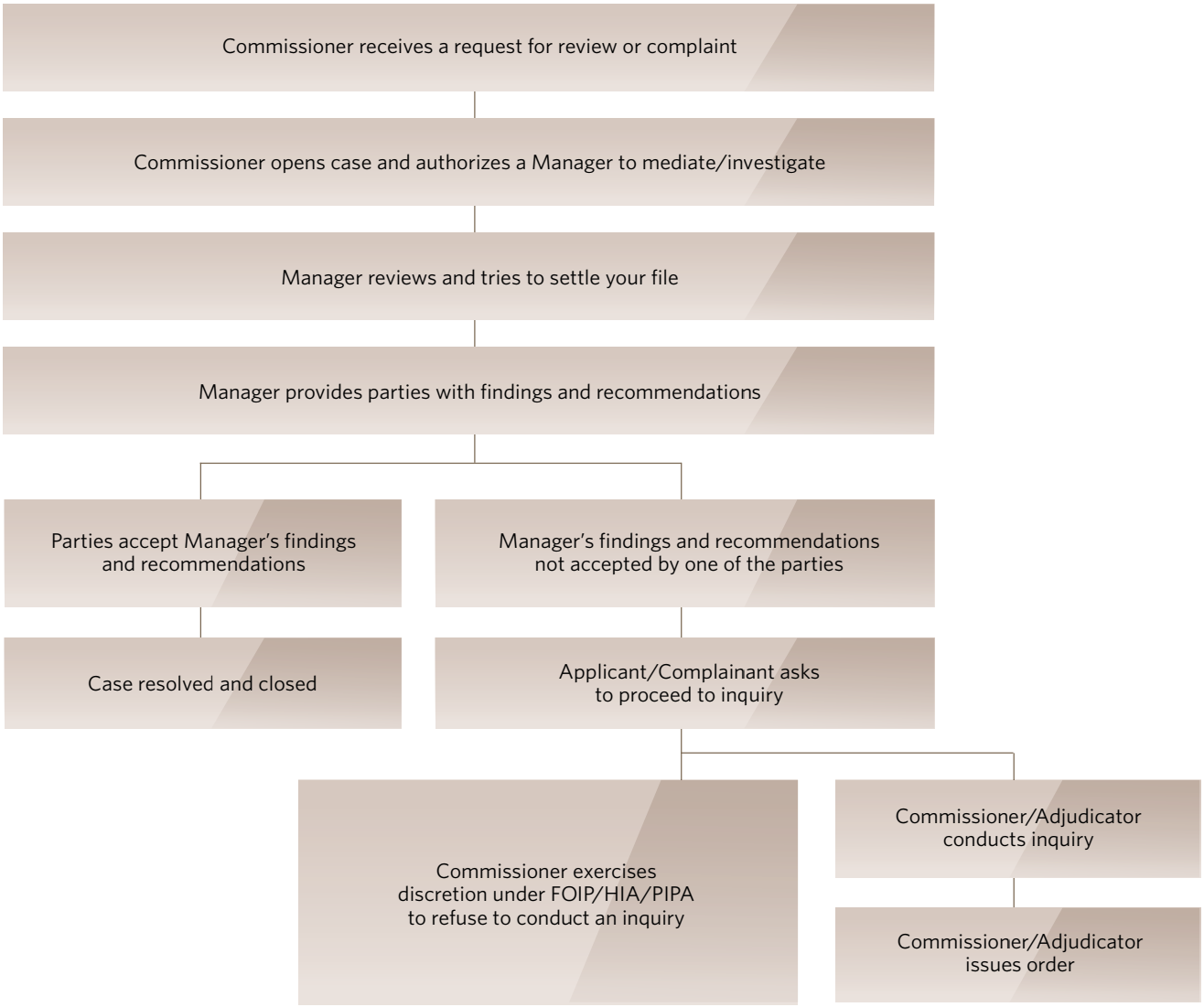
Our work toward supporting our vision includes:

- Advocating for the access and privacy 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

OIPC Organizational Structure 2018-19



Request for Review and Complaint Process



OIPC as a Public Body

FOIP REQUESTS TO THE OIPC

As a public body under the FOIP Act, the OIPC receives access requests on occasion.

In 2018-19, the OIPC received seven general information requests and three personal information requests under the FOIP Act. The OIPC responded to all of the requests within 30 days.

Individuals who disagree with the access request response received from the OIPC can request a review of the OIPC's decision. An External Adjudicator is then appointed by Order-in-Council to determine whether the OIPC properly excluded records subject to an access request.

There are three outstanding requests for review awaiting the appointment of External Adjudicators. Two matters reported on in the 2017-18 Annual Report remain outstanding. The third request for review was submitted in 2018-19.

OIPC PRIVACY MATTERS

In 2018-19, the OIPC conducted seven investigations into internal incidents involving potential privacy breaches.

Incident 1

A letter from the OIPC was mistakenly placed into an envelope that was sent to the wrong public body. Upon receipt of the letter, the FOIP Coordinator of the public body notified the OIPC of the error.

It was determined there was no real risk of significant harm to the affected individual whose name and mailing address was in the correspondence. Steps were immediately taken to contain the breach and assurances were received that the letter was securely destroyed.

Incident 2

The OIPC used an old and incorrect address from its case management system when sending correspondence to an organization about a complaint, rather than using the organization's new address provided by the complainant.

The correspondence was opened and read before it was returned to the OIPC by the individual who inadvertently received the correspondence.

No real risk of significant harm to the affected individual was determined; however, the complainant was notified about the incident.

The correspondence contained the name, address and signature of the complainant, information about the complaint, and names of involved third parties.

Incident 3

Two letters were inadvertently stuffed into the same envelope. In addition to the letter a custodian was intended to receive, the custodian received another letter meant for a different custodian. The letters were about the OIPC's review of the custodians' practice management systems. The letter, which included a custodian's name and business contact information, was returned to the OIPC by the custodian who received it in error.

There was no real risk of significant harm to the affected individual as the information was about the individual's business.

Incident 4

A letter was sent from Adjudication to an applicant's former mailing address, which had not been updated in the OIPC's case management system prior to the file being transferred to Adjudication. It was discovered that a staff member did not follow OIPC policy related to changing addresses. The information at issue included the affected individual's name, address and revealed that they had a file before the OIPC.

No real risk of significant harm was determined. Considering personal information was sent to the wrong address and the letter was not located, the OIPC decided to notify the affected individual about the incident. Staff were asked to review the OIPC's address change policy for when similar circumstances arise.

Incident 5

A representative for a staff member requested documents concerning the staff member. A package was sent to the representative who then reported to the OIPC that the package contained information about other OIPC staff members.

No real risk of significant harm to affected individuals was determined. The representative promptly returned the information to the OIPC. The individuals affected were notified.

Incident 6

Contents of a file attached to a letter meant for one public body were sent to the wrong public body, and vice versa. One of the files did not contain personal information; the other file revealed the name of an applicant and the nature of their access request.

The documents were viewed by staff responsible for responding to access requests. The public body that received the file with the applicant's personal information confirmed they securely shredded the document.

No real risk of significant harm to the affected individual was determined. The OIPC was assured the document was securely destroyed. No notification was given to the affected individual.

Incident 7

The auto-fill feature in an email was used by an OIPC staff member to populate the "cc" field, but the incorrect individual was selected, which was not noticed prior to the email being sent.

No real risk of significant harm to the affected individual was determined. The personal information at issue included a complainant's name and the fact that he made a complaint. The email was received by a privacy professional who immediately notified the OIPC of the error and promptly took steps to securely delete the email.

PROACTIVE TRAVEL AND EXPENSES DISCLOSURE

The OIPC continues to disclose the vehicle, travel and hosting expenses of the Commissioner, and the travel and hosting expenses of the Assistant Commissioner and Directors on a bi-monthly basis. The disclosures are available at www.oipc.ab.ca.

PUBLIC SECTOR COMPENSATION TRANSPARENCY ACT

The *Public Sector Compensation Transparency Act* requires public sector bodies, including the OIPC, to publicly disclose compensation and severance provided to an employee if it is more than $125,000 in a calendar year, as adjusted according to the Act. For the 2017 calendar year, the threshold was adjusted to $127,765. In addition, other non-monetary employer-paid benefits and pension must be reported.

This disclosure is made annually by June 30 and is available at www.oipc.ab.ca.

PUBLIC INTEREST DISCLOSURE (WHISTLEBLOWER PROTECTION) ACT

There were no disclosures received by the OIPC's designated officer under the *Public Interest Disclosure Act* in 2018-19.

Financial Overview

For the 2018-19 fiscal year, the total approved budget for the OIPC was $6,916,491. The total cost of operating expenses and capital purchases was $6.8 million. The OIPC returned $92,780 (1.34% of the total approved budget) to the Legislative Assembly.

TOTAL ACTUAL COSTS COMPARED TO BUDGET

	VOTED BUDGET	ACTUAL	DIFFERENCE
Operating Expenses*	$ 6,916,491	$ 6,823,711	$ 92,780
Capital Purchases	-	-	-
Total	$ 6,916,491	$ 6,823,711	$ 92,780

*Amortization is not included

Salaries, wages, and employee benefits make up approximately 84% of the OIPC's operating expenses budget. In 2018-19, payroll related costs and technology services were under budget. Legal fees, external adjudication, other contract services, and supplies and services were over budget.

TOTAL ACTUAL COSTS COMPARED TO PRIOR YEAR

	2018-2019	2017-2018	DIFFERENCE
Operating Expenses	$ 6,823,711	$ 6,668,403	$ 155,308
Capital Purchases	-	20,032	-20,032
Total	$ 6,823,711	$ 6,688,435	$ 135,276

Total costs for operating expenses and equipment purchases, including capital assets, increased by $135,276 from the prior year. The increase was primarily due to an increase in salaries, wages, and employee benefits, legal fees, offence investigations and other contract services. These increases were offset by a decrease in materials, supplies and technology services, and a decrease in capital expenditures.

TRENDS & ISSUES

Health Information Breaches

After much anticipation, health information breach reporting and notification requirements came into force under HIA on August 31, 2018. This change showed that no matter how much you can prepare for something to happen, it is difficult to predict what may result.

As of March 31, 2019, the OIPC was receiving approximately 20 breach reports per week from health custodians under the new requirements. Carried over a full year, that would equal approximately 1,040 breach reports, an increase of eight times more breaches than what had been voluntarily reported in prior fiscal years. (Approximately 130 breach reports per year were received from custodians between 2015-16 and 2017-18.)

Not only did the increase completely shift the number of breaches the OIPC would need to process and review, certain breach types came as a surprise. Approximately 20% of breach reports received were from pharmacists that had health and safety implications in that patients were receiving the wrong prescriptions from pharmacists due to labeling errors. Another issue that came to the fore was misguided requisition forms for lab tests.

Perhaps unsurprisingly, given the 10 convictions for knowingly accessing health information under HIA to date, there were also more snooping breaches reported (i.e. unauthorized access to health information by authorized users of health information systems). Cyberattacks were also reported more frequently, which is a concern that will need to be monitored.

Overall, however, the changes benefit Albertans, as the Commissioner said in a news release when the date was set for the amendments to come into force:[2]

> This is good news for the privacy of Albertans. I'm pleased that individuals affected by a health information breach will now have the right to be notified, which will bring Alberta in line with a majority of Canadian provinces and territories. Health information is among the most sensitive of personal details anyone can share. When health information is breached, it's important that people know so that they can take steps to protect themselves from potential harm.

Mandatory breach reporting and notification regimes are in place in most Canadian provinces. What types of breaches and how they need to be reported to Information and Privacy Commissioners' offices differs, however, so it is difficult to glean too much information for comparison purposes. That said, a couple of provinces publish data that shows Alberta is not alone in trying to prevent or reduce the number of health information breaches occurring.

[2] The OIPC issued a news release in May 2018 to announce that the changes were coming into force on August 31, 2018. The news release is available at www.oipc.ab.ca/news-and-events/news-releases/2018/mandatory-privacy-breach-reporting-coming-to-albertas-health-sector.aspx.

In Ontario, 2018 was the first full year of mandatory breach reporting and notification.[3] There are seven categories of breaches that must be reported to the Commissioner by Ontario's health custodians under its *Personal Health Information Protection Act* and related regulation. There are also annual statistics that custodians must report to the Commissioner, such as a breach that does not meet the threshold of reporting it to the Commissioner.

In total, there were 506 breaches reported to Ontario's Commissioner, 120 of which were snooping incidents, 15 cyberattacks, and 371 other types of unauthorized collection, use or disclosure of health information. Custodians also experienced, per annual statistics requirements, 11,278 incidences of personal health information breaches, more than 10,000 of which involved unauthorized disclosure from misdirected faxes, emails and other means (i.e. breaches that did not meet the criteria for reporting to the Commissioner).

Nova Scotia also has differences in the breaches health custodians are required to report to the Commissioner and for when notifying affected individuals. Only breaches that a custodian has determined do not require notification to affected individuals are reported to Nova Scotia's Commissioner. In 2018-19, 865 breaches with no potential for harm or embarrassment were reported to the Commissioner.[4] Since breaches that require notification to affected individuals, upon determination by the custodian, are not reported to the Commissioner, statistics on the number of breaches where individuals were notified are not readily available in the Commissioner's annual report.

Alberta's health sector is not alone in finding ways to stem the number of breaches occurring in the health system. Education and guidance will be key in this area going forward.

[3] The Information and Privacy Commissioner of Ontario reported on the first full year of mandatory breach reporting in Ontario's health sector in the 2018 Annual Report. The report is available at www.ipc.on.ca/wp-content/uploads/2019/06/ar-2018-e.pdf#page=28.

[4] The Office of the Information and Privacy Commissioner for Nova Scotia reported on the breaches requiring notification to the Commissioner in its 2018-19 Annual Report. The report is available from https://oipc.novascotia.ca/.

Importance of Records Management to the Right of Access to Information

There have been several developments that have proven the importance of records management to effective access to information systems.

Findings in four OIPC investigation reports since 2015-16 have reinforced the message that effective records management is central to strong and efficient access to information systems, including three reports issued in 2018-19.

Some of these findings include:

- No direct monitoring or review of the management or destruction of records kept at a government minister's office (Investigation Report F2016-IR-01).[5]
- No clear documented rationale for the destruction of records at a ministry and confusing records schedules (Investigation Report F2016-IR-01).
- Inconsistent documentation of how records searches were conducted by government departments (Investigation Report F2018-IR-01).[6]
- Not fully understood records management policies and procedures by employees at a government agency, and no training program to understand the difference between official and transitory records (Investigation Report F2018-IR-02).[7]
- No compliance program was established to ensure that staff members have received appropriate training and are following the records management plan for their department (Investigation Report F2019-IR-01).[8]
- Most staff members retained more email records than required causing difficulty in finding responsive information for business, legal, regulatory or FOIP Act responsibilities (Investigation F2019-IR-01).
- Inconsistency in how official email records were being stored by staff members in government departments (Investigation Report F2019-IR-01).

To respond to recurring findings on records management training, misunderstandings about official vs. transitory records, and deleting transitory email records, the OIPC issued "Guidelines on Managing Emails" and a tip sheet based on the guidelines in March 2019.[9] These education efforts will continue but other persisting records management issues may require legislative changes.

Other jurisdictions have experienced similar issues over the years.

[5] The OIPC's Investigation Report F2016-IR-01 is available at www.oipc.ab.ca/media/649105/f2016-ir-01.pdf.

[6] The OIPC's Investigation Report F2018-IR-01 is available at www.oipc.ab.ca/media/938544/F2018-IR-01.pdf.

[7] The OIPC's Investigation Report F2018-IR-02 is available at www.oipc.ab.ca/media/938547/F2018-IR-02.pdf.

[8] The OIPC's Investigation Report F2019-IR-01 is available at www.oipc.ab.ca/media/993311/f2019-ir-01.pdf.

[9] The OIPC announced the release of the "Guidelines on Managing Emails" and an associated tip sheet in a news release. The news release is available at www.oipc.ab.ca/news-and-events/news-releases/2019/oipc-releases-investigation-into-management-of-goa-emails.aspx.

A 2013 report by the Information and Privacy Commissioner for British Columbia found a number of responses to access requests resulted in "no responsive records".[10] The British Columbia government was also embroiled in what was colloquially known as the "triple delete scandal" that resulted in one former staffer being charged with two counts of wilfully making false statements to mislead, or attempt to mislead.[11]

In Ontario, top officials were eventually convicted in a matter where Ontario's former Information and Privacy Commissioner found that political officials broke access and privacy law by deleting all emails related to the cancellation of gas plants.[12]

In December 2018, the Information Commissioner of Canada opened an investigation into the Department of National Defence based on allegations the department inappropriately withheld information during the processing of access to information requests.[13] The allegations were the subject of a high-profile court case in which the defence in the criminal trial of Vice Admiral Mark Norman had difficulty attaining records involving decisions leading up to Norman's charges.

Nearly every jurisdiction has experienced situations in which allegations of government officials using personal devices to conduct government business have been made or individuals received "no responsive records" responses to access requests.

Taken together, these examples illustrate or reinforce why the Commissioner made records and information management recommendations during the Government of Alberta's consultations on its review of the FOIP Act in 2013. One recommendation was to ensure that all records are covered in records schedules. A second recommendation was to legislate a duty to document.

The duty to document recommendation calls for a statutory obligation for public bodies to "create such records as are reasonably necessary to document their decisions, actions, advice, recommendations and deliberations". A joint resolution was also issued in 2016 by Canada's Information Commissioners that called on governments to legislate a duty to document.

In British Columbia, a duty to document was recently created under the *Information Management Act*. However, a government ministry is responsible for investigating compliance with that law, not the Information and Privacy Commissioner for British Columbia.[14]

The Commissioner will continue to speak about the importance of effective records management to the right of access in Alberta. Recommendations for a duty to document, with independent oversight under the FOIP Act, and for all records to be covered in records retention and disposition schedules will also be reiterated.

[10] The Office of the Information and Privacy Commissioner for British Columbia's Investigation Report F13-01 is available at www.oipc.bc.ca/investigation-reports/1510.

[11] The Office of the Information and Privacy Commissioner for British Columbia's Investigation Report F15-03 is available at www.oipc.bc.ca/investigation-reports/1874.

[12] The Information and Privacy Commissioner of Ontario's special investigation report "Deleting Accountability: Records Management Practices of Political Staff" is available at www.ipc.on.ca/wp-content/uploads/2016/08/2013-06-05-Deleting-Accountability.pdf.

[13] The Information Commissioner of Canada's news release to announce the investigation into the Department of National Defence is available at www.oic-ci.gc.ca/en/resources/news-releases/information-commissioner-launches-systemic-investigation-department.

[14] In May 2019, the Information and Privacy Commissioner for British Columbia issued a statement to oppose the lack of independent oversight of the duty to document, as a result of allegations that the Minister responsible for oversight of the *Information Management Act* was in breach of that Act. That statement is available at www.oipc.bc.ca/news-releases/2312.

Smart Cities

Smart cities is a topic on which several privacy trends and issues from prior annual reports converge. Artificial intelligence and machine learning, ethical assessments in big data initiatives, the internet of things, information sharing, and deputizing the private sector are central to smart city initiatives and the debates surrounding them.

Over the past two years, certain projects and a national competition made smart cities a conversation topic in mainstream media and privacy circles alike.

The Waterfront Toronto-Sidewalk Labs partnership created a perfect storm of the issues to consider to move smart cities projects forward, and will offer a case study for how to develop large-scale, data-driven municipal projects.

Sidewalk Labs, a subsidiary of Alphabet Inc., the parent company of Google, amidst international debate about the influence of technology in our daily lives and democracies, partnered with Waterfront Toronto, a neighbourhood in Canada's largest city, who together envision a multibillion dollar data-driven community using countless data inputs, including personal information, to improve public services with hopes to be a model for future developments. Needless to say, there are layers of complexity involved.

Several of the public policy questions for the Waterfront Toronto-Sidewalk Labs project centre on data governance, data ethics, and public consultation and trust.

The privacy debate on the Waterfront Toronto-Sidewalk Labs project was in part the impetus for a joint letter from Canada's federal, provincial and territorial privacy protection authorities in response to Infrastructure Canada's Smart Cities Challenge.

In November 2017, the Government of Canada launched its Smart Cities Challenge in an effort to engage "communities across the country to develop bold and ambitious ideas to improve the lives of their residents using data and connected technology."[15] More than 200 communities participated and until Canada's privacy protection authorities wrote a letter to the federal Minister of Infrastructure and Communities in April 2018 discussions about privacy risks and mitigation controls in smart cities projects were not at the forefront.[16]

The letter stated:

> We appreciate the potential value of innovative smart city initiatives, such as allowing communities to more effectively address the challenges of urbanization and allocate resources accordingly. We do however urge you to ensure that this initiative, in supporting and encouraging innovation, requires project proposals to directly build in privacy protections. This is especially the case given that finalists from most jurisdictions will be subject to applicable access and privacy laws. In those jurisdictions yet to include municipalities under their access and privacy legislation, the insistence on these protections is even more vital.

[15] The Government of Canada's backgrounder on the Smart Cities Challenge is available at www.canada.ca/en/office-infrastructure/news/2019/05/backgrounder-the-government-of-canada-announces-winners-of-the-smart-cities-challenge.html.

[16] The letter from Canada's privacy authorities is available at www.oipc.ab.ca/media/933140/letter_smart_cities_challenge_apr2018.pdf.

Canada's Privacy Commissioners outlined several privacy risks and identified various privacy and security measures to mitigate those risks in the letter. They concluded by recommending that Infrastructure Canada include in its evaluation criteria for final proposals a consideration of privacy implications by the finalists. The guidance and recommendation was heeded by Infrastructure Canada. Privacy was a component that finalists needed to consider.

Smart cities may prove to be a topic where debate on prior privacy trends and issues will be accelerated in the coming years as municipalities tackle day-to-day issues, big and small, with the use of data. These daily influences on people's lives could affect how policymakers consider privacy rights in a variety of contexts.

BY THE NUMBERS

Totals Opened/Closed

(excluding Intake cases)

33% | 5%

INCREASE IN TOTAL CASES OPENED/CLOSED

3,273 total opened files in 2018-19; 2,467 in 2017-18

2,405 total closed files in 2018-19; 2,293 in 2017-18

Totals Opened/Closed under HIA

(excluding Intake cases)

83% | 14%

INCREASE OF HIA CASE TOTALS

1,865 opened HIA files in 2018-19; 1,018 in 2017-18

1,145 closed HIA files in 2018-19; 1,002 in 2017-18

Privacy Impact Assessments under HIA

37%

INCREASE OF PIAS OPENED UNDER HIA

1,059 opened PIAs in 2018-19; 771 in 2017-18

Total Breach Reports Opened

158%

INCREASE OF BREACH REPORTS OPENED UNDER HIA, PIPA AND FOIP

1,070 breach reports opened in 2018-19;
414 in 2017-18

407% ↑ HIA | 26% ↑ PIPA | 112% ↑ FOIP

Total Breach Reports Closed

47%

INCREASE OF BREACH REPORTS CLOSED UNDER HIA, PIPA AND FOIP

638 breach reports closed in 2018-19;
434 in 2017-18

137% ↑ HIA | 10% ↓ PIPA | 66% ↑ FOIP

DEEMED REFUSAL ORDERS UNDER FOIP

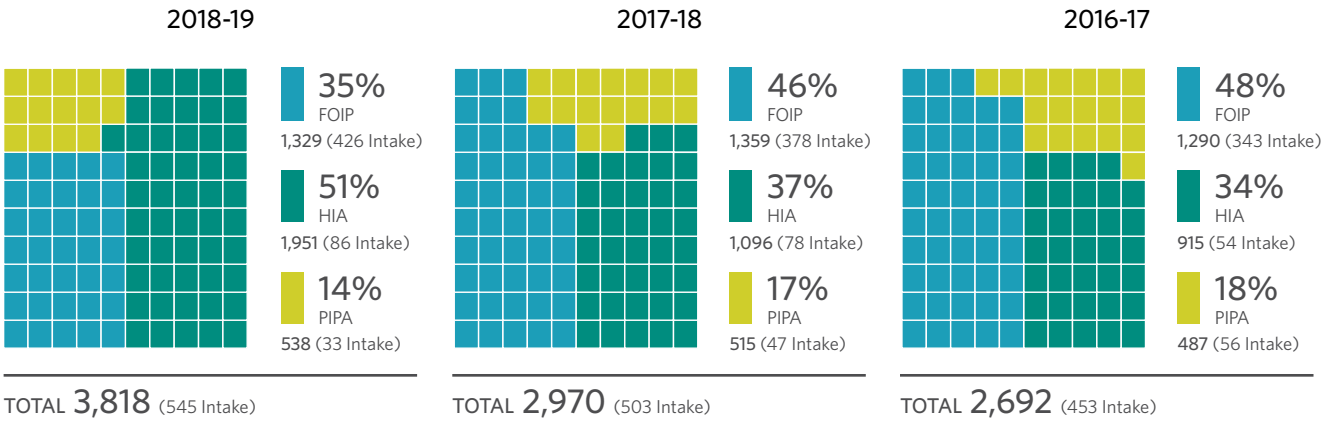
30

TIME EXTENSION REQUESTS UNDER FOIP

226

GRAPH A: TOTAL CASES OPENED

Three Year Comparison



GRAPH B: TOTAL CASES CLOSED

Three Year Comparison

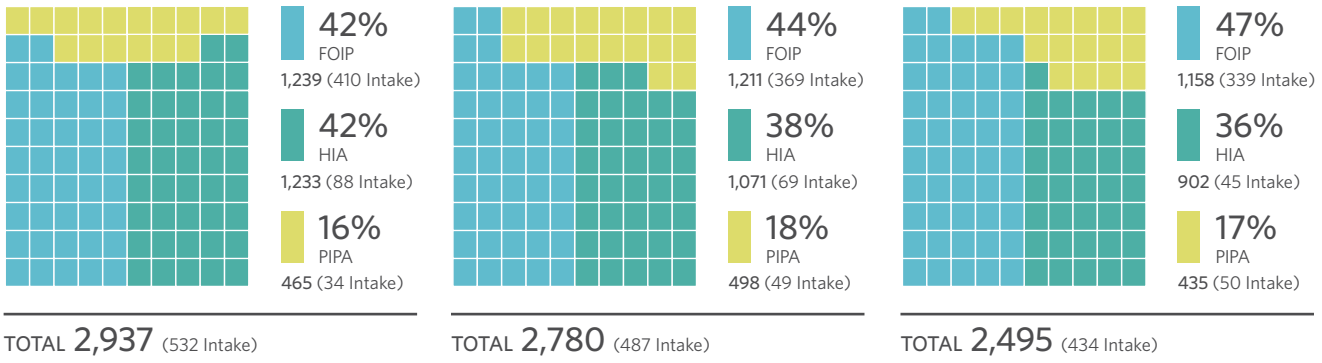


TABLE 1: CASES OPENED BY CASE TYPE

FOIP	2018-2019	2017-2018	2016-2017
Advice and Direction	1	1	2
Authorization to Disregard a Request	9	21	10
Complaint	91	96	92
Disclosure to Commissioner (Whistleblower)	0	0	0
Engage in or Commission a Study	0	1	0
Excuse Fee	16	9	10
Investigation Generated by Commissioner	8	10	27
Notification to OIPC	7	3	3
Offence Investigation	3	3	1
Privacy Impact Assessment	23	18	23
Request Authorization to Indirectly Collect	0	0	1
Request for Information	23	22	23
Request for Review	358	454	430
Request for Review 3rd Party	32	65	22
Request Time Extension	226	228	253
Self-reported Breach	106	50	50
Subtotal	**903**	**981**	**947**
Intake cases	426	378	343
Total	**1,329**	**1,359**	**1,290**

HIA	2018-2019	2017-2018	2016-2017
Advice and Direction	0	0	0
Authorization to Disregard a Request	3	0	0
Complaint	43	56	70
Engage in or Commission a Study	0	0	0
Excuse Fee	1	0	1
Investigation Generated by Commissioner	11	1	2
Notification to OIPC	0	0	0
Offence Investigation	11	3	7
Privacy Impact Assessment	1,059	771	583
Request for Information	39	23	37
Request for Review	24	31	30
Request Time Extension	0	0	1
Self-reported Breach	674	133	130
Subtotal	**1,865**	**1,018**	**861**
Intake cases	86	78	54
Overall Total	**1,951**	**1,096**	**915**

PIPA	2018-2019	2017-2018	2016-2017
Advice and Direction	1	0	0
Authorization to Disregard a Request	3	5	2
Complaint	112	119	159
Engage in or Commission a Study	0	0	0
Excuse Fee	0	0	0
Investigation Generated by Commissioner	7	6	6
Notification to OIPC	0	0	0
Offence Investigation	0	0	2
Privacy Impact Assessment	8	3	5
Request for Advanced Ruling	1	1	0
Request for Information	31	16	17
Request for Review	51	87	78
Request Time Extension	1	0	0
Self-reported Breach	290	231	162
Subtotal	**505**	**468**	**431**
Intake cases	33	47	56
Total	**538**	**515**	**487**

Notes

(1) See Appendix A for a complete listing of cases opened in 2018-19.

(2) Only FOIP allows a third party to request a review of a decision to release third party information to an applicant.

(3) Intake cases include determining whether parties coming to the OIPC are properly exercising the rights set out in FOIP, HIA and PIPA; whether the matters or issues identified by the parties are within the Commissioner's legislative jurisdiction; and investigating and trying to resolve certain requests or complaints.

TABLE 2: CASES CLOSED BY CASE TYPE

FOIP	2018-2019	2017-2018	2016-2017
Advice and Direction	0	1	2
Authorization to Disregard a Request	6	7	4
Complaint	82	83	69
Disclosure to Commissioner (Whistleblower)	0	1	0
Engage in or Commission a Study	0	1	0
Excuse Fee	14	8	8
Investigation Generated by Commissioner	31	19	15
Notification to OIPC	7	3	3
Offence Investigation	0	0	0
Privacy Impact Assessment	12	17	24
Request Authorization to Indirectly Collect	0	0	1
Request for Information	24	18	21
Request for Review	316	372	352
Request for Review 3rd Party	23	37	23
Request Time Extension	231	225	251
Self-reported Breach	83	50	46
Subtotal	**829**	**842**	**819**
Intake cases	410	369	339
Total	**1,239**	**1,211**	**1,158**

HIA	2018-2019	2017-2018	2016-2017
Advice and Direction	0	0	0
Authorization to Disregard a Request	0	0	0
Complaint	81	58	48
Engage in or Commission a Study	0	0	0
Excuse Fee	0	1	0
Investigation Generated by Commissioner	5	16	25
Notification to OIPC	0	0	0
Offence Investigation	6	4	1
Privacy Impact Assessment	669	707	576
Request for Information	30	26	37
Request for Review	18	48	23
Request Time Extension	0	0	1
Self-reported Breach	336	142	146
Subtotal	**1,145**	**1,002**	**857**
Intake cases	88	69	45
Total	**1,233**	**1,071**	**902**

PIPA	2018-2019	2017-2018	2016-2017
Advice and Direction	0	0	0
Authorization to Disregard a Request	5	2	3
Complaint	108	126	121
Engage in or Commission a Study	0	0	0
Excuse Fee	0	0	0
Investigation Generated by Commissioner	2	3	9
Notification to OIPC	0	0	0
Offence Investigation	0	2	1
Privacy Impact Assessment	0	4	4
Request for Advanced Ruling	0	1	0
Request for Information	30	15	16
Request for Review	66	54	67
Request Time Extension	1	0	0
Self-reported Breach	219	242	164
Subtotal	**431**	**449**	**385**
Intake cases	34	49	50
Total	**465**	**498**	**435**

Notes

(1) See Appendix B for a complete listing of cases closed in 2018-19.

(2) A listing of all privacy impact assessments accepted in 2018-19 is available at www.oipc.ab.ca.

(3) Only FOIP allows a third party to request a review of a decision to release third party information to an applicant.

(4) Intake cases include determining whether parties coming to the OIPC are properly exercising the rights set out in FOIP, HIA and PIPA; whether the matters or issues identified by the parties are within the Commissioner's legislative jurisdiction; and investigating and trying to resolve certain requests or complaints.

TABLE 3: PERCENTAGE OF CASES CLOSED BY RESOLUTION METHOD

Under FOIP, HIA and PIPA, only certain case types can proceed to Inquiry if the matters are not resolved at mediation/investigation. The statistics below are those case types that can proceed to Inquiry (Request for Review, Request for Review 3rd Party, Request to Excuse Fees and Complaint files).

RESOLUTION METHOD	NUMBER OF CASES (FOIP)	NUMBER OF CASES (HIA)	NUMBER OF CASES (PIPA)	TOTAL	%
Resolved by Mediation/Investigation	323	87	149	559	79%
Resolved by Order or Decision	82	0	10	92	13%
Resolved by Commissioner's decision to refuse to conduct an Inquiry	7	10	8	25	4%
Withdrawn during Inquiry process	18	0	5	23	3%
Discontinued during Inquiry process	5	2	2	9	1%
Total	435	99	174	708	100%

FOIP Orders: 74 (81 cases); **FOIP Decisions:** 1 (1 case); **PIPA Orders:** 8 (10 cases)

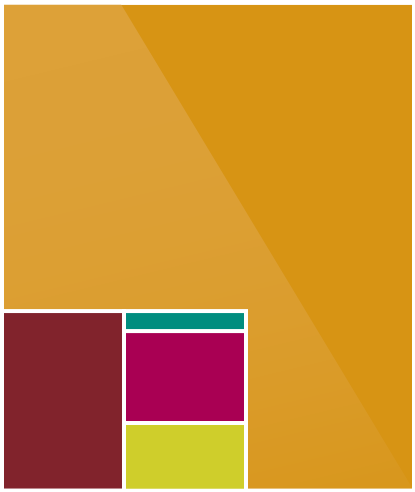
NOTES:

(1) This table includes only the Orders and Decisions issued that concluded/closed the file. See Appendix C for a list of all Orders, Decisions and public Investigation Reports issued in 2018-19. Copies of Orders, Decisions and public Investigation Reports are available at www.oipc.ab.ca

(2) Orders and Decisions are recorded by the date the Order or Decision was signed, rather than the date the Order or Decision was publicly released.

(3) An Inquiry can be discontinued due to a lack of contact with or participation of the applicant or complainant or the issues have become moot.

GRAPH C:
PERCENTAGE OF CASES CLOSED BY RESOLUTION METHOD



- 79% Mediation/ Investigation
- 13% Order/Decision issued
- 4% Commissioner's decision to refuse to conduct an Inquiry
- 3% Withdrawn during Inquiry process
- 1% Discontinued during Inquiry process

Of the **708** cases that could proceed to Inquiry:
7% were resolved within 90 days
19% were resolved within 91-180 days
74% were resolved in more than 180 days

TABLE 4: GENERAL ENQUIRIES

TELEPHONE CALLS		
FOIP	Number	Percentage
Public Bodies	93	21%
Individuals	358	79%
Total	451	100%

HIA	Number	Percentage
Custodians	389	37%
Individuals	661	63%
Total	1,050	100%

PIPA	Number	Percentage
Organizations	213	26%
Individuals	601	74%
Total	814	100%

NON-JURISDICTIONAL	96
EMAILS FOIP/HIA/PIPA	201
Overall Total	2,612

REGULATION & ENFORCEMENT

Privacy Breaches

MANDATORY BREACH REPORTING COMES TO ALBERTA'S HEALTH SECTOR

Alberta's mandatory breach reporting and notification provisions came into force on August 31, 2018, more than four years after the Government of Alberta passed amendments.

The amendments (in May 2014) were a response to a major breach of health information. In January 2014, Medicentres Canada Inc. publicly announced a breach involving the theft of an unencrypted laptop containing billing information for 631,000 Albertans. This incident drew attention to the importance of privacy breach reporting and notification requirements under HIA.

In February 2014, the Commissioner wrote to the former Minister of Health to request that the Government of Alberta consider amending HIA to include mandatory breach reporting and notification provisions, and identified several issues to consider. The Commissioner's letter noted that, at the time in Canada, six of nine jurisdictions with health privacy legislation had mandatory breach reporting or notification provisions in force or had passed amendments.

In response to the Medicentres incident, the Commissioner opened an investigation into privacy breach reporting in Alberta's health sector. After the May 2014 amendments were passed, that investigation's focus shifted to mandatory breach reporting preparedness in Alberta's health sector.

Released in December 2015, the investigation into privacy breach reporting in Alberta's health sector found that breach response practices "vary widely and the health sector is not uniformly prepared," said the Commissioner in the report.[17] The Commissioner added in a news release that, "Although larger health custodians have breach management and response frameworks in place, many regulated health professionals may not be able to meet their legislated obligations when the HIA amendments come into force."[18]

These messages on breach reporting preparedness were reiterated in May 2018 when the Commissioner issued a news release to publicly announce that mandatory privacy breach reporting was coming to Alberta's health sector on August 31, 2018. A government order in council approved on May 8, 2018 set the date for the requirements to be in force.

The amendments require that health custodians:

- Notify an individual affected by a privacy breach if there is a risk of harm to the individual.
- Notify the Information and Privacy Commissioner of a privacy breach when there is a risk of harm to an individual.
- Notify the Minister of Health of a privacy breach when there is a risk of harm to an individual.

There are also new offence and penalty provisions if a health custodian:

- Fails to report a breach.
- Does not take reasonable steps to maintain safeguards to protect health information, which includes administrative, technical and physical safeguards.

[17] The OIPC's Investigation Report H2015-IR-01 is available at www.oipc.ab.ca/media/621630/H2015-IR-01.pdf.

[18] The OIPC's news release is available at www.oipc.ab.ca/news-and-events/news-releases/2015/is-albertas-health-sector-prepared-for-mandatory-breach-reporting.aspx.

A person who is found guilty of one of these offences is liable to a fine.

Prior to August 31, 2018, the OIPC undertook several efforts to prepare for mandatory breach reporting. These efforts included:

- Updating the "Privacy Breach Report Form" to encompass all three of Alberta's privacy laws.
- Creating the "Reporting a Breach to the Commissioner" practice note to assist custodians and organizations in completing the form and meeting the mandatory breach reporting requirements under the *Health Information Regulation* and the *Personal Information Protection Act Regulation* when reporting a breach to the Commissioner.
- Updating other breach reporting resources, including the "How to Report a Privacy Breach" webpage, "Key Steps in Responding to a Privacy Breach" guidance and several PIPA breach reporting resources.
- Sending letters from the Commissioner to the heads of regulated health custodian colleges and associations outlining new requirements and resources.
- Writing articles for regulated health custodian colleges and associations to include in their newsletters.

HIA

After the mandatory breach reporting provisions came into force, the OIPC immediately recognized the impact the amendments would have on operations. Within two months, the OIPC received more breach reports than it had averaged in entire years with voluntary HIA breach reporting.

From 2015-16 to 2017-18, more than 390 breaches – approximately 130 per year on average – involving health information were voluntarily reported by health custodians to the OIPC.

A total of 674 breaches were reported under HIA in 2018-19, representing a 407% increase over 2017-18 (133).

The majority of breaches were caused by human error. Typical human error breaches include transmission errors – by mail, fax or email. However, there are two specific breach types that can have significant health and safety consequences.

Approximately 20% of all breaches reported since August 31, 2018 resulted from a patient receiving the wrong medication from their pharmacist. That is, a patient goes to pick up their prescription but is given another patient's prescription by mistake. Another regular occurrence is when a patient receives the wrong requisition to take to their local lab, which could potentially result in the wrong tests being administered.

By seeing certain types of trends in the types of breaches received, the OIPC takes steps to reduce the number of occurrences. For example, the OIPC has been in contact with the Alberta College of Pharmacy to try to reduce the number of prescription mix ups described above.

There were also more reports of "snooping" – unauthorized access to health information by authorized users. These reports can lead to offence investigations under HIA. It is an offence under HIA for a person to knowingly gain or attempt to gain access to health information in contravention of HIA (section 107(2)(b)).

The OIPC also saw an influx of electronic system compromises under HIA as a result of mandatory breach reporting. These types of breaches do not occur in similar proportions as they do in the private sector, but it is a type of breach that health custodians must be diligent in protecting against.

PIPA

The number of breaches reported by private sector organizations continues to increase. There were 290 breaches reported in 2018-19, an increase of 26% over 2017-18 (231).

The Commissioner made 220 breach decisions in 2018-19. The following determinations were made:

- 168 were found to have a real risk of significant harm
- 35 were found to have no real risk of significant harm
- 17 where PIPA did not apply (i.e. no jurisdiction)

It is mandatory for an organization with personal information under its control, to notify the Commissioner, without unreasonable delay, of a privacy breach where "a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure" (section 34.1).

Each year, breaches with similar causes are reported to the OIPC.

There were more than 50 incidents involving human error, such as transmission errors by email, mail or fax, or during IT system upgrades or settings changes. More than 20 instances of theft were reported, and approximately seven breaches were caused by rogue employees – authorized users who collected, used or disclosed personal information without authorization.

Below are descriptions of common types of breaches that resulted in real risk of significant harm decisions by the Commissioner, primarily electronic system compromises.

Email Phishing

Phishing is a type of social engineering attack carried out via electronic communications, typically email, but also instant messaging, text messaging and phone calls. A couple examples in the social engineering section below are of phishing phone calls. This section focuses on the use of email phishing to gain access to email accounts or IT infrastructure.

In the majority of breach decisions involving email phishing, the perpetrator used a successful phishing email to gain access to employee email accounts, or may have otherwise gained access to an employee's email account. In some of these incidents, a mail forwarding rule was established so that all emails being received by the employee would automatically be forwarded to the unauthorized individual(s). In other situations, the perpetrator would send further phishing emails that appeared to be coming from the employee. There were also several instances in which it appears the perpetrator simply accessed the personal information at issue within the employee's email account, but did not take further action.

Brute force attacks with the aim to exploit technical vulnerabilities in organizations' IT infrastructure is one way malicious actors install malware. A second and increasingly common way is to target employees through the use of phishing to gain or attempt to gain access to employee email accounts or to IT infrastructure. There were five breach decisions that involved an employee clicking on a malicious link or providing employee credentials to give unauthorized individuals access to information systems. After each successful attack, the perpetrator installed malware to capture personal information.

Finally, in one breach decision, the email account of an organization's CFO was accessed and the perpetrator used this access to attempt to request the immediate transfer of a sum of money, which was halted by the CEO who recognized the suspicious activity.

RiverMend Health, LLC, P2019-ND-034
Gerald J. Kugelmass Professional Corporation, P2019-ND-033
Columbia Bank, P2019-ND-031
CPT Group, Inc., P2019-ND-020
Institute for Supply Management, P2019-ND-012

Identifix, Inc., P2019-ND-008
Cassels Brock & Blackwell LLP, P2018-ND-162
Morneau Shepell Ltd., P2018-ND-156
Civeo (Civeo Services Employees LP), P2018-ND-140
Apple Canada Inc., P2018-ND-134
Ebbs, Roberts, Head & Daw Inc., P2018-ND-132
Northbridge General Insurance Corporation and Federated Insurance Company of Canada, P2018-ND-127
Feld Entertainment, Inc., P2018-ND-120
Fountain Tire Ltd., P2018-ND-106
Moore Stephens Tiller, LLC, P2018-ND-102
DIRTT Environmental Solutions Ltd., P2018-ND-095
JYSK Canada, P2018-ND-093
West Coast Reduction Ltd., P2018-ND-091
Northbridge General Insurance Corporation, P2018-ND-090
La Coop fédérée, P2018-ND-083
Luxury Retreats, P2018-ND-076
Newcom Business Media Inc., P2018-ND-073
Investia Financial Services Inc., P2018-ND-070
The Driving Force Inc., TDF Group Inc., Driving Force Investments Inc., 4505 Nunavut limited, Klondike Motors Inc., DF Western Inc., and The Driving Force Ltd, P2018-ND-058
Financial Literacy Counsel Inc., P2018-ND-051

Social Engineering

A number of breach decisions showed the lengths to which some perpetrators will go to dupe victims into providing personal information to cause harm, most often for financial gain. Often the perpetrators will have some personal information of clients or employees. This information is "weaponized" to gather more personal information in attempts to cause harm.

Three incidents reinforced the need for organizations to have effective authentication practices when verifying a client is who they say they are. Fraudsters posed as clients of the organizations in attempts to convince call centre employees to give them access to the clients' accounts. Organizations said that the authentication practices engaged by call centre employees were not adequate or were contrary to policy.

In another incident, a representative of the organization fell victim to a scam in which she called "Microsoft" after a pop-up notification on her computer screen indicated she had a virus. The individual provided her credit card information and allowed remote access to her computer to the unauthorized individual.

A similar incident occurred when customers of the organization received phone calls from one or more individuals falsely claiming to represent one of the organization's computer support service providers. The perpetrator(s) appeared to have some personal information about customers. They used that information to try to gain remote access to the customers' computers, online bank accounts, or to have the customers send money directly.

An unauthorized individual called customers of the organization relating to purchases they had made in attempts to obtain credit card information. The organization did not know how the unauthorized individual obtained the information of customers in order to make phone calls based on actual purchases and delivery orders.

Another incident involved the theft of mail, including an individual's new credit card. That personal information was then used to perpetrate a scam in which the burglar or an associate of the burglar posed as a member of a police service to gather more information about the individual to activate and use the credit card.

Another social engineering case affected thousands of individuals when the organization determined that unauthorized individual(s) were able to successfully answer questions about the affected individuals in order to reset their PINs. The perpetrators appeared to have carried out the attack in order to gain access to personal information related to employment and tax forms.

TALX Corporation and Allegis Group Inc., P2019-ND-030
Sun Life Assurance Company of Canada, P2018-ND-164
McAfee Ireland Ltd., P2018-ND-124

Envision Property Management Ltd., P2018-ND-118
Beaumont Credit Union Ltd., P2018-ND-100
IKEA Canada Limited Partnership, P2018-ND-089
Servus Credit Union Ltd., P2018-ND-069
Primerica Financial Services (Canada) Ltd., P2018-ND-060

E-Commerce and Electronic System Compromises

Given the ubiquity of online shopping and e-services in today's economy, e-commerce websites are often targeted by malicious actors. These incidents are not limited to specific industries or types of organizations.

The purpose of these attacks is for malicious actors to gain access to e-commerce website infrastructure. Once access is gained through exploited vulnerabilities, the unauthorized individual(s) will install or insert malware or a malicious code designed to skim or capture payment card information of customers on the e-commerce website.

In 2018-19, there were more than 20 breach decisions involving a real risk of significant harm where information entered on e-commerce websites was targeted.

Many organizations contract third party service providers to host and maintain the infrastructure for e-commerce websites. If a hacker or unauthorized individual gains access to the service provider's infrastructure it can affect dozens of organizations and thousands of individuals simultaneously.

Under PIPA, the organization having control of the personal information has the legal obligation to notify the Commissioner of a reportable breach (section 34.1). As a general rule, information is under the control of an organization when the organization has the authority to manage the information, including restricting, regulating and administering its use, retention and disposition, and demanding the return of the information.

Typically, when an organization contracts a third party service provider to host and maintain its e-commerce website, the organization maintains control of the information even though the information is under the custody of the service provider (e.g. personal information is stored on the service provider's servers). As a result, it is the responsibility of the organization, not the service provider, to report the breach.

There are situations in which e-commerce website infrastructure is administered by the organization itself. These incidents also occur regularly.

Newegg Inc., P2019-ND-039
Hairbow Center, LLC, P2019-ND-002
Plant Therapy, Inc., P2018-ND-145
LÍLLÉbaby, P2018-ND-131
Bombas, LLC, P2018-ND-125
Alpha Industries, Inc. P2018-ND-122
Rail Europe SAS (France), P2018-ND-117
Rail Europe North America Inc., P2018-ND-116
Plow and Hearth, LLC, P2018-ND-113
LA Fashion Enterprise Ltd., P2018-ND-099
Helly Hansen AS, P2018-ND-096
Tommie Copper Inc., P2018-ND-094
Write-On Stationery Supplies Inc., P2018-ND-085
Roberts Hawaii, Inc., P2018-ND-082
R.C. Purdy Chocolates Ltd., P2018-ND-081
Affy Tapple, LLC operating as Mrs. Prindables, P2018-ND-080
Interstate Plastics, Inc., P2018-ND-066
Carbon Environmental Boutique Ltd., P2018-ND-065
Tommie Copper Inc., P2018-ND-064
PLAE Inc., P2018-ND-063
Gentle Giant Studios, Inc. d/b/a Gentle Giant Ltd., P2018-ND-062
Bronson Nutritionals LLC, P2018-ND-046
Manduka, LLC, P2018-ND-044

Ransom Demands and Ransomware

There were five real risk of significant harm breach decisions that involved ransomware or ransom demands. In at least two incidents, the organization paid the ransom.

Ransomware occurs when servers are hacked and encrypted by the attackers. The attackers then demand payment to unencrypt the data, including the personal information at issue.

Ransom demands are slightly different in that the personal information at issue is accessed and stolen then an extortion attempt is made.

These types of incidents reinforce the importance of backing up information and system files regularly, and to test backups to ensure they are working as expected. If data and system files are backed up the ransom may not need to be paid.

In some cases where a ransom has been paid, the Commissioner has determined there continues to be a real risk of a possible harm. Despite assurances from a hacker that information will be deleted and/or not further disclosed, the Commissioner said in one decision, "[T]he fact remains that these assurances were given by individual(s) who deliberately accessed the information without authority, made ransom demands, and accepted payment of a ransom. These factors weigh heavily against accepting or trusting their assurances" (Tyrell Inc. o/a Zentrum, P2018-ND-141).

Blue Heron Vocational Training Centre, Athabasca, P2019-ND-029
Careem Inc., P2019-ND-018
Tyrell Inc. o/a Zentrum, P2018-ND-141
Nissan Canada Finance, P2018-ND-114
Westcorp Inc., P2018-ND-112

FOIP

The FOIP Act is now the only privacy law in Alberta without mandatory breach reporting and notification provisions. Despite this, the OIPC received 106 voluntary breach reports from public bodies in 2018-19, representing a 112% increase over 2017-18 (50).

More than half of the breaches reported were caused by human error, often misdirected emails. These are regularly caused by the "autocomplete" feature in email programs.

More egregious breaches were also reported. Educational institutions were subject to breaches where students accessed school information systems without authorization. In one such case, the individual altered information within the system

Additionally, there were several instances of external system compromises (e.g. hacking or malware) and inappropriate use of information by an authorized user.

Offence Investigations under HIA

More reports of "snooping" in 2018-19 led to more offence investigations being opened. These offence investigations could lead to more convictions under HIA in the coming years.

In 2018-19, there were two convictions for persons who knowingly accessed health information in contravention of HIA. As of March 31, 2019, there were 10 total convictions based on OIPC offence investigations, all for knowingly accessing health information in contravention of HIA (section 107(2)(b)).

On June 25, 2018, a registered nurse pleaded guilty to accessing health information in violation of HIA and received a $3,000 fine, plus a victim fine surcharge of 30% of the imposed fine.

Two individuals requested audit logs of accesses to their health information in Alberta Netcare, the provincial electronic health record, in 2016. Upon review of their audit logs, they alleged unauthorized access to their health information by the registered nurse. The nurse worked at a rural healthcare centre where the individuals had not received health services.

The individuals reported the matter to AHS' Access and Privacy Office. In October 2016, AHS reported the breaches to the OIPC. The individuals submitted complaints to the OIPC in December 2016.

The nurse pleaded guilty to accessing the health information of one of the individuals on 35 occasions from October 7, 2015 to July 18, 2016, and eight unauthorized accesses to the health information of the second individual from November 1, 2015 to July 18, 2016. Health information accessed included medical profile, demographic information, consultation details, lab results or analysis including blood work, and diagnostic imaging results such as x-rays and MRIs.

On January 15, 2019, a Calgary Laboratory Services (CLS) lab assistant pleaded guilty to accessing health information in contravention of HIA and received a $3,500 fine.

The lab assistant inappropriately accessed the health records of 11 individuals between July 18, 2016 and September 5, 2017. CLS initially discovered the breach of health information through a routine audit of accesses in an electronic health record system. It reported the breach to the OIPC, and notified affected individuals. Four of the individuals submitted complaints to the OIPC.

As of March 31, 2019, one charge for allegedly knowingly accessing health information in contravention of HIA was before the courts.

Privacy Impact Assessment Reviews

There were 645 privacy impact assessments (PIAs) accepted by the OIPC in 2018-19. Nearly all accepted PIAs, 99% or 637, were from health custodians under HIA.

Custodians under HIA "must prepare a privacy impact assessment that describes how proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy" of individuals and submit the PIAs to the OIPC for review and comment prior to implementation of the new practice or system (section 64).

Under the FOIP Act and PIPA, submitting PIAs to the OIPC is voluntary. The OIPC accepted eight PIAs from public bodies under the FOIP Act. No PIAs were accepted from organizations under PIPA.

When PIAs are submitted to the OIPC, the office reviews the assessment and, once satisfied that a public body, custodian or organization has addressed the relevant privacy considerations, will "accept" the PIA which acknowledges that reasonable efforts to protect privacy have been made. A PIA cannot be used to obtain a waiver of or relaxation from legislated requirements for the collection, use and disclosure of personal information in a new or redesigned project or legislative scheme.

A listing of all PIAs accepted by the OIPC in 2018-19 is available at www.oipc.ab.ca.

HIA

Of the hundreds of PIAs accepted by the OIPC annually, many are similar in nature, such as widely used electronic health record information systems, but a few stand out as unique.

PrescribeIT™ is a messaging exchange service that securely transmits prescription information between prescribers and pharmacies. Canada Health Infoway in partnership with Health Canada, the provinces and territories, and industry stakeholders created, operates and maintains PrescribeIT™. It started its national rollout in Alberta. The OIPC accepted a PIA on this project for its limited production release. The PIA was submitted by participating custodians. The purpose of the project is to connect community-based prescribers to community pharmacies to electronically transmit prescriptions to a patient's pharmacy of choice.

Alberta Health's final PIA prior to launching its MyHealth Records personal health portal was accepted in 2018-19, which was the sixth addendum to a years-long process for this project.[19] The addendum related to a change in service providers from Microsoft HealthVault to TELUS Health Space. The personal health portal is a collaborative project between Alberta Health and Alberta Health Services (AHS). The initial PIA was jointly submitted in 2015.

DynaLife Labs had its Incident Reporting and Management System PIA accepted in 2018-19. The system was built to report quality, workplace safety, or facility and equipment incidents to respective business units within DynaLife. Specifically, the incident management system is meant to provide a mechanism

[19] Alberta Health announced it was launching the MyHealth Records personal health portal on March 16, 2019. Subsequently, on July 12, 2019, the new government announced it was seeking requests for proposal to review three health information systems, including MyHealth Records, with a final report to be submitted to the Government of Alberta by December 31, 2019.

for the documentation and tracking of privacy and security incidents that have occurred within or have been identified from outside of the organization. It also provides an easy retrieval of information pertaining to a particular event, which may help to identify trends to assist with developing and implementing corrective or preventative actions and process improvements.

Also in 2018-19, the OIPC had representatives on the Security and Privacy Advisory Committee for AHS' Connect Care project. This project is meant to replace more than 1,300 information systems used by AHS into one all-encompassing health information system for Alberta's only regional health authority. The disparate systems currently in effect often results in Albertans regularly repeating their medical histories with different healthcare providers throughout the province. Considering the scope of the project, the PIA review, once undertaken by the OIPC, will be among the most complex ever reviewed by the office. The OIPC was anticipating to receive the Connect Care PIA in October 2019.[20]

PIAs Opened Annually Over 10 Years*

2009-10: **714**
2010-11: **530**
2011-12: **457**
2012-13: **420**
2013-14: **384**
2014-15: **356**
2015-16: **452**
2016-17: **611**
2017-18: **792**
2018-19: **1,059**

**Not all opened files are accepted.*

FOIP

Far fewer PIAs are submitted by public bodies voluntarily, relative to the mandatory PIA submission for health custodians under HIA. Nevertheless, certain PIAs are submitted to the OIPC by public bodies for projects or programs that involve the collection, use and disclosure of personal information.

Part of the MyAlberta eServices suite of online government products for residents, the Ministry of Community and Social Services launched its Evacuation Payments Service. A PIA was accepted by the OIPC on this service in 2018-19. The project is meant to eliminate in-person disbursement sites at the time of a disaster, such as when being forced to evacuate residences due to wildfires. Rather, Albertans can electronically apply for emergency evacuation assistance payment and receive the disbursement of financial assistance via Interac eTransfer. For those individuals that may not have the ability to receive Interac eTransfers, registering on the MyAlberta Evacuation Payment System will increase the processing efficiency and quicken the disbursement of emergency evacuation payments. Similar to other MyAlberta eServices, individuals eligible for evacuation payments must sign up for a MyAlberta Digital ID and verify their identity to receive payment.

The OIPC also accepted a PIA from the City of Airdrie in 2018-19 on its In-Car Digital Video (ICDV) Initiative. The initiative is for all municipal enforcement vehicles to be equipped with ICDV to support the city's municipal enforcement officers in the execution of their duties, as well as for employee performance management (upon complaint only) and training purposes. ICDVs are intended to capture specific incidents, not for 24-hour recording. The program is not meant to displace other responsibilities of enforcement officers; recordings are to support an officer's observations, rather than supplementing or replacing detailed notes.

[20] On July 12, 2019, the new government announced it was seeking requests for proposal to review three health information systems, including Connect Care, with a final report to be submitted to the Government of Alberta by December 31, 2019.

Investigation Reports

Managing and Storing Emails within the Government of Alberta

On March 12, 2019, the OIPC released an investigation report under the FOIP Act that looked into the management and storage of email at four Government of Alberta (GoA) departments – Service Alberta, Alberta Transportation, Alberta Education and Executive Council.

In December 2015, the Official Opposition requested the number of emails stored within inboxes of senior government and political staff under the FOIP Act. Similar requests for the number of emails in inboxes and the number of emails in sent, deleted and draft folders were made in February 2016 and the spring of 2016.

On September 28, 2017, the Official Opposition wrote a letter to the Commissioner and issued a news release outlining concerns and allegations about the GoA's use of email. On October 27, 2017, the Commissioner opened this investigation. In December 2017, the Commissioner retained the services of MT>3, a division of McCarthy Tétrault LLP, to investigate this matter.

The investigation found Service Alberta's guidelines, standards and procedures for information and email management detailed and emphasized the need to identify and segregate official records from transitory records. However, there was no consistent storage location for official records in GoA departments, training was not compulsory in all departments, and a compliance assessment program had not been established to ensure that staff members received training and were following the records management plan for their department. Service Alberta indicated it was in the process of developing an information management reporting and compliance program, but details were not available.

The investigation also found that the number of emails in a staff member's inbox had no bearing on whether official records were properly identified and retained. The investigation concluded that a majority of email mailboxes retained more records than required. Most staff seemingly erred on the side of caution and kept emails rather than disposing of emails, and managed these emails by creating subfolders for transferring the emails from inboxes.

Two interviewees said they actively deleted most emails. These senior staff members said they did not consider sending and receiving requests for information to be official records. The investigation noted that requests and replies for information would likely support business decisions and should be official records.

Based on the conclusions, the investigation made three recommendations that centred on what Service Alberta's compliance program should include and that Service Alberta should plan a government-wide official records electronic storage repository.

Investigation Report F2019-IR-01: Investigation into the management and storage of email by the Government of Alberta (Service Alberta, Alberta Transportation, Alberta Education and Executive Council)

> "Overall, this investigation reinforces the fundamental importance of a comprehensive, effective records management program to ensure that public bodies are able to fulfil their access and privacy obligations under the FOIP Act, and for meeting other business and legal responsibilities."
>
> *- Commissioner Jill Clayton, March 12, 2019*[21]

[21] The OIPC's news release is available at www.oipc.ab.ca/news-and-events/news-releases/2019/oipc-releases-investigation-into-management-of-goa-emails.aspx.

Searches in the Government of Alberta's Action Request Tracking System When Responding to Access Requests

On June 19, 2018, the OIPC issued an investigation report into searches made by the GoA in its Action Request Tracking System (ARTS) when responding to access requests. It found that GoA staff responsible for responding to access requests were well aware that records in a database are subject to the FOIP Act, but there were some differences in how GoA departments searched for records.

After the release of Investigation Report F2016-IR-01 into alleged improper destruction of records following the May 2015 provincial election, the Commissioner received a letter. The letter outlined an individual's concerns that the misunderstanding of the application of the FOIP Act to the information held in ARTS, as referenced in the report, may have affected responses to previous access requests made under the FOIP Act. Based on the concerns in the letter, the Commissioner opened the investigation into ARTS.

Overall, this investigation found that GoA departments, in responding to access requests where relevant records may be available in ARTS, made every reasonable effort to assist applicants and to respond to each applicant openly, accurately and completely. This was a general finding and did not implicate past, current or future OIPC reviews of GoA department responses to access requests.

The ARTS investigation resulted in the following four recommendations to the GoA:

- Establish and implement call for records practices that are less dependent on the knowledge or experience of individual FOIP Coordinators.
- Provide regular, ongoing FOIP Act training for all GoA staff, with more in-depth supplemental training for staff who are involved intimately in searching for responsive records.
- Develop a GoA-wide dedicated form for all departments to create and maintain a record of searches in order to consistently and systematically require department employees to document steps taken to identify and locate records that may be responsive to an access request.
- Remind staff, through the call for records, that records may exist in many different forms, including electronic information systems, and that a comprehensive search for responsive records must include a search of such systems.

Investigation Report F2018-IR-01: Investigation into searches of the Government of Alberta's Action Request Tracking System in response to access requests (19 GoA departments)

Guidelines for Managing Emails and Tip Sheet

Concurrent with the issuance of the investigation report on managing and storing emails, the OIPC published "Guidelines for Managing Emails". This high-level guidance document is meant to assist public bodies, health custodians and private sector organizations and their staff in understanding that emails are records and should be managed in accordance with records management principles and the requirements of Alberta's access to information and privacy legislation. The OIPC also published a one-page "8 Tips for Managing Emails" document based on the guidelines.

Balancing Pool's Management of Transitory Records

On June 19, 2018, the OIPC issued an investigation report concerning the Balancing Pool's management of transitory records.

The Commissioner opened this investigation to address whether the Balancing Pool destroyed records that were responsive to an access request, and whether the Balancing Pool complied with rules relating to the destruction of records as set out in any enactment of Alberta. This was in response to two letters the Commissioner received from individuals concerned about how the Balancing Pool processed their access requests.

The two applicants made similar access to information requests under the FOIP Act to the Balancing Pool on April 4, 2016 and August 23, 2016 related to power purchase agreements. The Balancing Pool responded to both requests on November 4, 2016 and February 9, 2017, respectively.

In their letters to the Commissioner, the first applicant had general concerns about records management and retention, and about an instruction in an email to delete a draft briefing note; the second applicant was also concerned about the instruction to delete the draft briefing note. The draft briefing note was attached to an email that read, "Sensitive and transitory. Please delete." An Alberta Energy employee sent the email to Balancing Pool employees.

The Balancing Pool investigation found that it had responded properly to the two access requests, despite the applicants' concerns. The Balancing Pool did not delete the email or the draft briefing note, and provided access to both when responding to the applicants' requests. However, the email and draft briefing note were not provided alongside each other (i.e. email with attachment) in the first applicant's response package.

The investigation also found that the Balancing Pool was not fully aware of its records management policies and procedures. Additionally, Balancing Pool employees had no training to understand the difference between official and transitory records.

The investigation made three recommendations to the Balancing Pool. The first recommendation related to the organization of access request response packages. The second recommendation was to create a records management program. The third recommendation was to ensure officials and employees receive training on applicable records management policies.

Finally, the investigation found that certain GoA public bodies are designated under Schedule 1 of the *Freedom of Information and Protection of Privacy Regulation*, with the result that those public bodies are subject to the GoA's *Records Management Regulation*. Others, including the Balancing Pool, are designated as public bodies under the *Freedom of Information and Protection of Privacy (Ministerial) Regulation*, with the result that they are not subject to the GoA's *Records Management Regulation*. The investigation recommended that the Commissioner write to the Minister of Service Alberta highlighting this inconsistency.

Investigation Report F2018-02: Investigation into the Balancing Pool's management of transitory records (Balancing Pool)

Alleged Unauthorized Accesses of Health Information at Alberta Hospital Edmonton

On October 17, 2018, the OIPC released an investigation report into thousands of alleged unauthorized accesses of health information at Alberta Hospital Edmonton by an affiliate of the custodian (employee). The custodian was Alberta Health Services (AHS).

AHS provided its first detailed report of the breach to the OIPC on December 3, 2015, and sent an updated report on March 16, 2016. During this time, and following the reports, AHS notified individuals affected by the breach. The OIPC received 30 complaints from individuals affected by the breach.

On September 26, 2016, AHS issued a news release to inform the public about a former employee who had improperly accessed the health information of more than 1,309 individuals from 2004 to 2015 in Alberta Netcare, the provincial electronic health record. An additional 11,539 individuals had their demographic information viewed by the former employee in Netcare Person Directory, a subsystem of the provincial electronic health record.

The investigation confirmed that the employee used individually identifying health information in contravention of the rules set out in sections 27 and 28 of HIA. Since AHS is responsible as a custodian for the actions of its affiliates under section 62(2) of HIA, AHS also contravened section 27 of HIA when its affiliate accessed and used health information for unauthorized purposes.

The investigation determined that AHS established reasonable policies and procedures to facilitate the implementation of the Act and the regulations, as required by section 63(1) of HIA. However, it failed to ensure the employee was aware of the safeguards put in place to protect health information, in contravention of the *Health Information Regulation* (section 8(6)).

The three recommendations that resulted from the investigation's findings related to privacy training, monitoring compliance with rules and procedures concerning access to and use of health information in Netcare (and other electronic health information systems), and AHS' approach to reviewing audit logs to detect and prevent unauthorized use of Netcare.

Investigation Report H2018-IR-01: Investigation into multiple alleged unauthorized accesses of health information at Alberta Hospital Edmonton (Alberta Health Services)

> "This report should be a wake-up call for anyone responsible for protecting Albertans' health information, alerting them to the potential consequences if they fail in their duty to implement and maintain reasonable safeguards to protect health information."
>
> *- Commissioner Jill Clayton, October 17, 2018*[22]

[22] The OIPC's news release is available at www.oipc.ab.ca/news-and-events/news-releases/2018/ahs-failed-to-properly-protect-health-information.aspx.

Alleged Unauthorized Disclosure of Personal Information by the City of Calgary

On September 21, 2018, an investigation report was released that looked into a privacy breach that the City of Calgary voluntarily reported to the OIPC in June 2016. The City of Calgary reported that a breach occurred when an employee, who was "seeking technical assistance from a close contact" on two different job assignments, disclosed spreadsheets containing personal information without authorization.

Upon being notified about the breach by the City of Calgary, seven individuals affected by the breach submitted privacy complaints to the OIPC. The Commissioner opened an investigation to look at whether the City of Calgary contravened the FOIP Act when the employee disclosed personal information, whether reasonable safeguards to protect personal information were in place and, based on the concerns of complainants, reviewed whether the City of Calgary followed the key steps in responding to a privacy breach.

The investigation found, and the City of Calgary acknowledged, that sending the emails and attachments to the "close contact" constituted an unauthorized disclosure under the FOIP Act.

The investigation also found that reasonable safeguards to protect personal information were generally in place. However, a formally established breach response protocol was not in place at the time of the incident.

The investigation determined that the City of Calgary followed the key steps in responding to a breach.[23]

The investigation's one recommendation was for the City of Calgary to complete its work to develop and communicate a breach response protocol to all staff.

Investigation Report F2018-IR-03: Investigation into an unauthorized disclosure of personal information by the City of Calgary (City of Calgary).

[23] The OIPC's "Key Steps in Responding to Privacy Breaches" guidance document is available at www.oipc.ab.ca/media/950540/guide_key_steps_breach_response_aug2018.pdf.

Mediation and Investigation

Hundreds of files are opened and resolved annually at mediation and investigation. These files include requests for review, requests for review third party, requests to excuse fees and privacy complaints.

In total, 79%, or 559, of the 708 cases that could proceed to inquiry were resolved by mediation and investigation in 2018-19. This compares to 79%, or 622, of 787 cases in 2017-18.

While fewer total cases went through the mediation and investigation process in 2018-19, complexity continues to increase in large part thanks to new technologies and the limitless nature of digital information in all sectors.

VIDEO SURVEILLANCE

With the availability of inexpensive video recording equipment more public bodies and private sector organizations are deploying this technology. The increased use combined with enhanced awareness of access and privacy rights has led to video surveillance being the subject of several requests for review and privacy complaints before the OIPC over the past few years.

The OIPC has received complaints that workplaces installed cameras with video and audio capability for security reasons, but then allegedly used the devices for employee surveillance. Another complaint related to a live video feed that connected a work space in one city to another worksite in a different city. Another complaint dealt with hidden video cameras at a rental property.

There have also been a significant number of requests for review from individuals incarcerated in correctional facilities who have sought access to video surveillance records.

Video surveillance involves several access and privacy challenges, including:

- Records retention: Video recordings are often overwritten after a certain period of time. This poses a challenge for requesting access to records prior to the records being destroyed.
- Severing third party information: Images of other individuals may be captured in video recordings, which may have to be redacted prior to providing access to the records. These can be time consuming and potentially expensive processes.
- Law enforcement purposes: Analysis of security and law enforcement purposes can be challenging depending on the nature of the video surveillance records subject to an access request or privacy complaint.

As video surveillance becomes cheaper, more readily available and easily paired with other technologies, the access and privacy implications will continue.

The OIPC has "Guidelines for Overt Video Surveillance in the Private Sector" that offer the principles to consider when embarking on a video surveillance project.

A privacy impact assessment (PIA) is also strongly encouraged if considering implementing video surveillance. PIAs offer a good starting point for evaluating the impact of this type of technology. A PIA will help organizations in all sectors turn their minds to the access and privacy implications of video surveillance, and will help them to explain their legal authority or purposes to stakeholders.

WORKPLACE INVESTIGATIONS

A number of requests for review stemmed from access requests for records related to workplace investigations. These access requests are often challenging for public bodies or private sector organizations to process as they regularly involve witness statements and other sensitive records. As a result, applicants commonly submit a request for review because third party personal information was withheld or because records subject to claims of solicitor-client privilege were withheld.

The FOIP Act and PIPA have sections that may except information from disclosure on the basis of an unreasonable invasion of a third party's privacy (section 17 of the FOIP Act), disclosure harmful to law enforcement (section 18 of the FOIP Act) or information was collected for an investigation or legal proceeding (section 24(2)(2) of PIPA). Solicitor-client privilege is also regularly claimed in responses to access requests for records relating to a workplace investigation.

It is notable that at least one other province has implemented a legislative solution to these types of access requests. Section 33 of Newfoundland and Labrador's *Access to Information and Protection of Privacy Act* excludes records gathered or created for a workplace or harassment investigation from an applicant unless the applicant is a party to the investigation, in which case it mandates disclosure to the party. However, if a party is a witness, only information pertaining to the witness themselves is to be disclosed.

HIA COMPLAINTS

In past years, the majority of complaints under HIA dealt with concerns about whether access to health information in Netcare, the provincial electronic health record, was authorized under the Act. However, due to mandatory breach reporting under HIA, several complaints were received in the past year after an individual was notified by a health custodian that their health information had been subject to a privacy breach.

Under the *Health Information Regulation,* a notice of a breach to an individual by a custodian must include a statement that the individual can ask the Commissioner to investigate the loss or unauthorized access or disclosure and contact information to file a complaint to the Commissioner's office must also be provided.

In these investigations, the OIPC typically investigates the circumstances surrounding the incident that gave rise to the notice. The investigation primarily addresses whether or not the custodian took reasonable steps to protect health information (section 60) that resulted in a reportable incident under section 60.1.

It will be interesting to follow whether there are marked increases in complaints from breach notices in the years to come.

Requests for Time Extensions by Public Bodies

There were 226 requests for time extensions received in 2018-19 under the FOIP Act, representing almost no change from 2016-17 (228).

Of the 226 time extension requests received in 2018-19:

- 61% were made by provincial government departments
- 23% were made by municipalities
- 5% were made by law enforcement
- 5% were made by post-secondary institutions
- 6% were made by other public bodies

Resolutions on the 226 time extensions requests were as follows:

- 60% were granted
- 21% were partially granted (extension period permitted was less than what was requested by the public body)
- 15% were denied
- 4% were withdrawn by the public body

A public body must make every reasonable effort to respond to a request for access under the FOIP Act within 30 calendar days (section 11). A public body may extend the time limit for responding by up to 30 days on its own authority in certain circumstances (section 14(1)). An extension period longer than an additional 30 days requires the Commissioner's approval. A failure by a public body to respond to a request within the 30-day time limit, or a time limit extended under section 14, is to be treated as a decision to refuse access under the FOIP Act (section 11(2)).

Deemed Refusals to Respond to Access Requests

There were 30 deemed refusal orders issued in 2018-19, all of which related to public bodies under the FOIP Act. In seven orders, the public body responded to the applicant during the inquiry.

Deemed refusal orders are issued when the public body has not responded to an access request within the time limit under the FOIP Act and an applicant requests a review. Typically, the Adjudicator orders the public body to respond to the applicant and meet its remaining duties under the Act in responding to the applicant, unless the public body responds during the inquiry.

Of the 30 deemed refusal orders issued in 2018-19, 17 related to government departments, five to municipalities, four to a police service, three to a regional health authority and one to a post-secondary institution.

In 2015-16, the OIPC began streamlining requests for review to the inquiry process when an applicant has not received a response to an access request that they have submitted to a public body, health custodian or organization within the time limits set out in the FOIP Act, HIA or PIPA, respectively. The Commissioner established this process after seeing an increase in requests for review where the only issue was that an applicant had not received a response to their access request within the time limits set out in the Acts.

Alberta Justice and Solicitor General, Order F2019-11
Edmonton Police Service, Order F2019-08
Edmonton Police Service, Order F2019-04
Alberta Agriculture and Forestry, Order F2019-03
City of Calgary, Order F2019-01
Alberta Health, Order F2018-80
Edmonton Police Service, Order F2018-73
Alberta Health Services, Order F2018-69
Town of Peace River, Order F2018-68
Town of Peace River, Order F2018-67
Town of Peace River, Order F2018-66
Alberta Justice and Solicitor General, Order F2018-65
Alberta Status of Women, Order F2018-64
Alberta Community and Social Services, Order F2018-63
Alberta Justice and Solicitor General, Order F2018-62
Alberta Energy, Order F2018-61
City of Calgary, Order F2018-58
Alberta Community and Social Services, Order F2018-57
Alberta Children's Services, Order F2018-56
Alberta Health, Order F2018-44
Service Alberta, Order F2018-42
Alberta Health, Order F2018-41
Alberta Health Services, Order F2018-40
Service Alberta, Order F2018-34
Alberta Seniors and Housing, Order F2018-30
Alberta Health Services, Order F2018-29
University of Alberta, Order F2018-28
Edmonton Police Service, Order F2018-23
Alberta Justice and Solicitor General, Order F2018-22
Alberta Agriculture and Forestry, Order F2018-19

Summary of Significant OIPC Decisions

Requests for Briefing Binders and Materials

An applicant made several requests to different government departments for copies of the contents of briefing binders that were created for different purposes.

In response to all requests, the government departments relied on section 6(4) of the FOIP Act to withhold certain records from the applicant. Section 6(4) states:

> 6(4) The right of access does not extend
>
> (a) to a record created solely for the purpose of briefing a member of the Executive Council in respect of assuming responsibility for a ministry, or
>
> (b) to a record created solely for the purpose of briefing a member of the Executive Council in preparation for a sitting of the Legislative Assembly.

In five of the eight orders, the applicant requested briefing binders from government departments containing information for the respective Minister in each department to know in preparation for a meeting of the Committee of Supply, and for information that its employees needed in order to brief the Minister in preparation for that meeting (Orders F2018-45, F2018-46, F2018-47, F2018-50 and F2018-51). The government departments withheld some responsive records on the basis that the records were created for the sole purpose of briefing a member of Executive Council in preparation for a sitting of the legislature (section 6(4)(b) of the FOIP Act).

For these five requests, the Adjudicator found that a meeting of the Committee of Supply is a process that is part of a sitting of the Legislative Assembly. The Adjudicator confirmed the departments' decisions to refuse access to the briefing binders created to enable employees of those departments to brief the Minister in preparation for a meeting of the Committee of Supply.

In two of the eight orders, an applicant requested briefing binders for a specified Standing Committee on Public Accounts meeting (Order F2018-48 and F2018-49). The government departments withheld some responsive records on the basis that the records were created for the sole purpose of briefing a member of Executive Council in preparation for a sitting of the legislature (section 6(4)(b) of the FOIP Act).

For these two requests, the Adjudicator found that section 6(4)(b) did not apply, and ordered the government departments to respond to the applicant without reliance on that section. The Adjudicator determined that the Standing Committee on Public Accounts may set its own agenda, and that the agenda is not determined by the Legislative Assembly. Further, preparing for a meeting of the Standing Committee on Public Accounts is not synonymous with preparing for a sitting of the legislature, given that the two need not coincide (i.e. the Standing Committee on Public Accounts may meet outside a sitting of the Legislative Assembly).

In the remaining order, the applicant requested briefing materials for the transition of a Deputy Minister (Order F2018-52). The Adjudicator confirmed Alberta Labour's decision in this case, as it relied on section 6(4)(a) in withholding records from the applicant. The Adjudicator noted that section 6(4)(a) requires that the record be created solely for the purpose of briefing the Minister in respect of assuming responsibility for a ministry, and does not require that a record be given only to the Minister or be intended only for the Minister's eyes.

Alberta Labour, Order F2018-52
Treasury Board and Finance, Order F2018-51
Executive Council, Order F2018-50
Alberta Culture and Tourism, Order F2018-49
Alberta Seniors and Housing, Order F2018-48
Alberta Education, Order F2018-47
Executive Council, Order F2018-46
Alberta Health, Order F2018-45

Twitter Account Names Found Not to be Personal Information

An applicant requested a list of Twitter users or accounts that had been blocked for each Twitter account operated or authorized by Alberta Education. In its response, Alberta Education severed the names of some blocked Twitter accounts citing disclosure harmful to personal privacy (section 17(1) of the FOIP Act).

Alberta Education argued in part that the fact that it blocked a Twitter account is likely to reveal personal information about inappropriate conduct on the part of an identifiable individual. The Adjudicator countered that the name of a Twitter account cannot be said to have a personal dimension necessarily, even though an account may have the appearance of being associated with an identifiable individual.

The Adjudicator stated at para. 25:

> While some names and corresponding pictures could possibly be genuine, others do not appear to be. In addition, some names appear to be the names of organizations and businesses. With regard to the names and photographs that appear to be of individuals, I am unable to find, on the evidence before me, that the accounts with which they are associated are actually being used by these individuals, or that the name of the account and the image associated with it, are about the same individual.

Using several sources, including the Alberta Court of Appeal, the Adjudicator noted that the information severed is "about a Twitter account", rather than "about an identifiable individual".

The Adjudicator provided some guidance at para. 32 to distinguish between types of personal information:

> (Alberta Education) raises the issue of email, and asks for guidance on the differences between email addresses and blocked Twitter accounts. In my view, sections 1(n) and 17 of the FOIP Act apply in the same way to email addresses and Twitter accounts. If there is evidence establishing that an email address or a Twitter account is connected to an identifiable individual, and the email address or Twitter account appears in a context that reveals personal information about the individual, then the information is personal information, and (Alberta Education) must consider the provisions of section 17 in deciding whether to disclose the information to a requestor. However, where the email address or Twitter account lacks a personal dimension, or does not clearly have a personal dimension, and no other information would be revealed about an identifiable individual if the information is disclosed, then section 17 is not applicable to the email address or Twitter account.

The Adjudicator ordered Alberta Education to give the applicant access to the information it severed from the records.

Alberta Education, Order F2019-02

Disclosure of Contract with Government

In Order F2013-47, the applicant requested a copy of the agreement between Alberta Health (AH) and Alberta Blue Cross (ABC) under which ABC administers the provincial drugs plan. AH produced the agreement but severed some information citing disclosure harmful to business interests (section 16) and disclosure harmful to economic and other interests (section 25) in the FOIP Act. The Adjudicator ordered AH to disclose the agreement in its entirety.

ABC applied for judicial review of Order F2013-47. On October 15, 2015, the order was partly upheld and partly quashed and remitted at the Court of Queen's Bench. The Court held that parts of the order by which the previous Adjudicator reasoned that the records did not meet the terms of disclosure harmful to business interests of a third party (section 16(1)(b)) were unreasonable. The Court remitted the matter for reconsideration as to whether the withheld records meet the criteria of sections 16(1)(b) and 16(1)(c) of the FOIP Act.

In this inquiry, heard by a different Adjudicator, AH provided further information about the records, including that some of them were already in the public realm. It also took the position for some of the records that AH rather than ABC had been the source of the information contained in them.

Based predominantly on the information provided by AH, the Adjudicator held that she was unable to find that the records meet the criteria of section 16(1)(b) of the FOIP Act. In relation to the remaining records, the Adjudicator accepted, or in some cases assumed, that the criteria of section 16(1)(b) were met. However, the Adjudicator concluded that neither ABC nor AH established that any of the records meet the harms test set out in section 16(1)(c).

The Adjudicator ordered that all of the records be disclosed to the applicant.[24]

Alberta Health, Order F2019-R-01

Requests for Personal Information in Private Sector Video Surveillance Footage

As highlighted in the Mediation and Investigation section, there has been an increase in the number of requests for review related to access requests for personal information in all recorded formats, including video recordings, under PIPA.

In one matter that made its way to inquiry, the applicant was employed by a tenant in Primaris Management Inc.'s (Primaris) shopping mall. The applicant was involved in an incident with an employee of Primaris while performing his duties for his employer. The incident was captured by Primaris' video surveillance system. The applicant requested a copy of the video.

Primaris initially provided still photographs from the video but refused to provide a copy of the video itself. The Adjudicator determined that the video cannot be withheld by Primaris under the exception that the information was collected for an investigation or legal proceeding (section 24(2)(c) of PIPA). Primaris used the video in the course of an investigation, but the video was not collected for the purpose of that investigation.

The Adjudicator determined that the video contained personal information of third parties, which must be withheld. The Adjudicator accepted Primaris' arguments that in this case it was not reasonable to require Primaris to sever third party information from the video and provide the applicant with access to the remainder (section 24(4) of PIPA). The Adjudicator stated at para. 19:

> In this case, (Primaris) would have to obtain technology it does not currently have in order to remove, pixilate, or otherwise render non-identifiable the personal information of the third parties. This would need to be done frame-by-frame to ensure that the Applicant's movements, which cross the field of the camera's view, remain visible. To require this is not reasonable in this case, given the particular facts discussed above.

In another inquiry, an applicant requested surveillance tapes of an incident involving him and another individual from 7-Eleven Canada, Inc. (7-Eleven). The applicant specified that he was seeking the unaltered video, in order to pursue the other individual in the video.

The Adjudicator determined that the video contained personal information of third parties, which must be withheld. Given that the applicant requested unaltered video, the Adjudicator said at para. 26:

> Under different circumstances, severing third party personal information from a video in order to provide an applicant with their own personal information might not render the remaining information "meaningless." However, given the Applicant's request, I agree with (7-Eleven) that the Applicant is not seeking a severed version of the video. It would be unreasonable in this case to require (7-Eleven) to sever the third party personal information and provide the Applicant with only his own personal information in the video given that the Applicant specifically asked that this not be done.

The Adjudicator agreed with 7-Eleven that it was not reasonable to require it to sever third party personal information from the video recording in these circumstances.

7-Eleven Canada, Inc., Order P2018-08
Primaris Management Inc., Order P2018-04

[24] Order F2019-R-01 was issued on March 31, 2019. ABC applied for judicial review on this order in May 2019.

Request for Health Information by an Executor of an Estate

The applicant requested access to his deceased mother's health information under HIA from Alberta Health Services (AHS) in his capacity as the executor of her estate. The applicant explained that the requested records were "required for the administration of [his mother's] estate" and that he was making the access request as the "personal representative" of his deceased mother.

The issues for inquiry were whether the applicant was authorized by section 104 of HIA to make an access request for his deceased mother's health information, and whether the applicant was entitled to receive the records he had requested in certain items or categories of records of his access request.

The Adjudicator determined that the applicant, as the executor of his mother's will, was authorized to make an access request for the purpose of administering his mother's estate. The Adjudicator found that the access request, which had been made for the purpose of determining whether to bring a legal action, had been made for the purpose of administering his mother's estate. The Adjudicator interpreted section 104 in the following way at paras. 24 and 25:

> I do not interpret section 104 as authorizing a custodian to step into the shoes of an executor so as to assess, on a record-by-record basis, which particular records he or she needs, once an executor has established he or she is an executor and indicated the request relates to the administration of the estate. Section 104 confers the rights or powers of a deceased person on an executor provided the exercise of the right or power relates to the administration of the estate. Once the executor of a will has established that making the access request – the exercise of a right in this case – relates to the administration of the estate, the executor may exercise the right. A custodian may then withhold health information from the executor only if it would be authorized to withhold the information from the testator under section 11 of the HIA.
>
> In addition, where litigation is being contemplated, a custodian's questions as to how requested records relate to the litigation could require the executor to disclose privileged communications and litigation strategies to the custodian, who may be the respondent in the litigation. In my view, while section 104 contains implicit authority for a custodian to ask whether an individual is acting in the capacity of an executor of a will and administering an estate, it does not contain authority to require a requestor to divulge privileged communications in order to obtain individual records that are the subject of the access request.

In conclusion, the Adjudicator found that AHS was not entitled to withhold the requested information on the basis that it considered the records to be unrelated to the administration of the applicant's mother's estate.

AHS was ordered to conduct a search for records responsive to certain categories of records and to respond to that portion of the applicant's access request. It was also ordered to document the search it conducted. It was not precluded from relying on section 11 of HIA to withhold records, if it considered this provision to apply.

Alberta Health Service, Order H2018-01

Producing Records to the Commissioner: Privilege Update

In the 2017-18 Annual Report, the Commissioner's special report to the Legislative Assembly entitled "Producing Records to the Commissioner: Restoring Independent and Effective Oversight under the FOIP Act" was summarized. The report outlined developments compromising the Commissioner's ability to perform certain functions under the FOIP Act, specifically the Commissioner's ability to require public bodies to provide records to the Commissioner over which public bodies are claiming privilege.

In 2016, the Supreme Court of Canada decided that the wording in the FOIP Act was not specific enough to allow the Commissioner to compel records over which solicitor-client privilege was claimed. Further, public bodies were not providing records required for reviews by the Commissioner.

The Commissioner maintained that the legislature established the position of Information and Privacy Commissioner to provide for an accessible, affordable and timely process for reviewing access to information decisions made by public bodies. The alternative, outlined in the report, is to transfer the power of the Commissioner to the Courts and have the Courts decide whether a public body properly applied privilege to records when responding to an access request. For a number of reasons, the Commissioner stated that this would not be feasible, including increasing the cost for the Courts, public bodies, the OIPC and citizens, having multiple decision makers in a single case, and having multiple appeal routes, all of which unduly complicate the process.

This issue and the Commissioner's predictions in the report came to a head in judicial reviews of the Commissioner's decisions about whether records are subject to solicitor-client privilege. The Court decided that it has the authority to review those records on judicial review, even though the records were not before the Adjudicator in the first instance.

In *Calgary (Police Service) v. Alberta (Information and Privacy Commissioner),*[25] the Court of Appeal said:

> [2] The question before us today is limited…it is whether, on a judicial review application under the *Freedom of Information and Protection of Privacy Act,* a Court is entitled to review documents over which claims of solicitor client privilege have been made even though those documents were not reviewed by the Privacy Commissioner and are not "formally" part of the certified record.
>
> [3] We are satisfied that on a judicial review application where the dispute centres on whether the documents in question are subject to solicitor client privilege, those documents should be put before the reviewing Court. It is this simple. The issue – whether solicitor client privilege exists with respect to the disputed documents – cannot be properly determined in these circumstances without examining the documents themselves. This approach is consistent with the supervisory role of the Court.

The OIPC has since worked with public bodies and the Court to develop a process whereby the public bodies are able to put the records before the Court for the Court's review in a judicial review.

[25] *Calgary (Police Service) v Alberta (Information and Privacy Commissioner),* 2017 ABQB 656, 2018 ABCA 114 and 2019 ABQB 109.

What has happened in two cases to date is that, either on the application for judicial review or just before the public bodies must produce the records to the Court for the Court's review, the public bodies have decided that solicitor-client privilege or litigation privilege does not apply to some of the records over which they originally claimed privilege.

In the Calgary Police Service (CPS) case, on the date that CPS brought the judicial review in 2016, it decided to disclose redactions on 27 pages of records to which it had originally claimed that solicitor-client privilege applied (out of a total of 74 pages). The result was that the access requester waited three years from the date of CPS' response to the access request in 2013, for those records to be disclosed to the requester.

In the CPS case, there was a further delay to 2019 (for a total of nearly six years) before the Court decided that solicitor-client privilege did not apply to redactions on 3.5 other pages of records, and for those records to be disclosed to the requester.

In the Ministry of Municipal Affairs' (Municipal Affairs) case,[26] the access requester waited from 2015, which was the date of Municipal Affairs' response to the access request, to 2019 when Municipal Affairs had to provide the records to the Court (a total of four years), to learn that Municipal Affairs was withdrawing its litigation privilege claim on 51 of 249 pages of records. Municipal Affairs then provided those 51 pages of records to the Commissioner and asked the Commissioner to review those 51 pages under another exception to disclosure.

The conclusion that may be drawn is that privilege is over-claimed, resulting in public bodies reassessing privilege claims immediately before the Court reviews the records. In the CPS case, privilege was over-claimed on approximately 30% of the records. In the Municipal Affairs case, privilege was over-claimed on approximately 20% of the records.

The amount of time it takes to get to a decision about whether privilege applies is also an issue in this process. In the two cases discussed, it took four to six years for applicants to get access to records, either because public bodies decided to provide those records to the Commissioner or provide access to the records before the records had to be provided to the Court, or because the access requester had to wait for the Court's decision.

There were 11 other orders being judicially reviewed on the issue of claims of privilege that were before the Courts as of March 31, 2019.[27]

As of March 31, 2019, a response to the report on producing records to the Commissioner has not been received from government or the Legislative Assembly.

[26] *Alberta (Municipal Affairs) v Alberta (Information and Privacy Commissioner),* 2019 ABQB 74 and 2019 ABQB 436.

[27] As of October 3, 2019, there were 14 orders being judicially reviewed on the issue of claims of privilege.

Judicial Reviews and Other Court Decisions

Calgary (Police Service) v Alberta (Information and Privacy Commissioner)

2019 ABQB 109 – continuation of 2017 ABQB 656 which was upheld by the Alberta Court of Appeal in 2018 ABCA 114 – Judicial Review of Order F2016-35

In this final installment of the judicial review of Order F2016-35, the Court was able to undertake its review of records over which the Calgary Police Service (CPS) had asserted solicitor-client privilege. Since the time of the original access request dated August 2, 2013, this was the first time the records had been viewed by anyone other than CPS.

In the Court's initial decision (2017 ABQB 656), the Court held that although the records had been withheld from the Adjudicator, the Court could accept them as new evidence on judicial review to determine whether claims of solicitor-client privilege had been correctly made by CPS. This decision was upheld by the Alberta Court of Appeal (2018 ABCA 114).

Notably, as is discussed above, CPS continued to disclose records over which it had previously asserted solicitor-client privilege up until shortly before the time the records were provided to the Court for review of the privilege claims in the first instance.

In this decision, the Court set out the test to determine whether a claim of solicitor-client privilege has been correctly claimed over a record as follows:

- Is there a communication between a solicitor and a client?
- Does the communication entail the seeking, giving or receiving of legal advice?
- Is the communication intended by the parties to be confidential?
- Is the lawyer acting as a lawyer?
- What was the purpose for which the record came into existence?
- Is the particular communication part of a continuum in which legal advice is given?
- Does the particular communication reveal that legal advice has been sought or given?
- If there is privileged information, can it be reasonably severed from the rest of the record, without revealing the privilege?

After reviewing the remaining records over which CPS maintained its assertion of solicitor-client privilege, the Court provided a record by record summary of whether the record or a portion of it was subject to the privilege. The Court found that most of the remaining records or portions of them were privileged, but a few were not and were producible. This matter took nearly six years to be resolved.

Alberta Health Services v Information and Privacy Commissioner of Alberta

2018 ABQB 467 – Judicial Review of Order H2014-02

An individual complained that a program coordinator employed by Alberta Health Services (AHS) had called up and read his health information from Netcare on 17 occasions, alleging that this was contrary to section 25 of HIA. Ten of the occasions had taken place after the complainant had discontinued his physiotherapy treatment.

AHS argued that the program coordinator had used the complainant's health information in compliance with section 27(1)(a) (use for the purpose of providing a health service) and (b) (use for the purpose of determining eligibility for a health service) of HIA.

The Adjudicator found that neither the complainant nor anyone providing health services to him had requested that he receive health services, nor had the complainant agreed to receive any such health services. Since health services can only be provided to someone who has agreed to receive them, the Adjudicator determined that AHS' use of the health information could not be said to be for the purpose of providing a health service or determining eligibility for one. She found, in the alternative, that there was no evidence the program coordinator had restricted her use of the complainant's health information to only that health information essential for carrying out her purpose, as required by section 58 of HIA

The Adjudicator found that AHS had not prescribed the circumstances in which the program coordinator would be authorized to call up and read health information from Netcare in the course of her duties. While AHS had created a new guideline for Netcare use in its physiotherapy program, which was far more restrictive, AHS' evidence raised the issue that the guideline was not necessarily followed. AHS was ordered to cease using the complainant's health information and to ensure that employees in the physiotherapy area complied with the new guideline.

AHS requested a judicial review, arguing *inter alia* that the Adjudicator had not considered section 27(1)(g). The Court declined to review the matter under section 27(1)(g) of HIA, as no evidence had been provided by AHS regarding that provision and that issue had not been argued before the Adjudicator. The Court then continued with an analysis of the reasonableness of the Adjudicator's decision. The Court referred to the purposes of HIA set out in section 2, stating that HIA recognizes and seeks to guard the privacy rights of health care users, and thus generally prohibits the use of health information except for in specific circumstances authorized by the Act.

The Court held that the Adjudicator's findings under sections 27(1)(a) and (b) were reasonable, and further held it was reasonable for the Adjudicator to conclude that AHS had failed to safeguard the complainant's health information in contravention of section 60 of HIA. The Court concluded that this was a case where it should exercise its discretion and refuse to engage in judicial review, and in any event, the Adjudicator's decision was reasonable and not to be disturbed.

Alane Davis v Alberta Privacy Commissioner

Oral decision of Millar J., Action Nos. 1709 0094 and 1709 0095, February 28, 2018 – Judicial Reviews of Orders F2017-39 and F2017-40

In Order F2017-39, an individual complained that the Peace River School Division No. 10 (PRSD) relied on inaccurate or incomplete personal information when deciding not to hire her for a position because it determined that the complainant's references were not supportive of hiring her for the position for which she had applied. The Adjudicator held the information PRSD relied on was accurate and complete.

In Order F2017-40, an applicant requested that PRSD correct information in its custody and control under section 39 of the FOIP Act. PRSD declined to make the correction, and instead attached an annotation to the information. The Adjudicator found that PRSD properly responded to the applicant's request.

The judicial reviews of the two orders were heard together. The Court held that the orders were reasonable and dismissed the applications. See also: Davis v. Clayton, 2018 ABQB 312, wherein PRSD was awarded costs against the applicant.

Lin Xing v Office of the Information and Privacy Commissioner and Mount Royal University

Oral decision of Campbell J., Action No. 1601 03122
May 1, 2018 – Judicial Review of Order F2017-38

A student at Mount Royal University (MRU) complained that MRU disclosed her personal information in contravention of the FOIP Act when it provided various employees of MRU with a copy of a behavioural contract (the contract) between herself and MRU, which set out certain expectations.

The Adjudicator found it was appropriate for MRU to disclose the contract to employees of MRU so that the terms of the contract could be adhered to but that it disclosed the contract to department heads in contravention of the FOIP Act.

The complainant disputed the Adjudicator's finding that it was appropriate to disclose the contract to some employees; however, the Court held the Adjudicator's findings were reasonable and dismissed the judicial review application.

Glen Carter v Alberta (Ministry of Justice and Solicitor General) (MJSG), Calgary Police Service (CPS) and Alberta (Office of the Information and Privacy Commissioner)

Oral decision of Ashcroft J., Action No. 1801 05226
January 10, 2019

The applicant filed an originating application seeking a Court order for production of various records, including wiretap and surveillance records, believed to be held by the respondents. The Court noted that from 2001 to 2013 the applicant had brought approximately 94 various matters before the OIPC primarily relating to alleged police surveillance and monitoring.

After reviewing all the evidence and submissions, the Court held there was no evidence that the applicant was under investigation or surveillance and dismissed the application. The Court held that the application was a vexatious filing and an abuse of the Court. The applicant was ordered to pay costs to the respondents.

Further, on its own motion and under its inherent jurisdiction, the Court initiated a process to determine whether the applicant should be subject to litigation gatekeeping through court access restrictions. Further submissions were provided by the parties on this issue.[28]

[28] On August 9, 2019, the Court of Queen's Bench in *Carter v Alberta (Ministry of Justice and Solicitor General),* 2019 ABQB 491 declared the applicant to be a vexatious litigant. As a result, the applicant may not commence or continue any proceedings under the FOIP Act, HIA or PIPA unless he first applies and obtains leave of the Court. The Court gave the Commissioner an "advisory" role in any application the applicant may make to the Court. The applicant will require a Court order before he can make any access request under all three Acts.

EDUCATION & OUTREACH

Speaking Engagements

In 2018-19, the Commissioner and staff participated in 49 presentations, panels or workshops. This represented a decrease based on the average of 72 events at which the OIPC presented from 2015-16 to 2017-18. Due to caseload pressures, the OIPC unfortunately had to decline more speaking engagement requests in 2018-19.

RIGHT TO KNOW WEEK FORUM

As the OIPC prepared for mandatory breach reporting under HIA, and updated resources accordingly, only one Right to Know Week Forum was organized in 2018. Typically, the OIPC hosts forums in Calgary and Edmonton to recognize Right to Know Day.

The 2018 event in Edmonton was well attended. The forum included opening comments from the Commissioner, a presentation by Professor Steven Penney from the Faculty of Law at the University of Alberta who spoke about police disclosures of the identities of victims of crime, and a showing of the documentary entitled "Truth in Numbers? Everything, According to Wikipedia", which raises a number of questions broadly related to access to information in the 21st century.

Right to Know Day is internationally recognized annually on September 28. In 2015, the United Nations Educational, Scientific and Cultural Organization (UNESCO) adopted a resolution to proclaim September 28 as the "International Day for the Universal Access to Information". Right to Know Day recognizes the importance of the right to access public information as an integral component of freedom of expression.

DATA PRIVACY DAY EVENTS

Smart cities and breach reporting were the topics covered at the OIPC's 2019 Data Privacy Day events in Calgary and Edmonton.

Both the Edmonton and Calgary events included presentations by the City of Edmonton's Healthy City Initiative, which was a $50 million finalist for Infrastructure Canada's Smart Cities Challenge. The City of Edmonton's smart cities proposal was guided by its challenge statement, which read, "Edmonton will lead the transformation of Canadian healthcare using an unprecedented municipal approach by focusing on leveraging relationships, health data and innovative technologies to provide a personalized health connection and experience as unique as the health of every Edmontonian."

In Calgary, Infrastructure Canada's Smart Cities Challenge was described in detail by a representative of Infrastructure Canada who explained the thinking behind the ambitious, nationwide contest, and how its focus on privacy was guided in part by federal, provincial and territorial Privacy Commissioners who wrote an open letter to the federal Minister of Infrastructure and Communities outlining the importance of considering privacy risks and mitigation strategies in smart cities initiatives.

In Edmonton, the OIPC welcomed a representative from the Office of the Privacy Commissioner of Canada (OPC) to speak about mandatory breach reporting under the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which came into force on November 1, 2018. Concurrent with the event in Edmonton, the OIPC was hosting staff members from the OPC to learn about how the OIPC manages breach reports from private sector organizations, since Alberta was the first and only jurisdiction in Canada to require private sector organizations to report certain privacy breaches between May 2010 and October 2018.

The OIPC also presented on the first four months of mandatory breach reporting under HIA in both Calgary and Edmonton.

Data Privacy Day is internationally recognized on January 28 to promote the protection of personal information.

GDPR'S IMPACT IN COLOMBIA AND THE AMERICAS

The Commissioner had the honour of presenting at a conference hosted by Colombia's Superintendence of Industry and Commerce in Santa Marta, Colombia in June 2018. The focus of the conference was the impact of the European Union's *General Data Protection Regulation* (GDPR) in Colombia and the Americas. The Commissioner participated in two different presentations:

- A panel discussion on the "GDPR's New Approach to Consent", with private sector and regulatory representatives from Canada, the United States, and Latin and Central America
- A plenary on consent from a Canadian privacy regulator's perspective in a presentation entitled "Implementation of the Principle of Demonstrated Responsibility by Public Entities"

Max Schrems Visits the OIPC

One of the world's most recognized privacy advocates, Max Schrems, made an impromptu visit to the OIPC's Edmonton office in April 2018. Taking time out of his Canadian vacation, Schrems graciously agreed to talk to staff about how he helped dismantle the EU-US Safe Harbor arrangement, what his views were on GDPR a month before it came into force, and his new, non-governmental advocacy organization called "noyb" – an abbreviation for none of your business – and briefly discussed what his plans for it were.

PIA AND BREACH WORKSHOPS FOR ALBERTA'S HEALTH SECTOR

In light of the increase in PIAs submitted by health custodians and new breach reporting requirements under HIA, the OIPC invited certain regulated health professions to attend its May 2018 workshops.

Considering the additional responsibilities for health custodians, a more targeted approach was undertaken to ensure regulated health professionals and their staff have an opportunity to learn about how to respond to and report privacy breaches, and to better understand the essentials for completing PIAs.

In prior workshops the OIPC offered, most if not all of the registrants were employees from public bodies as this is an audience most easily reached through the OIPC's established communications channels.

Collaboration with Other Jurisdictions

The OIPC annually partners with Information and Privacy Commissioners across Canada, as well as international counterparts, on a variety of initiatives.

JOINT RESOLUTION ON POLITICAL PARTIES

Canada's federal, provincial and territorial Information and Privacy Commissioners and Ombudspersons held their annual meeting in Regina, Sask. in September 2018, at which they passed a joint resolution on political parties.

The joint resolution, "Securing Trust and Privacy in Canada's Electoral Process", called on governments to pass legislation requiring political parties to comply with globally recognized privacy principles, to provide Canadians with a right of access to the personal information political parties hold about them, and to provide for independent oversight to verify and enforce privacy compliance.

Largely spurred by events earlier in the year that exposed how political parties collect and use personal information to target individuals in specific and unique ways for political gain, the resolution garnered plenty of media attention, especially with the Alberta and federal elections slated for 2019.

Over the years, the OIPC has received several privacy complaints from Albertans about how political parties have handled their personal information. In those cases, the OIPC has had to inform individuals that the office does not have jurisdiction to review their complaints.

Only in British Columbia are political parties subject to privacy legislation. In February 2019, the Information and Privacy Commissioner for British Columbia released an investigation report on how the province's major political parties manage personal information of British Columbians. Among several findings, the report concluded that political parties were collecting too much personal information without getting proper consent. The report made 17 recommendations.[29]

Political Parties and Privacy Laws

> "Political parties collect and analyze vast amounts of personal information on voters. However, Albertans have limited recourse when they have concerns about how political parties have handled their personal information. Albertans also have no explicit right to request access to the personal information that political parties gather about them. Privacy rights are about transparency and control. Albertans should have these rights when interacting with political parties."
>
> *- Commissioner Jill Clayton, September 17, 2018*[30]

[29] The Office of the Information and Privacy Commissioner for British Columbia's news release on the investigation into political parties is available at www.oipc.bc.ca/news-releases/2279. Investigation report P19-01 is available at www.oipc.bc.ca/investigation-reports/2278.

[30] The OIPC's news release is available at www.oipc.ab.ca/news-and-events/news-releases/2018/canadas-access-to-information-and-privacy-guardians-call-for-privacy-regulation-and-oversight-of-political-parties.aspx.

SMART CITIES CHALLENGE

In April 2018, Canada's federal, provincial and territorial privacy protection authorities wrote to the federal Minister of Infrastructure and Communities to urge Infrastructure Canada to proactively take steps to ensure that privacy and security of personal information are specifically considered in the selection, design and implementation of the winning proposals in its Smart Cities Challenge, which had been launched under the Government of Canada's Impact Canada Initiative.

The Commissioners recognized the potential value of smart city initiatives, such as allowing communities to more effectively address the challenges of urbanization and allocate resources accordingly. Yet, they also outlined some of the privacy risks of such projects, such as enabling the privacy-invasive technologies of surveillance or profiling, which can compromise public trust. To ensure that privacy and security are protected and embedded into smart city projects, the Commissioners outlined mitigating controls for municipalities to consider in their smart city proposals.

This call to action by Canada's privacy authorities led to collaboration between Infrastructure Canada and Commissioners' offices to ensure that privacy became a component in final proposals by the challenge's finalists. Finalists had to engage their respective Commissioner's office and submit a preliminary PIA to those offices for review. A privacy grading component was also established as part of the selection process.

The OIPC worked with the City of Edmonton, City of Airdrie, and the joint submission of Parkland, Brazeau, Lac Ste. Anne and Yellowhead Counties, which were the finalists from Alberta.

More information about the Smart Cities Challenge is available at www.infrastructure.gc.ca.

ICDPPC RESOLUTION ON E-LEARNING PLATFORMS

Through the International Conference of Data Protection and Privacy Commissioners (ICDPPC), the OIPC joined the Digital Education Working Group in 2018-19. As part of that working group, the OIPC co-authored a resolution that was passed at ICDPPC in October 2018 entitled "Resolution on E-Learning Platforms".[31]

The resolution recognizes that some e-learning platforms or apps "have enormous capacity to foster the development of innovative and effective learning practices", such as helping connect students, parents and teachers. However, these education tools may pose threats to the privacy and security of students, parents and educators due to companies' opaque personal information practices. Additionally, education and awareness of digital privacy rights and knowledge of secure practices has not kept pace with the proliferation of e-learning tools in classrooms.

For the purposes of Alberta's education sector, there are certain actions educational authorities are called upon to incorporate to help improve the understanding of digital privacy rights and compliance with privacy laws, and to help ensure students' personal information is secure.

In March 2019, the Commissioner wrote to the Minister of Education and Superintendents of Schools at Alberta's publicly-funded school districts to raise awareness of the resolution, and to highlight recommended actions education authorities could take to improve vetting and implementation of education apps and tools in Alberta's classrooms.

[31] The ICDPPC's resolution is available at https://icdppc.org/document-archive/adopted-resolutions/.

ICDPPC Declaration on Ethics in AI

In addition to the resolution on e-learning platforms, the International Conference of Data Protection and Privacy Commissioners also passed the "Declaration on Ethics in AI".[32]

The international declaration recognizes that artificial intelligence systems have incredible potential and are being used for innovations in a variety of disciplines, often without any privacy implications, such as in industrial systems. But there are other considerations, especially privacy and other human rights implications when massive personal data sets make decisions about or for individuals.

The conference endorsed principles for ethical assessments based on:

- Fairness for individuals and groups, such as ensuring that AI systems remain consistent with their original purposes
- Accountability for all relevant stakeholders, such as establishing governance processes or setting up independent ethics committees or oversight
- Transparency, such as promotion of algorithmic transparency and the auditability of systems
- Ethics by design, such as assessing and documenting the expected impacts on individuals and society at the beginning of an artificial intelligence project
- Empowerment of the individual by providing individuals with a way to exercise their individual rights
- Mitigating unlawful biases or discriminatory practices by investing in research to discover technical ways to identify, address and diminish biases

The declaration also emphasizes the need for trust, and the need for international standards and approaches to ensure human rights, human dignity and information privacy are components of artificial intelligence technologies that involve the use of personal information.

INTERNATIONAL CONFERENCE OF INFORMATION COMMISSIONERS

The Commissioner was involved in two committees of the International Conference of Information Commissioners (ICIC) in 2018-19.

The Commissioner is a member of the ICIC Governance Working Group, established to develop a governance structure and processes. Work on that committee in 2018-19 involved reviewing and providing input on a founding charter, which includes guiding principles, vision and mission, conference structure and membership accreditation, operational leadership, executive leadership, and funding.

The Commissioner also participated in the ICIC Planning Committee for its 2019 conference in South Africa, which included providing input on conference theme, plenary speakers and panel topics.

At ICIC 2019, the "Johannesburg Charter" was adopted by a resolution of the Information Commissioners present at the closed meeting of ICIC in South Africa. The charter establishes the governance framework of ICIC by setting out the guiding principles, the vision and the mission, the values, the goals, the role of the conference, its membership, its governance structure, and the rules governing the participation of its members. ICIC is now undertaking an accreditation process for members based on the charter.

More information about ICIC is available at www.informationcommissioners.org.

[32] The ICDPPC's declaration is available at https://icdppc.org/document-archive/adopted-resolutions/.

Media Awareness

TRADITIONAL MEDIA

The OIPC received 72 media requests in 2018-19 compared to 73 in 2017-18.

New technologies for the collection, use and disclosure of personal information, the state of access to information in Alberta, and investigation reports issued by the OIPC received the most attention.

The use of at-home genetic or DNA testing services exploded over the past couple years. The OIPC received a few media requests about the privacy implications of these technologies. The Commissioner noted that genetic information is deeply personal and cannot be changed in the event of a breach, unlike credit card information or other types of personal information. Ultimately, it is about consumer choice as to whether to use a genetic testing service, but it is important that individuals understand the risks and know what questions to ask companies about how their privacy is being protected.

Facial recognition technology used in certain Calgary shopping malls received plenty of media coverage. Initially, the Commissioner was following media reports and the OIPC noted that anyone with concerns that their personal information was collected without consent could submit a complaint. A news release was subsequently issued to announce that the Commissioner had opened an investigation into the use of facial recognition without consent by Cadillac Fairview Corporation Limited at shopping centres it operates in Calgary.

Other technologies that reporters asked questions about included licence plate scanning at Edmonton International Airport, Edmonton Police Service's Intelligence Command Unit and identification scanners at licensed establishments.

After the Commissioner presented the 2017-18 Annual Report and 2019-20 Budget Estimate to the Standing Committee on Legislative Offices, during which she stated that the OIPC had reached its "breaking point", a few reporters requested interviews to discuss the state of access to information in Alberta. While many of the caseload pressures are a result of delays and added complexity when public bodies respond to access requests, the OIPC also had additional privacy responsibilities that contributed to the office's "breaking point".

The OIPC's investigation reports on managing and storing emails within the Government of Alberta, and alleged unauthorized accesses of health information at Alberta Hospital Edmonton also garnered media requests.

SOCIAL MEDIA

The OIPC uses Twitter to share orders, investigation reports, publications and news releases, and promote events or raise awareness about access and privacy laws. When appropriate, the OIPC will also respond to questions or concerns.

The following topics received among the most views on Twitter:

- The announcement on opening an investigation into Cadillac Fairview Corporation Limited's use of facial recognition technology without consent at shopping centres it operates in Calgary.
- The Edmonton Journal's editorial board's agreement with Canada's Privacy Commissioners about the need for privacy regulation and oversight of Canada's federal and provincial political parties.
- The City of Edmonton's Smart Cities Challenge presentation at the OIPC's Data Privacy Day event.
- The OIPC's commissioned research report on "Designing Freedom of Information Systems: An Overview from Legislation to Implementation".
- The OIPC's 2017-18 Annual Report, specifically the Trends and Issues section, which highlighted political parties, GDPR, artificial intelligence and machine learning, genetic testing, and blockchain.

The OIPC's Twitter account is available at www.twitter.com/ABoipc.

Designing Freedom of Information Systems: An Overview from Legislation to Implementation

Implementation of Service Alberta's project to consolidate the administration of FOIP Services for the Government of Alberta (GoA) began in 2018-19. Prior to implementation of this project, the OIPC heard that changes to how the FOIP Act is administered by the GoA were being considered.

In response, the OIPC commissioned an independent research paper entitled "Designing Freedom of Information Systems: An Overview from Legislation to Implementation". The research paper examines the implications of different models that governments use to handle access to information requests. Specifically, it compares a decentralized system where the response mandate is held by individual government departments to a system where response is centralized in one government department.

The research paper is available at www.oipc.ab.ca.

FINANCIAL STATEMENTS

Auditor General
OF ALBERTA

Independent Auditor's Report

To the Members of the Legislative Assembly

Report on the Financial Statements

Opinion

I have audited the financial statements of the Office of the Information and Privacy Commissioner, which comprise the statement of financial position as at March 31, 2019, and the statements of operations, change in net debt, and cash flows for the year then ended, and notes to the financial statements, including a summary of significant accounting policies.

In my opinion, the accompanying financial statements present fairly, in all material respects, the financial position of the Office of the Information and Privacy Commissioner as at March 31, 2019, and the results of its operations, its changes in net debt, and its cash flows for the year then ended in accordance with Canadian public sector accounting standards.

Basis for opinion

I conducted my audit in accordance with Canadian generally accepted auditing standards. My responsibilities under those standards are further described in the *Auditor's Responsibilities for the Audit of the Financial Statements* section of my report. I am independent of the Office of the Information and Privacy Commissioner in accordance with the ethical requirements that are relevant to my audit of the financial statements in Canada, and I have fulfilled my other ethical responsibilities in accordance with these requirements. I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my opinion.

Other information

Management is responsible for the other information. The other information comprises the information included in the *Annual Report,* but does not include the financial statements and my auditor's report thereon. The *Annual Report* is expected to be made available to me after the date of this auditor's report.

My opinion on the financial statements does not cover the other information and I do not express any form of assurance conclusion thereon.

In connection with my audit of the financial statements, my responsibility is to read the other information identified above and, in doing so, consider whether the other information is materially inconsistent with the financial statements or my knowledge obtained in the audit, or otherwise appears to be materially misstated.

If, based on the work I will perform on this other information, I conclude that there is a material misstatement of this other information, I am required to communicate the matter to those charged with governance.

Responsibilities of management and those charged with governance for the financial statements

Management is responsible for the preparation and fair presentation of the financial statements in accordance with Canadian public sector accounting standards, and for such internal control as management determines is necessary to enable the preparation of the financial statements that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements, management is responsible for assessing the Office of the Information and Privacy Commissioner's ability to continue as a going concern, disclosing, as applicable, matters related to going concern and using the going concern basis of accounting unless an intention exists to liquidate or to cease operations, or there is no realistic alternative but to do so.

Those charged with governance are responsible for overseeing the Office of the Information and Privacy Commissioner's financial reporting process.

Auditor's responsibilities for the audit of the financial statements

My objectives are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes my opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with Canadian generally accepted auditing standards will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of these financial statements.

As part of an audit in accordance with Canadian generally accepted auditing standards, I exercise professional judgment and maintain professional skepticism throughout the audit. I also:

- Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for my opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.
- Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Office of the Information and Privacy Commissioner's internal control.
- Evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by management.
- Conclude on the appropriateness of management's use of the going concern basis of accounting and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the Office of the Information and Privacy Commissioner's ability to continue as a going concern. If I conclude that a material uncertainty exists, I am required to draw attention in my auditor's report to the related disclosures in the financial statements or, if such disclosures are inadequate, to modify my opinion. My conclusions are based on the audit evidence obtained up to the date of my auditor's report. However, future events or conditions may cause the Office of the Information and Privacy Commissioner to cease to continue as a going concern.
- Evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation.

I communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that I identify during my audit.

Original signed by
W. Doug Wylie FCPA, FCMA, ICD.D

Auditor General
July 17, 2019
Edmonton, Alberta

Financial Statements

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
STATEMENT OF OPERATIONS

Year ended March 31, 2019

	2019		2018
	Budget	Actual	Actual
Revenues			
Prior Year Expenditure Refund	$ -	$ 533	$ 9,482
Other Revenue	-	157	734
	-	690	10,216
Expenses – Directly Incurred (Note 3b)			
Salaries, Wages, and Employee Benefits	$ 5,816,291	$ 5,151,582	$ 5,132,348
Supplies and Services	1,100,200	1,672,129	1,536,055
Amortization of Tangible Capital Assets (Note 4)	55,000	50,591	47,003
Total Program-Operations	6,971,491	6,874,302	6,715,406
Net Cost of Operations	$ (6,971,491)	$ (6,873,612)	$ (6,705,190)

The accompanying notes and schedules are part of these financial statements.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

STATEMENT OF FINANCIAL POSITION

As at March 31, 2019

	2019	2018
Financial Assets		
Cash	$ 200	$ 200
Accounts Receivable	10	2,490
	210	2,690
Liabilities		
Accounts Payable and Accrued Liabilities	190,440	310,886
Accrued Vacation Pay	461,903	498,119
	652,343	809,005
Net Debt	(652,133)	(806,315)
Non-Financial Assets		
Tangible Capital Assets (Note 4)	63,615	114,206
Prepaid Expenses	30,538	13,606
	94,153	127,812
Net Liabilities	$ (557,980)	$ (678,503)
Net Liabilities at Beginning of Year	$ (678,503)	$ (713,181)
Net Cost of Operations	(6,873,612)	(6,705,190)
Net Financing Provided from General Revenues	6,994,135	6,739,868
Net Liabilities at End of Year	$ (557,980)	$ (678,503)

Contractual obligations (Note 6)

The accompanying notes and schedules are part of these financial statements.

Financial Statements

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

STATEMENT OF CHANGE IN NET DEBT

Year ended March 31, 2019

	2019		2018
	Budget	Actual	Actual
Net Cost of Operations	$ (6,971,491)	$ (6,873,612)	$ (6,705,190)
Acquisition of Tangible Capital Assets (Note 4)	-	-	(20,032)
Amortization of Tangible Capital Assets (Note 4)	55,000	50,591	47,003
Change in Prepaid Expenses	-	(16,932)	(2,869)
Net Financing Provided from General Revenues	6,916,491	6,994,135	6,739,868
Decrease in Net Debt	-	154,182	58,780
Net Debt, Beginning of Year	-	(806,315)	(865,095)
Net Debt, End of Year	$ -	$ (652,133)	$ (806,315)

The accompanying notes and schedules are part of these financial statements.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
STATEMENT OF CASH FLOWS

Year ended March 31, 2019

	2019	2018
Operating Transactions		
Net Cost of Operations	$ (6,873,612)	$ (6,705,190)
Non-cash Items Included in Net Cost of Operations		
Amortization of Tangible Capital Assets (Note 4)	50,591	47,003
	(6,823,021)	(6,658,187)
Decrease in Accounts Receivable	2,480	1,156
(Increase) in Prepaid Expenses	(16,932)	(2,869)
(Decrease) in Accounts Payable and Accrued Liabilities	(156,662)	(59,936)
Cash Applied to Operating Transactions	(6,994,135)	(6,719,836)
Capital Transactions		
Acquisition of Tangible Capital Assets (Note 4)	-	(20,032)
Financing Transactions		
Net Financing Provided from General Revenues	6,994,135	6,739,868
Cash, Increase	-	-
Cash, at Beginning of Year	200	200
Cash, at End of Year	$ 200	$ 200

The accompanying notes and schedules are part of these financial statements.

Financial Statements

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NOTES TO THE FINANCIAL STATEMENTS

March 31, 2019

Note 1 Authority

The Office of the Information and Privacy Commissioner (the Office) operates under the authority of the *Freedom of Information and Protection of Privacy Act*. General Revenues of the Province of Alberta fund both the cost of operations of the Office of the Information and Privacy Commissioner and the purchase of tangible capital assets. The all-party Standing Committee on Legislative Offices reviews and approves the Office's annual operating and capital budgets.

Note 2 Purpose

The Office provides oversight on the following legislation governing access to information and protection of privacy:

Freedom of Information and Protection of Privacy Act
Health Information Act
Personal Information Protection Act

The major operational purposes of the Office are:

- To provide independent reviews of decisions made by public bodies, custodians and organizations under the Acts and the resolution of complaints under the Acts;
- To advocate protection of privacy for Albertans; and
- To promote openness and accountability for public bodies.

Note 3 Summary of Significant Accounting Policies and Reporting Practices

These financial statements are prepared in accordance with Canadian public sector accounting standards, which use accrual accounting. The Office has adopted PS 3450 Financial Instruments. The adoption of this standard has no material impact on the financial statements of the Office, which is why there is no statement of remeasurement gains and losses.

The Office has adopted PS 3430 Restructuring Transactions effective April 1, 2018. The adoption of this standard has no material impact on the financial statements of the Office.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2019

Note 3 Summary of Significant Accounting Policies and Reporting Practices (continued)

Other pronouncements issued by the Public Sector Accounting Board that are not yet effective are not expected to have a material impact on future financial statements of the Office.

a) Revenue

All revenues are reported on the accrual basis of accounting.

b) Expenses

The Office's expenses are either directly incurred or incurred by others:

Directly incurred

Directly incurred expenses are those costs incurred under the authority of the Office's budget as disclosed in the Office's budget documents.

Pension costs included in directly incurred expenses comprise employer contributions to multi-employer plans. The contributions are based on actuarially determined amounts that are expected to provide the plans' future benefits.

Incurred by others

Services contributed by other entities in support of the Office's operations are not recognized and are disclosed in Schedule 2.

c) Financial assets

Financial assets are assets that could be used to discharge existing liabilities or finance future operations and are not for consumption in the normal course of operations.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2019

Note 3 Summary of Significant Accounting Policies and Reporting Practices (continued)

d) Liabilities

Liabilities are present obligations of the Office to external organizations and individuals arising from past transactions or events, the settlement of which is expected to result in the future sacrifice of economic benefits. They are recognized when there is an appropriate basis of measurement and management can reasonably estimate the amounts.

e) Non-financial assets

Non-financial assets are acquired, constructed, or developed assets that do not normally provide resources to discharge existing liabilities, but instead:

(a) are normally employed to deliver the Office's services;
(b) may be consumed in the normal course of operations; and
(c) are not for sale in the normal course of operations.

Non-financial assets of the Office are limited to tangible capital assets and prepaid expenses.

f) Tangible capital assets

Tangible capital assets are recorded at historical cost less accumulated amortization. Amortization begins when the assets are put into service and is recorded on a straight-line basis over the estimated useful lives of the assets. The threshold for tangible capital assets is $5,000 except new systems development is $250,000 and major enhancements to existing systems is $100,000.

g) Net debt

Net debt indicates additional cash required from General Revenues to finance the Office's cost of operations to March 31, 2019.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2019

Note 4 Tangible Capital Assets

	Office equipment and furniture	Computer hardware and software	Total
Estimated Useful Life	5 years	5 years	
Historical Cost			
Beginning of Year	$ 83,318	$ 452,343	$ 535,661
Additions	-	-	-
	$ 83,318	$ 452,343	$ 535,661
Accumulated Amortization			
Beginning of Year	$ 75,959	$ 345,496	$ 421,455
Amortization Expense	3,680	46,911	50,591
	$ 79,639	$ 392,407	$ 472,046
Net Book Value at March 31, 2019	$ 3,679	$ 59,936	$ 63,615
Net Book Value at March 31, 2018	$ 7,359	$ 106,847	$ 114,206

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2019

Note 5 Defined Benefit Plans

The Office participates in the multi-employer pension plans: Management Employees Pension Plan, Public Service Pension Plan and Supplementary Retirement Plan for Public Service Managers. The expense for these pension plans is equivalent to the annual contributions of $666,011 for the year ended March 31, 2019 (2018 – $671,822).

At December 31, 2018, the Management Employees Pension Plan reported a surplus of $670,700,000 (2017 - surplus $866,006,000) and the Public Service Pension Plan reported a surplus of $519,218,000 (2017 – surplus $1,275,843,000). At December 31, 2018 the Supplementary Retirement Plan for Public Service Managers had a deficit of $70,310,000 (2017 - deficit $54,984,000).

The Office also participates in a multi-employer Long Term Disability Income Continuance Plan. At March 31, 2019, the Management, Opted Out and Excluded Plan reported an actuarial surplus of $24,642,000 (2018 – surplus $29,805,000). The expense for this plan is limited to employer's annual contributions for the year.

Note 6 Contractual Obligations

Contractual Obligations are obligations of the Office to others that will become liabilities in the future when the terms of those contracts or agreements are met.

	2019	2018
Obligations under operating leases and contracts	$ 18,955	$ 23,399

Estimated payment requirements for each of the next three years are as follows:

	Total
2019-20	$ 11,844
2020-21	6,226
2021-22	885
	$ 18,955

Note 7 Approval of Financial Statements

These financial statements were approved by the Information and Privacy Commissioner.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

SCHEDULE 1 - SALARY AND BENEFITS DISCLOSURE

Year ended March 31, 2019

	2019			2018
	Base Salary [a]	Other Non-cash Benefits [b][c]	Total	Total
Senior Official				
Information and Privacy Commissioner	$ 242,743	$ 61,728	$ 304,471	$ 306,402

[a] Base salary is comprised of pensionable base pay.

[b] Other non-cash benefits include the Office's share of all employee benefits and contributions or payments made on behalf of employee, including pension, supplementary retirement plan, health care, dental coverage, group life insurance, short and long term disability plans, health spending account, conference fees, professional memberships, and tuition fees.

[c] Other non-cash benefits for the Information and Privacy Commissioner paid by the Office includes $6,248 (2018: $8,185) being the lease, fuel, insurance and maintenance expenses for an automobile provided by the Office.

Financial Statements

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

SCHEDULE 2 - ALLOCATED COSTS

Year ended March 31, 2019

	2019					2018
	Expenses - Incurred by Others					
Program	Expenses [a]	Accommodation Costs [b]	Telephone Costs [c]	Business Services [d]	Total Expenses	Total Expenses
Operations	$ 6,874,302	$ 500,790	$ 18,816	$ 43,000	$ 7,436,908	$ 7,268,206

[a] Expenses - Directly Incurred as per Statement of Operations.
[b] Costs shown for Accommodation (includes grants in lieu of taxes), allocated by square meters.
[c] Other costs are for telephone land line charges.
[d] Business services includes charges for shared services, finance services, technology services, IMAGIS, and Corporate Overhead.

APPENDICES

APPENDIX A: CASES OPENED UNDER FOIP, HIA, PIPA BY ENTITY TYPE

Statistics are from April 1, 2018 to March 31, 2019

FOIP

Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Disclosure to Commissioner (Whistleblower)	Engage in or Commission a Study	Excuse Fee	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request Authorization to Indirectly Collect	Request for Information	Request for Review	Request for Review 3rd Party	Request Time Extension	Self-reported Breach	Total
Agencies												2		4	1		**7**
Boards			9						2			10	2	2			**25**
Colleges			1						1			3	1		8		**14**
Commissions			1						1		3	5	1	2	1		**14**
Committees																	**0**
Crown Corporations																	**0**
Federal Departments									1								**1**
Foundations																	**0**
Government Ministries/Departments		5	24			4	1		1	10		6	117	6	131	32	**337**
Health Quality Council of Alberta																	**0**
Hospital Board (Covenant Health)																	**0**
Law Enforcement Agencies	1	1	9					7	2	1			72		12	3	**108**
Legislative Assembly Office																	**0**
Local Government Bodies			5									1	2			2	**10**
Long Term Care Centres																	**0**
Municipalities		1	28			5	2			7		6	84	14	51	32	**230**
Nursing Homes												1	1				**2**
Office of the Premier/ Alberta Executive Council													1		7		**8**
Officers of the Legislature			1				1									1	**3**
Panels																	**0**
Regional Health Authorities (Alberta Health Services)		2	4				1					1	20	7	4		**39**
School Districts			4			7	2					4	26		2	11	**56**
Universities			5										15	1	11	7	**39**
Other							1					1				8	**10**
Total	**1**	**9**	**91**	**0**	**0**	**16**	**8**	**7**	**3**	**23**	**0**	**23**	**358**	**32**	**226**	**106**	**903**

Note: The statistics do not include Intake cases.

APPENDIX A: CASES OPENED UNDER FOIP, HIA, PIPA BY ENTITY TYPE

Statistics are from April 1, 2018 to March 31, 2019

HIA

Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Engage in or Commission a Study	Excuse Fee	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Affiliates and Information Managers (Electronic Medical Record Vendors, Consultants)									1				1	**2**
Associations, Boards, Councils, Committees, Commissions, Panels or Agencies, created by Custodians									2					**2**
Chiropractors									51	3				**54**
Dental Hygienists									12					**12**
Dentists			1						363				5	**369**
Denturists			1											**1**
Government Ministries/Departments														**0**
Health Professional Colleges and Associations										5				**5**
Health Quality Council of Alberta														**0**
Hospital Board (Covenant Health)									3	2	1		9	**15**
Long Term Care Centres									2		1		1	**4**
Midwives														**0**
Minister of Health (Alberta Health)									10	2	2		65	**79**
Nursing Homes									2				2	**4**
Opticians														**0**
Optometrists									52	1	1			**54**
Pharmacies/Pharmacists			5			3		1	164				137	**310**
Physicians			17			4		1	315	16	12		120	**485**
Podiatrists									4					**4**
Primary Care Networks			1						18	2			9	**30**
Regional Health Authorities (Alberta Health Services)		3	17		1	4			42	1	7		295	**370**
Registered Nurses									17	2			1	**20**
Research Ethics Boards														**0**
Researchers														**0**
Subsidiary Health Corporations			1					1	1	1			18	**22**
Universities/Faculties of Medicine										1			1	**2**
Other								8		3			10	**21**
Total	**0**	**3**	**43**	**0**	**1**	**11**	**0**	**11**	**1059**	**39**	**24**	**0**	**674**	**1865**

Note: The statistics do not include Intake cases.

APPENDIX A: CASES OPENED UNDER FOIP, HIA, PIPA BY ENTITY TYPE

Statistics are from April 1, 2018 to March 31, 2019

PIPA Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Engage in or Commission a Study	Excuse Fee	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request for Advanced Ruling	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Accommodation & Food Services			4								2		8		**14**
Admin & Support Services											1		8		**9**
Agriculture, Forestry, Fishing and Hunting											1		1		**2**
Arts, Entertainment & Recreation			1					1	1	1	1		8		**13**
Child Day-Care Services			4			1					2		4		**11**
Collection Agencies			2							1					**3**
Construction			1								2		5		**8**
Credit Bureaus											2		2		**4**
Credit Unions			1							1	1		12		**15**
Dealers in Automobiles			1										1		**2**
Educational Services										4	1		7		**12**
Finance		1	4								5	1	36		**47**
Health Care & Social Assistance			1							2			5		**8**
Information & Cultural Industries	1		4			3							6		**14**
Insurance Industry			6					2		4	3		23		**38**
Investigative & Security Services			2							1					**3**
Legal Services		2	8								4		10		**24**
Management of Companies & Enterprises			1			1							1		**3**
Manufacturing			1							1			12		**14**
Medical & Diagnostic Laboratories			1							1	1		2		**5**
Mining, Oil and Gas			5								6		14		**25**
Nursing Homes/Home Health Care			5					2			4		10		**21**
Private Health Care & Social Assistance			6					1		2	2		11		**22**
Professional, Scientific & Technical			8					1		1	1		22		**33**
Public Administration										1			1		**2**
Real Estate, Rental, Leasing			15			1				1	2		5		**24**
Retail			2			1				3			40		**46**
Trades/Contractors			2								2				**4**
Transportation			6										12		**18**
Utilities			2												**2**
Wholesale Trade			1										4		**5**
Other			18					1		7	8		20		**54**
Total	**1**	**3**	**112**	**0**	**0**	**7**	**0**	**0**	**8**	**1**	**31**	**51**	**1**	**290**	**505**

Note: The statistics do not include Intake cases.

APPENDIX B: CASES CLOSED UNDER FOIP, HIA, PIPA BY ENTITY TYPE

Statistics are from April 1, 2018 to March 31, 2019

FOIP

Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Disclosure to Commissioner (Whistleblower)	Engage in or Commission a Study	Excuse Fee	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request Authorization to Indirectly Collect	Request for Information	Request for Review	Request for Review 3rd Party	Request Time Extension	Self-reported Breach	**Total**
Agencies			1				1			1			3		4		**10**
Boards			6										9		2		**17**
Colleges			7											3	1	4	**15**
Commissions			1									2	6		2	1	**12**
Committees																	**0**
Crown Corporations																	**0**
Federal Departments			1														**1**
Foundations																	**0**
Government Ministries/Departments		3	19			5	23			6		7	115	8	137	25	**348**
Health Quality Council of Alberta																	**0**
Hospital Board (Covenant Health)																	**0**
Law Enforcement Agencies			8					7				1	59		10	2	**87**
Legislative Assembly Office													1				**1**
Local Government Bodies			3										1			1	**5**
Long Term Care Centres																1	**1**
Municipalities		2	18			2	2			4		7	67	9	50	31	**192**
Nursing Homes												1					**1**
Office of the Premier/Alberta Executive Council							2						5	1	8	1	**17**
Officers of the Legislature																1	**1**
Panels																	**0**
Regional Health Authorities (Alberta Health Services)		1	8				1					1	27	1	5		**44**
School Districts			5			7				1		3	9			11	**36**
Universities			5				1					1	13	1	11	2	**34**
Other			0				1			0		1	1		1	3	**7**
Total	**0**	**6**	**82**	**0**	**0**	**14**	**31**	**7**	**0**	**12**	**0**	**24**	**316**	**23**	**231**	**83**	**829**

Note: The statistics do not include Intake cases.

APPENDIX B: CASES CLOSED UNDER FOIP, HIA, PIPA BY ENTITY TYPE

Statistics are from April 1, 2018 to March 31, 2019

HIA

Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Engage in or Commission a Study	Excuse Fee	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Affiliates and Information Managers (Electronic Medical Record Vendors, Consultants)												1		**1**
Associations, Boards, Councils, Committees, Commissions, Panels or Agencies, created by Custodians														**0**
Chiropractors								27	1			1		**29**
Dental Hygienists								7						**7**
Dentists								164				3		**167**
Denturists			1											**1**
Government Ministries/Departments														**0**
Health Professional Colleges and Associations			1						6			1		**8**
Health Quality Council of Alberta								1						**1**
Hospital Board (Covenant Health)			3					1	2	1		9		**16**
Long Term Care Centres								1		1				**2**
Midwives														**0**
Minister of Health (Alberta Health)						1		13	2	1		54		**71**
Nursing Homes								1		1		1		**3**
Opticians														**0**
Optometrists								54	1					**55**
Pharmacies/Pharmacists			5					161				65		**231**
Physicians			19			1		1	187	9	7	72		**296**
Podiatrists								2						**2**
Primary Care Networks								11	1			3		**15**
Regional Health Authorities (Alberta Health Services)			47			2		23	1	7		109		**189**
Registered Nurses								15	2			1		**18**
Research Ethics Boards														**0**
Researchers														**0**
Subsidiary Health Corporations			4				1	1	1			7		**14**
Universities/Faculties of Medicine									1			1		**2**
Other			1			1	4		3			8		**17**
Total	**0**	**0**	**81**	**0**	**0**	**5**	**0**	**6**	**669**	**30**	**18**	**0**	**336**	**1145**

Note: The statistics do not include Intake cases.

APPENDIX B: CASES CLOSED UNDER FOIP, HIA, PIPA BY ENTITY TYPE

Statistics are from April 1, 2018 to March 31, 2019

PIPA Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Engage in or Commission a Study	Excuse Fee	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request for Advanced Ruling	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Accommodation & Food Services													8		**8**
Admin & Support Services			1								1		7		**9**
Agriculture, Forestry, Fishing and Hunting													1		**1**
Arts, Entertainment & Recreation			3			1				1	2		4		**11**
Child Day-Care Services			1								2		2		**5**
Collection Agencies			1							1			1		**3**
Construction			5								1		3		**9**
Credit Bureaus											2		1		**3**
Credit Unions										3	2		11		**16**
Dealers in Automobiles			2								2		2		**6**
Educational Services			2							3			7		**12**
Finance		1	4								7	1	27		**40**
Health Care & Social Assistance			15							5	9		20		**49**
Information & Cultural Industries			1										4		**5**
Insurance Industry			3							2	3		13		**21**
Investigative & Security Services			1							2			1		**4**
Legal Services			12								2		3		**17**
Management of Companies & Enterprises		1	1								1		1		**4**
Manufacturing			1								2		10		**13**
Medical & Diagnostic Laboratories										1	1				**2**
Mining, Oil and Gas			5								9		10		**24**
Motor Vehicle Parts & Accessories															**0**
Nursing Homes/Home Health Care													1		**1**
Private Health Care & Social Assistance															**0**
Professional, Scientific & Technical			7								2		22		**31**
Public Administration			1			1				2					**4**
Real Estate, Rental, Leasing			14							1	4		6		**25**
Retail			4							1	2		36		**43**
Trades/Contractors			1								1				**2**
Transportation			1								5		9		**15**
Utilities			2												**2**
Wholesale Trade			1										1		**2**
Other		3	19							8	6		8		**44**
Total	**0**	**5**	**108**	**0**	**0**	**2**	**0**	**0**	**0**	**0**	**30**	**66**	**1**	**219**	**431**

Note: The statistics do not include Intake cases.

APPENDIX C: ORDERS, DECISIONS AND PUBLIC INVESTIGATION REPORTS ISSUED

Statistics are from April 1, 2018 to March 31, 2019

FOIP Respondent	Orders	Decisions	Public Investigation Reports	Total
Agriculture and Forestry	2			2
Alberta Corporate Human Resources	1			1
Alberta Energy Regulator	1			1
Alberta Health Services	5			5
Alberta Human Rights Commission	1			1
Alberta Human Rights Commission and Justice and Solicitor General	1			1
Alberta Status of Women	1			1
Balancing Pool			1	1
Calgary Police Service	1			1
Children's Services	2			2
City of Calgary	4	1	1	6
City of Leduc	1			1
City of Lethbridge	1			1
Community and Social Services	3			3
Culture and Tourism	2			2
Edmonton Police Commission	1			1
Edmonton Police Service	7			7
Education	2			2
Energy	1			1
Environment and Parks	3			3
Executive Council	2			2
Government of Alberta*			2	2
Health	6	1		7
Justice and Solicitor General	8	2		10
Labour	3			3
Northern Alberta Institute of Technology	1			1
Parkland School Division No. 70	1			1
Peace River School Division No. 10	2			2
Seniors and Housing	2			2
Service Alberta	3			3
Town of Peace River	3			3
Treasury Board and Finance	1			1
University of Alberta	2			2

FOIP Respondent	Orders	Decisions	Public Investigation Reports	Total
University of Calgary	1			1
Workers' Compensation Board	4			4
Subtotal	79	4	4	87

HIA Respondent	Orders	Decisions	Public Investigation Reports	Total
Alberta Health Services	1		1	2
Subtotal	**1**	**0**	**1**	**2**

PIPA Respondent	Orders	Decisions	Public Investigation Reports	Total
Ninkovich Gravel Ltd. and Safety Documents	1			1
Primaris Management Inc.	2			2
Syncrude Canada Ltd	1			1
Ideal Housing Cooperative Ltd.	1			1
Canadian Energy Workers' Association	1			1
7-Eleven Canada, Inc.	1			1
Maxim Research and Consulting Corporation and Elise J. Lavinge Professional Corporation	1			1
Subtotal	8	0	0	8

Total	**88**	**4**	**5**	**97**

Total of number of Orders, Decisions, and Investigation Reports Issued:
FOIP Orders: 79 (91 cases)
FOIP Decisions: 4 (8 cases)
HIA Orders: 1 (1 case)
HIA Decisions: 0 (0 cases)
PIPA Orders: 8 (10 cases)
PIPA Decisions: 0 (0 cases)
FOIP Investigation Reports: 4 (26 cases)
HIA Investigation Reports: 1 (1 case)

*Refers to two investigation reports involving multiple Government of Alberta departments.

Investigation Report F2018-IR-01 involved Advanced Education, Agriculture and Forestry, Culture and Tourism, Economic Development and Trade, Education, Energy, Environment and Parks, Executive Council, Health, Human Services, Indigenous Relations, Infrastructure, Justice and Solicitor General, Labour, Municipal Affairs, Seniors and Housing, Service Alberta, Transportation, and Treasury Board and Finance.

Investigation Report F2019-IR-01 involved Education, Executive Council, Transportation and Service Alberta.

Notes:

This table contained all Orders and Decisions released by the OIPC whether or not the issuance of the Order or Decision conluded the matter.

The number of Orders, Decisions and Investigation Reports are counted by the number of Order, Decision or Investigation Report numbers assigned. A single Order, Decision or Investigation Report can relate to more than one entity and more than one file.

Orders and Decisions are recorded by the date the Order or Decision was signed, rather than the date the Order or Decision was publicly released.

Only those Investigation Reports that are publicly issued are reported in the annual report.

Copies of all Orders, Decisions and public Investigation Reports are available at www.oipc.ab.ca.

www.oipc.ab.ca