Office of the Information and
Privacy Commissioner of Alberta

ANNUAL REPORT
2019-20

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 2020

Office of the Information and
Privacy Commissioner of Alberta

November 2020

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, 2019 to March 31, 2020.

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

In reviewing my office's case statistics for 2019-2020, I was struck by one thing in particular: the sheer number of privacy impact assessments (PIAs) and self-reported breaches (SRBs) we received last year. These two case types made up over 75% of the 3,658 cases we opened.

I contrasted this statistic to two years ago, in 2017-18, when these case types represented just under half of the cases we opened in a year; more dramatically, in 2012-2013 – my first full year as Commissioner – these case types made up only 43% of our work.

A number of factors have contributed to this shift over the years. For one thing, around the world we have seen increasingly rigorous privacy laws enacted, such as the European Union's *General Data Protection Regulation* (GDPR) in 2018. GDPR made data privacy impact assessments (DPIAs) mandatory and breach reporting a new legal obligation in many jurisdictions. Public awareness has also increased, such that submitting PIAs or DPIAs and breach reports to regulators has become an expectation.

In my view, these are positive changes. I have said many times that our work reviewing PIAs is among the most important proactive work we do. Rather than respond to individual complaints that may arise after an information system has been implemented, we have an opportunity to provide advice and recommendations at the outset and during the development of a new system – and, hopefully, avoid individual complaints arising after the fact because risks have already been identified and mitigated.

Our PIA reviews also provide an important reassurance to the public. Many information systems are sophisticated and complex – and opaque. It would not be possible for individuals to have the time or knowledge to review and understand every information system that affects their life. Instead, privacy,

security and technical experts in my office can delve deep where necessary and ask the important questions, helping to ensure that new systems are compliant with Alberta's privacy laws.

Similarly, with respect to privacy breaches, the legal requirement to report certain incidents to my office helps to provide the public with some reassurance that organizations and health custodians are accountable for their management of personal and health information. The requirement for health custodians to notify affected individuals of certain breaches, and my ability to require private sector organizations to do the same, also empowers individuals by ensuring they have the information they need to take steps to protect themselves from such harms as identity theft and fraud. It is not really surprising that organizations and health custodians that are accountable up front, and open and transparent with affected individuals, seldom see formal complaints filed against them with my office.

As I see many jurisdictions around the world incorporating mandatory PIA or DPIA reviews and breach reporting into their privacy laws, I am proud of Alberta's record. We have had mandatory PIA requirements in Alberta's *Health Information Act* (HIA) since it came into force in 2001. Alberta's *Personal Information Protection Act* (PIPA) has included mandatory breach reporting requirements since 2010, and HIA since 2018.

Not surprisingly, reflecting on these legislative achievements also highlights the work we still need to do. PIAs are not mandatory in the public sector, and public bodies are not required to report breaches to my office or notify affected individuals. Some public bodies do so voluntarily, of course, but there is no real substitute for a legislated duty. My office has called for these and other amendments to Alberta's *Freedom of Information and Protection of Privacy Act* (FOIP Act) in the past, but the current reality is that these changes would only be a start towards bringing our public sector law up to the minimum standard we are now seeing around the world.

The truth is that all three of Alberta's access and privacy laws are due for modernization. The last substantive review of the FOIP Act by a Legislative Assembly committee was completed in 2010, and none of the reviewing Committee's recommendations were brought forward. The last PIPA review resulted in a single recommendation for amendment, and it has not been brought forward. HIA was amended in 2018 to include breach reporting and notification, but that was four years after the amendments had been passed and no other changes were made.

Information sharing, artificial intelligence, synthetic data, virtual healthcare and other apps, technical innovation, and global markets and information flows – these are just some of the forces changing personal and health information management, and they all have privacy implications. Alberta has been a leader in the past and there is an opportunity now to lead into the future.

I understand that governments are, rightly, preoccupied dealing with the COVID-19 pandemic. But the pandemic itself is another factor that weighs in favour of reviewing and modernizing our access and privacy laws. Modernization of Alberta's privacy laws will help to ensure that we have the right legislative framework to harness the potential of information through research and analytics, while protecting personal privacy. In addition, updating freedom of information legislation, with a focus on making information available proactively and improving response times, will help to engender public trust in accountable and transparent government. To this end, I plan to write to the Ministers responsible for Alberta's access and privacy laws in the coming weeks to ask that they turn their attention to these matters.

For now though, I would like to express my deep appreciation to my OIPC colleagues. We have had another record year, with 3,658 cases opened – an increase of 12% over the last fiscal year. At the same time, and more importantly, we closed 2,968 cases – an increase of 23% over the last year. I recognize that these two statistics, while meaningful, do not begin to capture the dedicated, quality work that you do. For your day to day efforts that go above and beyond, particularly during these challenging times, I thank you.

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 1,000 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 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.

The Act 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 (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.

The Act seeks to balance individuals' right 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

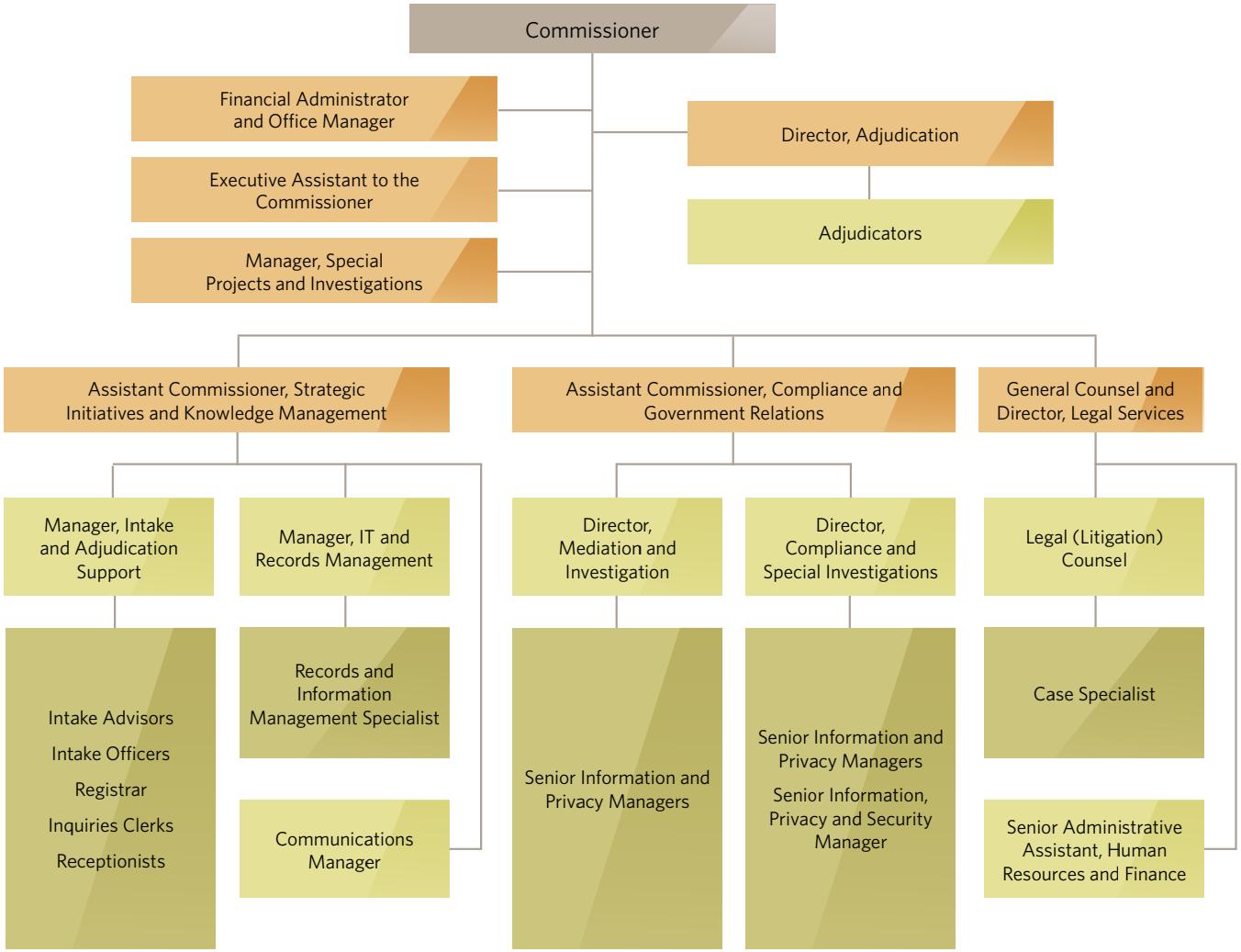
A society that values and respects access to information and personal privacy.

MISSION

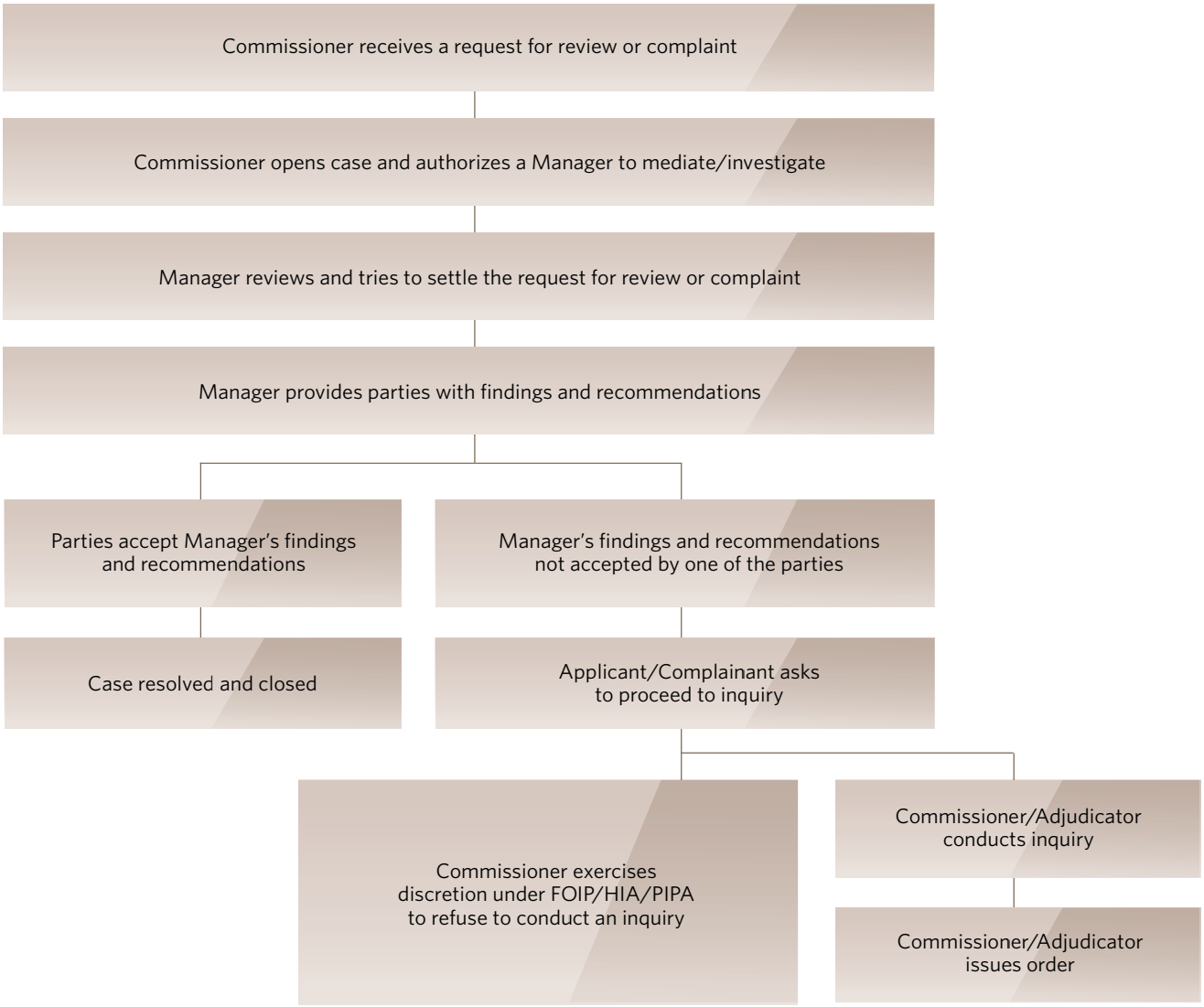
Our work toward supporting our vision includes:

- 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

Organizational Structure



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 2019-20, 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 appointed by order in council to determine whether the OIPC properly excluded records subject to an access request.

As of March 31, 2020, there were five outstanding requests for review awaiting the appointment of External Adjudicators.

OIPC PRIVACY MATTERS

In 2019-20, the OIPC conducted nine investigations into internal incidents involving potential privacy breaches.

Incident 1

An unmarked envelope was received by the Government of Alberta (GoA) mail room. The GoA mail room opened the envelope, which contained two OIPC files.

The incident involved personal information, but posed minimal risk that it could be used to cause harm. The risk was further mitigated by the fact that the files were received by GoA staff entrusted to manage and direct mail, and the mail was opened only to identify to whom it should be directed. There was no real risk of significant harm and notification was not necessary.

Incident 2

An email about a recently issued OIPC order was sent to OIPC staff. However, the email was also sent inadvertently to an individual who had a matter before the OIPC.

The email was addressed to certain named staff and revealed only their business email addresses. There was no real risk of significant harm and notification was not necessary.

Incident 3

The OIPC was notified by an individual that the OIPC mailed correspondence to her former address, despite her notifying the OIPC of an address change. The OIPC confirmed that while the correspondence was sent to the former address, it was sent a month prior to receiving the request to change the address.

The correspondence contained personal information about the individual and her children. Despite not receiving the request to change the address in time to prevent the incident, an apology was extended and notification was provided to the affected individual.

Incident 4

The OIPC mistakenly sent an acknowledgment package to the wrong public body. The OIPC found that the mailing envelope was either incorrectly labelled or correspondence was inadvertently put into an envelope that was correctly labelled for another public body.

The correspondence contained personal information about an individual and their access request, as well as information about nine other individuals named in the related records. The correspondence was received by a FOIP Office for a public body. The FOIP Office regularly deals with personal information under the FOIP Act and understands the need to keep personal information confidential. The FOIP Office returned the documents to the OIPC. There was no real risk of significant harm to the affected individuals and notification was not necessary.

Incident 5

The OIPC received a complaint about an organization. The OIPC sent an acknowledgment letter to the complainant and the organization. The letter included a copy of the complaint, which contained the complainant's personal information as well as the personal information of an individual the complaint was about. The Privacy Advisor for the organization informed the OIPC that the organization had not received a copy of the complaint, and could not find the letter.

The OIPC found that the organization had a corporate address and a clinic address. In its system, the OIPC had the clinic address and sent the letter to that location. However, prior to sending the letter, the OIPC had received a notice from the organization about a change in contact or address. The address to the organization's corporate address had changed. The OIPC had not yet entered the changed address into its system when the letter was sent.

The OIPC notified the complainant about the loss of their personal information. The OIPC also notified the individual the complaint was about.

Incident 6

The OIPC improperly sent two emails to a public body's employee whose last name was identical to another staff member of the public body, and who had a nearly identical email address. A staff member used the auto-complete function for populating names in the two emails.

The content of the emails contained personal information about an individual and information about two files that she had before the OIPC, including a letter of finding for one of the files. The letter of finding was encrypted, and the recipient would have had to call an OIPC staff member to obtain the password. The individual who received the emails in error forwarded them to the intended recipient, deleted the emails from her working records and confirmed that she had done so. There is no evidence that she obtained the password and viewed the contents of the letter of finding.

The emails contained minimal personal information. The emails also remained within the public body. There was no real risk of significant harm and notification was not necessary.

Incident 7

The OIPC inadvertently sent a complaint acknowledgement package to an organization, when the correct respondent was the organization's Edmonton chapter. The organization alerted the OIPC to the error and shredded the documents that it had received.

The package included personal information, including details of the matter brought before the OIPC. Considering another organization, with the same role and function as the correct respondent, received the package, notified the OIPC of the error and shredded the documents, there was no real risk of significant harm and notification was not necessary.

Incident 8

Records related to a review of an access request response were prepared at the OIPC's Calgary office for courier delivery to a public body in Edmonton. The public body advised the OIPC that the records were not received.

The lost records involved personal information about an applicant and approximately two dozen other individuals.

The OIPC assessed that the personal information in the records could be used to cause embarrassment and possibly damage to personal or professional relationships. The incident presented a real risk of significant harm and all affected individuals were notified.

Incident 9

The OIPC mailed request for review correspondence to the wrong public body.

The recipient alerted the OIPC, and the documents were retrieved. There was no real risk of significant harm, and notification was not necessary. However, the applicant was nevertheless told about the error and received an apology.

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 2018 calendar year, the threshold was adjusted to $129,809. 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 2019-20.

Financial Overview

For the 2019-20 fiscal year, the total approved budget for the OIPC was $7,577,671. The total cost of operating expenses and capital purchases was $6,835,179. The OIPC returned $742,492 (9.80% of the total approved budget) to the Legislative Assembly.[1]

TOTAL ACTUAL COSTS COMPARED TO BUDGET

	VOTED BUDGET	ACTUAL	DIFFERENCE
Operating Expenses*	$ 7,577,671	$ 6,779,170	$ 798,501
Capital Purchases	-	56,009	(56,009)
Total	$ 7,577,671	$ 6,835,179	$ 742,492

*Amortization is not included

Salaries, wages, and employee benefits make up approximately 85% of the OIPC's operating expenses budget. In 2019-20, payroll related costs, legal fees and technology services were under budget. Contract services, supplies and services, and capital purchases were over budget.

TOTAL ACTUAL COSTS COMPARED TO PRIOR YEAR

	2019-2020	2018-2019	DIFFERENCE
Operating Expenses	$ 6,779,170	$ 6,823,711	$ (44,541)
Capital Purchases	56,009	-	56,009
Total	$ 6,835,179	$ 6,823,711	$ 11,468

Total costs for operating capital and equipment purchases, increased by $11,468 from the prior year.

[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 to November 30, 2019) was being held to the 2018-19 budget forecast, not the voted budget of the Standing Committee on Legislative Offices.

TRENDS & ISSUES

COVID-19 Pandemic

As 2019-20 came to a close, the global COVID-19 pandemic was declared, and employers in all sectors began to navigate the myriad of issues involved in collecting, using and disclosing personal information to protect employee privacy and uphold workplace safety.

Within days, the OIPC updated its "Privacy in a Pandemic" guidance, which quickly became one of the most viewed documents on the OIPC's website – ever.[2] The advisory opened with the statement that:

> Privacy laws are not a barrier to appropriate information sharing in a pandemic or emergency situation.
>
> It is important that public bodies, health custodians and private sector organizations know how personal or health information may be shared during a pandemic or emergency situation.

The advisory drew attention to Alberta's three privacy laws, and the relevant provisions in each, that apply to the collection, use and disclosure of personal or health information in emergency situations, such as the sections that permit disclosure to avert or minimize an imminent danger to the health or safety of any person.

The advisory also noted that, "In the event that a public health or general emergency is declared, orders issued under public health legislation could require the collection, use and disclosure of certain personal information relating to employees and customers." It noted that employers "should communicate to your employees the specific legislative authority that is engaged to do so" if a public health order places collection, use or disclosure requirements upon the public body, custodian or organization.

VIRTUAL HEALTHCARE

In response to the pandemic, many healthcare providers were forced to close their physical locations and adapt to providing care virtually, engaging the requirement under HIA to prepare a privacy impact assessment (PIA) for submission to and review by the OIPC (section 64). The OIPC published a statement to provide guidance to custodians completing PIAs. The notice, called "PIAs During a Public Health Emergency", said:[3]

> The OIPC understands that there is some confusion about whether the Commissioner can relax the requirements for submitting a PIA during a public health emergency. To be clear, the Commissioner has no authority under HIA to disregard a health custodian's section 64 obligations during a public health emergency, even if the new administrative practice or information system is a measure to combat the pandemic.

[2] Office of the Information and Privacy Commissioner of Alberta, "Privacy in a Pandemic", March 2020. Retrieved from https://www.oipc.ab.ca/resources/privacy-in-a-pandemic-advisory.aspx.

[3] Office of the Information and Privacy Commissioner of Alberta, "Notice: PIAs During a Public Health Emergency", March 19, 2020. Retrieved from https://www.oipc.ab.ca/news-and-events/news-releases/2020/notice-pias-during-a-public-health-emergency.aspx.

The OIPC has noted that privacy laws do not impede the work of public health officials during a public health emergency. What constitutes "reasonable safeguards" during a public health emergency may be different from normal circumstances.

During these unprecedented times, if a health custodian is considering new administrative practices or information systems with implications for individuals' privacy to combat the pandemic, the OIPC is asking that health custodians, at the very least, notify the Commissioner about the new administrative practice or information system. Notification of a new administrative practice or information system can be submitted to the OIPC via email.

When notifying the Commissioner, please describe what the new program is meant to achieve and any safeguards for health information.

After the notice was issued on March 19, 2020, the OIPC received more than 100 PIAs on virtual healthcare systems by March 31, 2020.

The OIPC also worked with healthcare professional associations to assist in updating the guidance those organizations were providing to their members about virtual care practices and the obligation to prepare a PIA.

TIME EXTENSION REQUESTS

With respect to access to information, the OIPC updated its guidance for requesting time extensions, noting that "[a] public body does not have authority to grant itself a 30-day extension under section 14(1) if unable to access or process records due to a disaster or pandemic. Furthermore, the Commissioner has no ability to grant an extension in such circumstances."[4]

This issue had previously arisen in the context of floods, building fires and wildfires, and the Commissioner recommended in 2013 that the legislative gap be fixed under section 14(1) by amending it "to allow for extensions in unforeseen emergency or disaster situations."[5]

[4] Office of the Information and Privacy Commissioner of Alberta, "Notice: Requests for Time Extensions During an Emergency", March 16, 2020. Retrieved from https://www.oipc.ab.ca/news-and-events/news-releases/2020/notice-requests-for-time-extensions-during-an-emergency.aspx.

[5] Office of the Information and Privacy Commissioner of Alberta, "Making the FOIP Act Clear, User-Friendly & Practical: Submission to the 2013 Government of Alberta FOIP Act Review", July/August, 2013. Retrieved from https://www.oipc.ab.ca/news-and-events/news-releases/2013/becoming-a-leader-in-access-and-privacy.aspx.

Facial Recognition Technology

It has been more than 15 years since the OIPC reviewed its first privacy impact assessment (PIA) related to the use of facial recognition technology.[6] Over the years, however, the technology has been refined and the scope of its use has expanded, attracting many headlines in 2019-20.

Much of the attention was directed at Clearview AI, a facial recognition company. After a feature article in the New York Times delved into the company's tactics, the widespread use of Clearview AI by law enforcement agencies and many private sector businesses drew headlines globally.[7] The coverage only intensified after it came to light that Clearview AI's client list had been hacked, exposing the use of Clearview AI by many Canadian police services, including some that had previously denied using the product.[8,9] The OIPC opened investigations into Clearview AI and the use of Clearview AI by public bodies in 2019-20.

Clearview AI was not the only facial recognition story that captured people's attention. For example:

- The City of San Francisco in May 2019 approved a ban on police and other public agencies using facial recognition technology.[10]
- The Chief of the Toronto Police Service reported to the Toronto Police Services Board that the service was using facial recognition technology "to compare images of potential suspects captured on public or private cameras to its internal database of approximately 1.5 million mugshots".[11]
- The United Kingdom's Information Commissioner opened an investigation in August 2019 into "the use of live facial recognition technology in King's Cross, London" and warned that "any organizations wanting to use facial recognition technology must comply with the law... They must have documented how and why they believe their use of the technology is legal, proportionate and justified."[12]

[6] Office of the Information and Privacy Commissioner of Alberta, "Commissioner Accepts Facial Recognition Software Privacy Impact Assessment", May 14, 2004. Retrieved from https://www.oipc.ab.ca/news-and-events/news-releases/2004/commissioner-accepts-facial-recognition-software-privacy-impact-assessment.aspx.

[7] Hill, Kashmir, "The Secretive Company That Might End Privacy as We Know It", New York Times, January, 18, 2020. Retrieved from https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[8] Smith, Alanna, "Two Calgary officers tested Clearview AI facial-recognition software", Calgary Herald, February 29, 2020. Retrieved from https://calgaryherald.com/news/local-news/two-calgary-officers-tested-clearview-ai-facial-recognition-software/.

[9] Mac, Ryan, Haskins, Caroline & McDonald, Logan, " Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA", BuzzFeed News, February 27, 2020. Retrieved from https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

[10] CBS News, "San Francisco bans facial recognition technology", May 15, 2019. Retrieved from https://www.cbsnews.com/news/san-francisco-becomes-first-us-city-to-ban-facial-recognition-technology-today-2019-05-14/.

[11] Allen, Kate & Gillis, Wendy, "Toronto police have been using facial recognition technology for more than a year", The Star, May 28, 2019. Retrieved from https://www.thestar.com/news/gta/2019/05/28/toronto-police-chief-releases-report-on-use-of-facial-recognition-technology.html.

[12] Information Commissioner's Office (UK), "Statement: Live facial recognition technology in King's Cross", August 15, 2019. Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/.

- The federal Standing Committee on Access to Information, Privacy and Ethics (ETHI Committee) agreed in February 2020 to "study the use or possible use of facial recognition technology by various levels of government in Canada, law enforcement agencies, private corporations and individuals", including "that the committee examine the impacts of facial recognition technology and the growing power of artificial intelligence".[13]

The use of new technologies by law enforcement agencies often garners public interest. Police agencies generally have broad authority to collect, use and disclose personal information for law enforcement purposes under privacy laws. There remain several questions, however, about the implementation of these technologies to ensure privacy and security risks are identified and mitigated. Some of the questions include:

- Why is the use of these new technologies required? How will it improve public safety?
- Does this represent a new collection of personal information?
- Will personal information already collected be used for a new purpose? If so, is the new use authorized?
- Will information be shared with other agencies and government and, if so, how is this sharing performed and authorized?
- What information will be collected and for how long will it be retained?
- What steps are taken to safeguard personal information?
- How is security managed in contractual arrangements?
- How are employees trained on the use of the new technology? What positions have access to what personal information?
- What is the process for responding to requests for access to personal information?

The OIPC strongly encourages law enforcement and other agencies contemplating the use of new technologies, such as facial recognition, to complete a privacy impact assessment, and submit it to the OIPC for review to allow for an independent review of the privacy and security protections in place.

[13] ETHI Committee, "Minutes of Proceedings", February 24, 2020. Retrieved from https://www.ourcommons.ca/DocumentViewer/en/43-1/ETHI/meeting-2/minutes.

Connect Care

In November 2019, Alberta Health Services (AHS) submitted dozens of PIAs to the OIPC for its implementation of the Connect Care Clinical Information System (Connect Care), where "healthcare providers collect, store, access and analyze patient and healthcare information."[14] AHS launched the first wave of Connect Care in November 2019.

AHS said it anticipates Connect Care to be completed by the end of 2022, and that it "will be used to document 80% of the health services provided by AHS, Covenant Health, Alberta Precision Laboratories and affiliated organizations where AHS holds the legal record of care across the province."

The Connect Care PIA identifies three primary purposes:

- "Improve patient safety, health services delivery, and health outcomes."
- "Reduce unhelpful and inadvertent clinical and operational variance."
- "Improve health system sustainability by focusing information technology investment in a single [clinical information system]."

AHS and Covenant Health employees, physicians, students, Alberta Precision Laboratories and other stakeholders will connect with various facilities, such as those for acute, cancer and community-based care, and addiction and mental health.

Connect Care implementation also includes the MyAHS Connect patient portal and the Connect Care Provider Portal, which is meant to allow healthcare providers who work outside of AHS to access some health information in Connect Care and to allow for referrals to AHS programs and clinics.

AHS said it currently operates approximately 1,300 information systems to support patient care and fulfill operational responsibilities, but that many of these systems duplicate care services, while others are near their end of life technologically. AHS said it planned to decommission approximately 500 legacy information systems by the end of 2022, as a result of Connect Care.

The OIPC initially received nearly 50 PIAs for wave one implementation of Connect Care. In addition to PIAs on Connect Care itself and an update to its organizational management PIA, AHS is also required to provide PIAs on each of the legacy systems it plans to interface with Connect Care. In total, more than 100 PIAs are expected from AHS over the course of the project.

During the OIPC's reviews, a number of privacy and security concerns have been identified and communicated to AHS. As of March 31, 2020, PIAs related to Connect Care, including AHS' updated organizational privacy management PIA, were not accepted.

[14] Alberta Health Services, "Connect Care", June 28, 2017. Retrieved from https://youtu.be/UD0uBj2-zuE.

BY THE NUMBERS

Totals Opened/Closed
(excluding Intake cases)

12% | 23%

INCREASE IN OPENED/CLOSED TOTAL CASES

3,658 total opened files in 2019-20; 3,273 in 2018-19

2,968 total closed files in 2019-20; 2,405 in 2018-19

Privacy Impact Assessments (PIAs)

33% | 57%

INCREASE IN OPENED/CLOSED PIAs

1,454 opened PIAs in 2019-20; 1,090 in 2018-19

1,071 closed PIAs in 2019-20; 681 in 2018-19

Self-Reported Breaches (SRBs)

26% | 61%

INCREASE IN OPENED/CLOSED SRBS

1,344 opened SRBs in 2019-20; 1,070 in 2018-19

1,030 closed SRBs in 2019-20; 638 in 2018-19

Totals Opened/ Closed under HIA
(excluding Intake cases)

35% | 62%

INCREASE IN OPENED/ CLOSED HIA CASE TOTALS

2,510 opened HIA files in 2019-20; 1,865 in 2018-19

1,851 closed HIA files in 2019-20; 1,145 in 2018-19

Totals Opened/ Closed under FOIP
(excluding Intake cases)

19% | 13%

DECREASE IN OPENED/ CLOSED FOIP CASE TOTALS

735 opened FOIP files in 2019-20; 903 in 2018-19

723 closed FOIP files in 2019-20; 829 in 2018-19

Totals Opened/ Closed under PIPA
(excluding Intake cases)

18% | 9%

DECREASE IN OPENED/ CLOSED PIPA CASE TOTALS

413 opened PIPA files in 2019-20; 505 in 2018-19

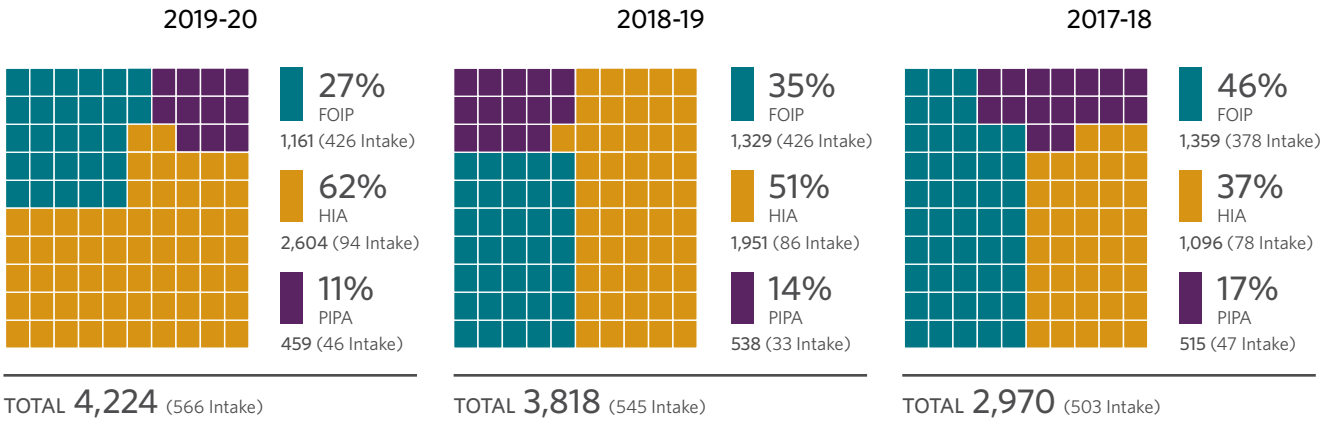
394 closed PIPA files in 2019-20; 431 in 2018-19

231

TIME EXTENSION REQUESTS UNDER FOIP 18

GRAPH A: TOTAL CASES OPENED

Three Year Comparison



GRAPH B: TOTAL CASES CLOSED

Three Year Comparison

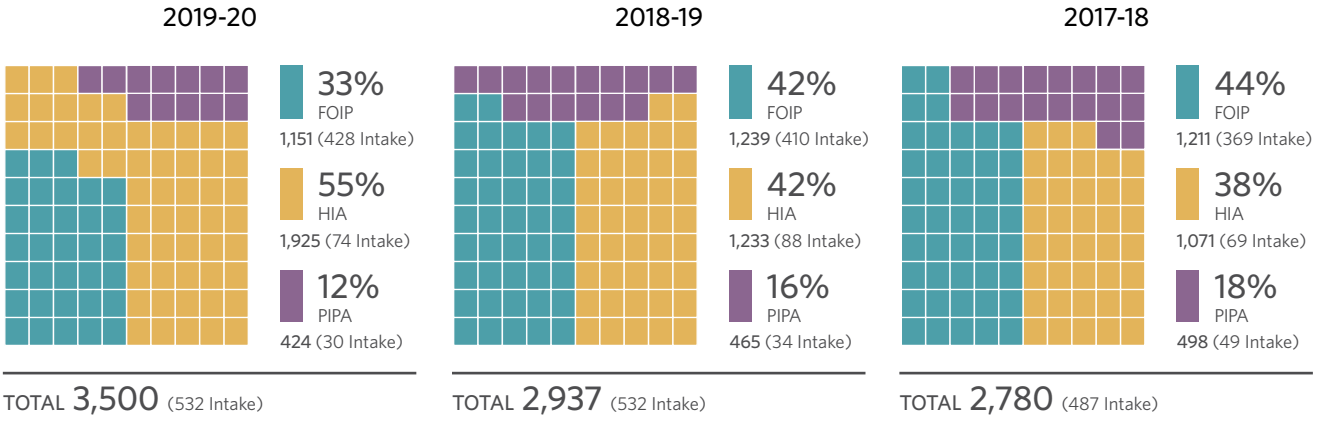


TABLE 1: CASES OPENED BY CASE TYPE

FOIP	2019-2020	2018-2019	2017-2018
Advice and Direction	1	1	1
Authorization to Disregard a Request	7	9	21
Complaint	45	91	96
Disclosure to Commissioner (Whistleblower)	0	0	0
Engage in or Commission a Study	0	0	1
Excuse Fee	7	16	9
Investigation Generated by Commissioner	9	8	10
Notification to OIPC	29	7	3
Offence Investigation	0	3	3
Privacy Impact Assessment	23	23	18
Request Authorization to Collect Indirectly	0	0	0
Request for Information	14	23	22
Request for Review	251	358	454
Request for Review 3rd Party	23	32	65
Request Time Extension	231	226	228
Self-reported Breach	95	106	50
Subtotal	**735**	**903**	**981**
Intake cases	426	426	378
Total	**1,161**	**1,329**	**1,359**

HIA	2019-2020	2018-2019	2017-2018
Advice and Direction	0	0	0
Authorization to Disregard a Request	0	3	0
Complaint	64	43	56
Engage in or Commission a Study	0	0	0
Excuse Fee	0	1	0
Investigation Generated by Commissioner	7	11	1
Notification to OIPC	0	0	0
Offence Investigation	18	11	3
Privacy Impact Assessment	1,428	1,059	771
Request for Information	38	39	23
Request for Review	17	24	31
Request Time Extension	0	0	0
Self-reported Breach	938	674	133
Subtotal	**2,510**	**1,865**	**1,018**
Intake cases	94	86	78
Total	**2,604**	**1,951**	**1,096**

PIPA	2019-2020	2018-2019	2017-2018
Advice and Direction	0	1	0
Authorization to Disregard a Request	1	3	5
Complaint	52	112	119
Engage in or Commission a Study	0	0	0
Excuse Fee	0	0	0
Investigation Generated by Commissioner	8	7	6
Notification to OIPC	0	0	0
Offence Investigation	0	0	0
Privacy Impact Assessment	3	8	3
Request for Advanced Ruling	1	1	1
Request for Information	11	31	16
Request for Review	25	51	87
Request Time Extension	1	1	0
Self-reported Breach	311	290	231
Subtotal	**413**	**505**	**468**
Intake cases	46	33	47
Total	**459**	**538**	**515**

Notes

(1) See Appendix A for a complete listing of cases opened in 2019-20.

(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	2019-2020	2018-2019	2017-2018
Advice and Direction	1	0	1
Authorization to Disregard a Request	3	6	7
Complaint	61	82	83
Disclosure to Commissioner (Whistleblower)	0	0	1
Engage in or Commission a Study	0	0	1
Excuse Fee	8	14	8
Investigation Generated by Commissioner	2	31	19
Notification to OIPC	29	7	3
Offence Investigation	2	0	0
Privacy Impact Assessment	15	12	17
Request Authorization to Collect Indirectly	0	0	0
Request for Information	10	24	18
Request for Review	239	316	372
Request for Review 3rd Party	47	23	37
Request Time Extension	222	231	225
Self-reported Breach	84	83	50
Subtotal	**723**	**829**	**842**
Intake cases	428	410	369
Total	**1,151**	**1,239**	**1,211**

HIA	2019-2020	2018-2019	2017-2018
Advice and Direction	0	0	0
Authorization to Disregard a Request	1	0	0
Complaint	31	81	58
Engage in or Commission a Study	0	0	0
Excuse Fee	1	0	1
Investigation Generated by Commissioner	5	5	16
Notification to OIPC	0	0	0
Offence Investigation	9	6	4
Privacy Impact Assessment	1,050	669	707
Request for Information	44	30	26
Request for Review	15	18	48
Request Time Extension	0	0	0
Self-reported Breach	695	336	142
Subtotal	**1,851**	**1,145**	**1,002**
Intake cases	74	88	69
Total	**1,925**	**1,233**	**1,071**

PIPA	2019-2020	2018-2019	2017-2018
Advice and Direction	1	0	0
Authorization to Disregard a Request	0	5	2
Complaint	83	108	126
Engage in or Commission a Study	0	0	0
Excuse Fee	0	0	0
Investigation Generated by Commissioner	2	2	3
Notification to OIPC	0	0	0
Offence Investigation	0	0	2
Privacy Impact Assessment	6	0	4
Request for Advanced Ruling	1	0	1
Request for Information	14	30	15
Request for Review	35	66	54
Request Time Extension	1	1	0
Self-reported Breach	251	219	242
Subtotal	**394**	**431**	**449**
Intake cases	30	34	49
Total	**424**	**465**	**498**

Notes

(1) See Appendix B for a complete listing of cases closed in 2019-20.

(2) A listing of all privacy impact assessments accepted in 2019-20 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: 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 for 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	%
Mediation/Investigation	262	38	93	393	75%
Order or Decision	32	6	12	50	10%
Commissioner's decision to refuse to conduct an Inquiry	9	2	4	15	3%
Withdrawn during Inquiry process	22	0	4	26	5%
Discontinued during Inquiry process	31	0	5	36	7%
Total	356	46	118	520	100%

FOIP Orders: 32 (32 cases); **HIA Orders:** 6 (6 Cases); **PIPA Orders:** 9 (12 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 2019-20. 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

75% Mediation/ Investigation

10% Order/Decision issued

3% Commissioner's decision to refuse to conduct an Inquiry

5% Withdrawn during Inquiry process

7% Discontinued during Inquiry process

Of the **520** cases that could proceed to Inquiry:
2% were resolved within 90 days
5% were resolved within 180 days
93% were resolved in more than 180 days

TABLE 4: GENERAL ENQUIRIES

TELEPHONE CALLS		
FOIP	Number	Percentage
Public Bodies	75	16%
Individuals	387	84%
Total	462	100%

HIA	Number	Percentage
Custodians	324	32%
Individuals	676	68%
Total	1,000	100%

PIPA	Number	Percentage
Organizations	158	22%
Individuals	576	78%
Total	734	100%

NON-JURISDICTIONAL	265
EMAILS FOIP/HIA/PIPA	169
Total	2,630

REGULATION & ENFORCEMENT

Privacy Breaches

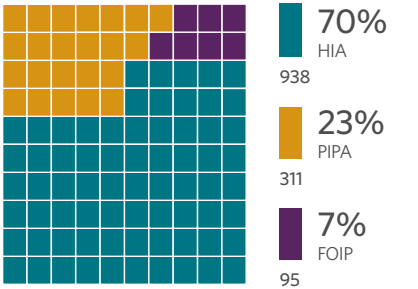
The OIPC received 1,344 reports of privacy breaches in 2019-20 under all three laws, representing a 26% increase over 2018-19 (1,070).

There are obligations under HIA and PIPA for health custodians and private sector organizations to report certain privacy breaches to the OIPC, and 2019-20 marked the first full year in which mandatory breach reporting was in effect for both laws. Public bodies also voluntarily report breaches on occasion.

The OIPC closed 1,030 self-reported breach files in 2019-20 under all three laws, representing a 61% increase over 2018-19 (638).

To manage the recent influx of breaches reported to the office, certain breaches are prioritized for review, including files where affected individuals have not yet been notified or when a potential offence is suspected.

BREACH REPORTS OPENED



70% HIA
938

23% PIPA
311

7% FOIP
95

TOTAL 1,344

PIPA

There were 311 breaches reported in 2019-20, a 7% increase over 2018-19 (290).

The Commissioner issued 251 breach decisions in 2019-20, representing a 14% increase over 2018-19 (220).
The following determinations were made in 2019-20:

- 203 (81%) were found to have a real risk of significant harm
- 39 (15%) were found to have no real risk of significant harm
- 9 (4%) where PIPA did not apply (i.e. no jurisdiction)

Of the 203 breaches in which the Commissioner determined there was a real risk of significant harm to an individual:

- More than 100 incidents were caused by electronic systemic compromise, such as hacking, phishing, malware, system vulnerabilities, or a combination of factors.
- More than 35 incidents involved human error, such as transmission errors by email, mail or fax, or during IT system upgrades or settings changes.
- More than 20 incidents of theft, which remains a common cause of breaches.

Other causes of breaches include rogue employees, social engineering and loss (e.g. couriered packages go missing).

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). Section 37.1 of PIPA provides authority for the Commissioner to require an organization to notify individuals of a loss or unauthorized access or disclosure of personal information.

Social Engineering Affects Credit Union

The importance of strong authentication practices was underscored in several breach decisions where a real risk of significant harm to an individual was found.

In four incidents, an unauthorized individual was able to access client accounts after a call agent for the organization did not follow policy when confirming the identity of the caller.

In the other incidents, the caller successfully answered authentication questions, leading to unauthorized access to client accounts.

In each of the six incidents, up to three people were affected and the breaches involved a combination of name, account information, transaction history and patterns, bill payees and associated account numbers for the payees, and e-transfer details.

P2019-ND-050, Servus Credit Union Ltd.
P2019-ND-066, Servus Credit Union Ltd.
P2019-ND-067, Servus Credit Union Ltd.
P2019-ND-174, Servus Credit Union Ltd.
P2019-ND-186, Servus Credit Union Ltd.
P2020-ND-009, Servus Credit Union Ltd.

Misconfigured Settings

As more organizations move their operations to cloud services, or provide clients with portals through which to access personal information, there is an increased risk of breaches when settings are misconfigured. These breaches are generally the result of human error, and emphasize the need for diligence in reviewing and confirming server or website properties. Some of these breaches are commonly referred to as "web bucket" breaches.

In three incidents, misconfigured settings allowed employees or clients to be able to access information of other employees or clients.

In eight incidents, misconfigured settings allowed personal information to be accessible publicly – either through search engines or on websites.

Each of the incidents affected between one and 13,000 individuals, and involved personal information such as names, insurance claims history, banking details, beneficiary information, date of birth, addresses, email addresses, telephone numbers, passwords, passport information, driver's licences, among other types of personal information.

P2019-ND-055, Westlake Chemical Corporation
P2019-ND-056, Sun Life Assurance Company of Canada
P2019-ND-076, Prudent Benefits Administration Services Inc.
P2019-ND-077, The Canadian Kennel Club
P2019-ND-080, The Japan Foundation - Toronto
P2019-ND-087, Bayer Inc. / Bayer AG
P2019-ND-088, TeenSafe
P2019-ND-093, Entrust Disability Services, as reported by Box Clever
P2019-ND-159, RWH Travel Limited
P2019-ND-179, Discovery Communications, LLC
P2020-ND-022, Koff Productions

Stolen Credentials

A relatively common type of breach that was summarized in the 2018-19 Annual Report continued in 2019-20. There were six incidents where customer credentials were acquired illicitly in other incidents, and those credentials were used to gain access to another website or online service. These incidents are called "credential stuffing attacks", and they serve as a reminder for individuals to use different username and password combinations on each of the websites or online services for which they have an account.

In each of these six incidents, the organization was unable to identify a security vulnerability through which there was unauthorized access to client accounts. The breaches affected between three and 6,500 individuals.

P2019-ND-166, Canadian Tire Corporation
P2019-ND-167, eHarmony, Inc.
P2019-ND-208, Mountain Equipment Coop
P2020-ND-020, Skip The Dishes Restaurant Services Inc.
P2020-ND-027, News America Marketing Digital LLC
P2020-ND-034, Skip The Dishes Restaurant Services Inc.

Rogue Employees

Among the most difficult type of incident to prevent, rogue employees were responsible for 12 breaches where the Commissioner determined there was a real risk of significant harm to an affected individual.

The risk of harm in these types of incidents is typically elevated, as many cases appear to involve malicious intent. In each of these types of cases, employees have authorized access to personal information for their job responsibilities, but use the information for unauthorized purposes.

In at least four incidents, for example, personal information was stolen, or otherwise accessed, for financial gain. In other incidents, employees may have not acted maliciously but otherwise transferred personal information without authorization (e.g. from work to personal accounts or mobile devices).

P2019-ND-058, Canon Medical Systems Canada Limited
P2019-ND-078, McKenzie Lake Community Association
P2019-ND-083, Calgary French & International School
P2019-ND-117, Kahane Law Office
P2019-ND-129, Solara Condominium Corporation
P2019-ND-136, TGS Canada Corp.
P2019-ND-137, TransCanada Credit Union Ltd.
P2019-ND-140, The Children's Cottage Society of Calgary
P2019-ND-187, Microsoft Corporation
P2019-ND-203, Zedi Canada Inc.
P2019-ND-204, McNeill, Lalonde & Associates
P2020-ND-035, Chamberlain Group, Inc.

HIA

The 2019-20 fiscal year marked the first full year of mandatory breach reporting under HIA. There were 938 breaches reported by custodians to the OIPC, representing a 39% increase over 2018-19 (674).

It is mandatory for a custodian having individually identifying health information in its custody or control to notify the Commissioner of a privacy breach if the custodian determines "there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure" (section 60.1(2)). In addition to notifying the Commissioner of the privacy breach, the custodian is also required by section 60.1(3) of HIA to notify the Minister of Health and the individuals affected by the privacy breach.

The number of "snooping" incidents reported to the OIPC has increased with mandatory breach reporting requirements. Several incidents occurred when someone who is authorized to access health information does so without a legitimate business reason to do so.

Misdirected correspondence continues to be a common cause of breaches, through fax or email. A common issue with fax machines is using outdated address books or typing an incorrect fax number. Many misdirected emails are caused by entering the wrong email address using auto-complete features in email programs.

Other incidents involving unauthorized disclosure of health information include:

- When healthcare providers discuss health information with other providers not involved in a patient's care
- There is a lack of security controls leaving health information exposed online
- Health information is shared on social media

The OIPC has also seen breaches where ransomware affected information systems containing health information.

Social engineering incidents were also reported where an individual would impersonate a pharmacist, call a number of pharmacies and request information about patients. In February 2020, the Alberta College of Pharmacy issued a notice about this scam to its members.

FOIP

The FOIP Act remains the only Alberta privacy law that does not require regulated entities to report certain privacy breaches to the Commissioner and notify affected individuals. Despite this, the OIPC continues to receive breach reports voluntarily from public bodies. There were 95 breaches received from public bodies, representing a 10% decrease over 2018-19 (106).

The most common type of breach reported by public bodies to the OIPC is misdirected emails, primarily those where the wrong recipient was added using auto-complete features in email programs. Another common type of incident is theft, such as when a briefcase containing personal information is stolen from a car.

Other incidents include unauthorized access to employees' personal information by colleagues, a successful phishing attack that led to unauthorized disclosure of personal information, and a breach of third party service providers who had custody of personal information that was accessed without authorization.

Offence Investigations under HIA

There were four convictions for unauthorized access to health information in 2019-20. All four stemmed from breaches that occurred prior to August 31, 2018, when mandatory breach reporting provisions under HIA came into force. This means that OIPC offence investigations that led to the convictions were either opened as a result of a breach reported voluntarily by a health custodian or from a complaint submitted by an individual about unauthorized access to health information.

Upon conclusion of an offence investigation, the OIPC refers its findings to the Specialized Prosecutions Branch of Alberta Justice.

The convictions included:

- A former billing clerk with Alberta Health Services (AHS) who pled guilty in August 2019 to illegally accessing the health information of 52 Albertans. AHS voluntarily reported the breaches, which occurred in Red Deer, to the OIPC in June 2018. AHS initiated an audit after allegations were made that the billing clerk had accessed health information without authorization. The former billing clerk was fined $5,000 and ordered not to access health information for one year.
- A medical office assistant pled guilty in September 2019 to knowingly accessing the health information of two Albertans. The affected individuals requested access to their audit logs in Alberta Netcare, the provincial electronic health record, and discovered the unauthorized accesses. The medical office assistant, who worked at the Terwillegar Family Clinic in Edmonton, made suspicious statements to the individuals about personal medical details, which led them to request access to their audit logs. The individuals submitted complaints to the OIPC, and offence investigations were subsequently opened. The medical office assistant was fined $3,500, and issued a victim fine surcharge of $525.
- A former billing clerk with AHS pled guilty in September 2019 to accessing the health information of 81 individuals on 471 occasions in contravention of HIA. AHS reported the breaches to the OIPC in May 2018. The breaches occurred at the Michener Centre in Red Deer. The former billing clerk was fined $8,000 and sentenced to one year of probation with conditions, including attending treatment and counselling as directed and to not be employed in a position that permits access to health information for one year.
- A former Covenant Health employee pled guilty in January 2020 to accessing the health information of 16 individuals on 465 occasions without authorization. The accesses occurred at the Misericordia Community Hospital in Edmonton, where the individual had been employed as a secretary. Covenant Health reported the breaches to the OIPC in November 2017. The former secretary received a $3,000 fine and was sentenced to one year of probation, including no access to health information.

The four convictions in 2019-20 brought the total number of convictions under HIA to 14. It is an offence to knowingly gain or attempt to gain access to health information in contravention of HIA (section 107(2)(b)).

As noted in the Commissioner's Message in the 2018-19 Annual Report, the OIPC went from having five to six active offence investigations open at any one time to more than 20 active cases in 2019-20, with dozens more flagged as potential offences. In total, 18 additional offence investigations under HIA were opened in 2019-20, representing a 64% increase over 2018-19 (11).

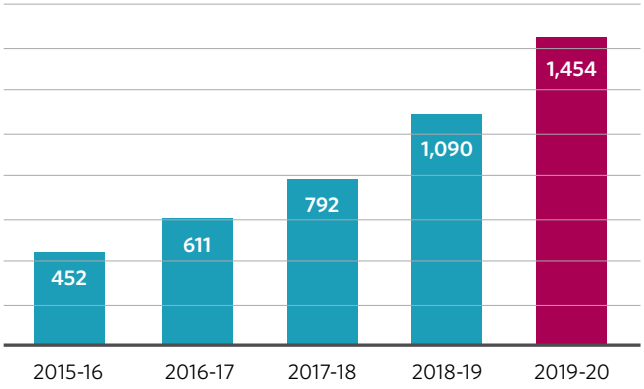
As of March 31, 2020, six cases were before the courts.

Privacy Impact Assessment Reviews

The OIPC accepted 1,031 privacy impact assessments (PIAs) in 2019-20, representing a 60% increase from 2018-19 (645). Nearly all accepted PIAs (98% or 1,014), were submitted by health custodians under HIA.

Only health custodians are required to submit PIAs to the OIPC in certain circumstances. Similar PIA requirements do not exist for public bodies or private sector organizations under the FOIP Act and PIPA.

PIAs OPENED ANNUALLY OVER FIVE YEARS*



**Not all opened files are accepted*

HIA

HIA requires custodians to prepare a PIA for any new or changed administrative practice or information system that involves individually identifying health information, and submit the PIA to the OIPC for review prior to implementation (section 64). Most PIAs each year relate to Netcare access, commonly used information systems or organizational privacy management policies.

Each year, many PIAs stand out as unique. In 2019-20, the OIPC received, as highlighted in the Trends and Issues section, dozens of PIAs related to AHS' wave one implementation of Connect Care.

In 2019-20, the OIPC also reviewed and accepted a PIA on AHS' community information integration (CII) project, which is meant to "bridge the gap" when a patient's interactions in a hospital are not automatically made available to the patient's family physician or primary care provider. Without CII, primary care providers are often unaware that their patients have visited a hospital or emergency department unless or until the patients visit their physician for follow up care.

CII sends electronic notifications to primary care providers via the provider's electronic medical record system when a patient is admitted to a hospital or acute care facility, for example.

When AHS sends hospital admissions, discharges and transfers for a patient to the CII hub, CII uses the central patient attachment registry to obtain the attached primary care provider and related information for the patient. CII then uses the metadata captured during the submission to identify the appropriate primary care provider, clinic and electronic medical record to send the electronic notification, in order to advise the primary care provider of their patient's hospital status.

PIPA

Relatively few PIAs are received from private sector organizations under PIPA.

In 2019-20, however, the OIPC accepted a notable PIA from ATB Financial (ATB) on its enterprise cloud implementation project.

ATB engaged the OIPC in 2017 when it began transforming its banking services. As part of the transformation, ATB began migrating its enterprise systems to what ATB calls a "hyper scale cloud provider ecosystem".

ATB submitted the PIA in relation to the migration of its enterprise systems to cloud providers. ATB anticipates that all of its systems will be migrated from its datacentres to the cloud providers by the end of 2022.

ATB's PIA was accepted by the OIPC in March 2020.

Another PIA submitted under PIPA was from Cybera Inc. related to a partnership it has with Alberta school divisions. The PIA was on its Pika Identity Federation solution, which is based on federated identity management (FIM). FIM refers to a collaboration by trusted independent organizations that agree to a common set of policies, practices and protocols to facilitate access to shared services using a single identity.

Cybera Inc.'s partnership with school divisions helps to provide secure access to educational resources or tools for students and employees in the K-12 education system.

Cybera's PIA was accepted by the OIPC in September 2019.

Mediation and Investigation

The OIPC mediation and investigation team reviews access request responses (requests for review) and responds to privacy complaints under all three laws. In 2019-20, 75% (393) of cases that could proceed to inquiry were resolved by mediation and investigation in 2019-20.

Several themes from prior years continued in 2019-20.

SURVEILLANCE

Access requests for video surveillance continue to pose a challenge to public bodies and organizations with respect to severing third party personal information.

Two common requests for review made to public bodies are by inmates in correctional facilities wanting access to surveillance footage and insurance companies seeking recordings from public transit or on roadways to investigate accident claims. The OIPC also received its first request for review related to a police service's use of body worn cameras.

In the private sector, the OIPC typically receives privacy complaints related to use or disclosure of information captured by surveillance cameras that the complainant believes is not consistent with the purpose for collection (i.e. security purposes). An example of this is a former employee of an organization who complained that the organization monitored a conversation between the individual and a co-worker, which the OIPC found was not consistent with preventing or investigating security incidents (e.g. theft).

There are other cases where the complainant believes collection is not for a reasonable purpose. An example of this was a complaint made against a landlord alleging they surreptitiously recorded and livestreamed activity in a common area of the building to monitor tenants' animal activity. The complainant said the camera was in a birdhouse, without notice.

Particularly in the private sector, complaints about video surveillance often require education to organizations about PIPA, such as ensuring that there is a reasonable purpose for the collection of personal information and outlining the notice requirements for collecting personal information.

COMPLAINTS REGARDING DISABILITY AND WCB CLAIMS

A theme in privacy complaints submitted to the OIPC continues to be individuals who question the collection, use and disclosure of personal information for disability claims with insurance companies under PIPA or Workers' Compensation Board (WCB) claims under the FOIP Act. In fact, the OIPC's first public investigation report, issued in June 1998, related to a complaint about the WCB's collection of personal information.[15]

The complaints generally relate to the collection and use of medical or other information that the complainant asserts is not relevant to their disability or WCB claim, or question the accuracy or adequacy of information disclosed to independent medical examiners.

[15] Office of the Information and Privacy Commissioner, "Investigation Report 98-IR-001: Workers' Compensation Board", June 4, 1998, is available from www.oipc.ab.ca/decisions/investigation-reports.aspx.

Other complainants have said that while they consented to the collection of their personal information, they subsequently questioned the extent and types of personal information collected, used or disclosed in the claims process. Complainants have also voiced concerns about the amount of personal information the WCB or its Appeals Commission should disclose to other interested parties, such as the date-of-accident employer.

A common challenge in these complaints is the expectations of complainants when the OIPC makes a finding. It is important to note that if the OIPC finds an organization or public body contravened PIPA or the FOIP Act by, for example, over-collecting personal information in processing a disability or WCB claim, the OIPC does not – and cannot – change a decision about whether or not to provide a benefit arising from the claim.

EMPLOYMENT ISSUES

Employment issues are often at the centre of mediation and investigation files.

A common situation is an employee who has been terminated from their employment and is seeking access to their personnel files, or other information, to defend themselves. The primary challenge for the OIPC in mediating these types of matters is that the individual may expect that a finding of contravening PIPA or the FOIP Act will result in reinstatement of employment or compensation, which are not remedies the OIPC can offer individuals.

In lieu, the OIPC uses these types of files as a way to educate all parties about the OIPC's role and what it can and cannot do. Meanwhile, if the OIPC finds a public body or organization contravened the FOIP Act or PIPA, recommendations are made to improve processes and the OIPC educates the entity about its legal obligations.

CLAIMS OF PRIVILEGE UNDER FOIP

The Commissioner has mentioned in prior annual reports the challenges the OIPC has faced in matters where a public body has claimed privilege over records to which an applicant has requested access, and does not provide those records for the OIPC's review.

If the public body does not provide the records to the OIPC for review, the public body is asked to provide information based on the OIPC's "Privilege Practice Note" to review if the exception for access is met.[16] The criteria for the practice note is based on the process used for claims of solicitor-client privilege in the context of civil litigation.

At mediation and investigation, when the OIPC receives strong submissions from public bodies, based on the practice note, it can result in a finding that the public body properly claimed the privilege exception.

However, instances continue to arise where a public body refuses to provide any information on the application of the privilege exception at mediation and investigation, forcing an applicant to request an inquiry for resolution of the claim of privilege. Given the challenges mentioned by the Commissioner about this issue in the past, it is concerning a public body may choose to unduly complicate the process by requiring an applicant to exhaust all stages of the request for review process, without any efforts made to prove its privilege claim at mediation and investigation.

[16] Office of the Information and Privacy Commissioner, "Privilege Practice Note", December 2016. Retrieved from https://www.oipc.ab.ca/media/768676/practice_note_privilege_dec2016.pdf.

Alleged Unauthorized Accesses and Disclosures of Health Information

On May 21, 2019, the OIPC released an investigation report that reviewed alleged unauthorized accesses and disclosure of health information at the Consort and District Medical Society Clinic (clinic).

On July 4, 2016, the OIPC received a letter enclosing a "...Privacy Breach Report Form regarding privacy breaches that occurred at the Consort Medical Clinic in Consort, Alberta" from Dr. Peter Idahosa Professional Corporation. At the time, Dr. Idahosa practiced at the clinic as a family physician.

The breach report alleged that:

- On January 19, 2016, two employees entered the clinic and accessed the electronic medical records database using one of their access codes.
- On January 21, 2016, one of the employees (Employee A) was on leave but visited the clinic during office hours and may have accessed a number of electronic medical records with the other employee's (Employee B) credentials.
- On February 10 and 11, 2016, Employee A accessed and may have printed, copied, shredded and/or taken medical records from the clinic.

On October 13, 2016, the Commissioner opened files to consider possible offences under HIA. In January 2018, the Commissioner determined that there was insufficient evidence to substantiate charges.

The investigation nonetheless proceeded as a compliance investigation on the Commissioner's own motion under section 84(1)(a) of HIA.

The investigation found that the employees (affiliates) of the physician (custodian) accessed and used patient information in contravention of HIA. However, the investigation also found that the physician failed to establish or adopt policies and procedures to facilitate implementation of HIA and the *Health Information Regulation,* and failed to ensure that employees were made aware of and adhering to the administrative and technical safeguards put in place to protect health information.

As noted in the Commissioner's Message in the report, "This investigation marks the fourth report over two years that I have released under the *Health Information Act* (HIA) where the focus of an investigation into a privacy breach shifted from an affiliate of the custodian to the custodian itself. This is a troubling trend."

In addition to the findings on unauthorized access and disclosure, and the failure to safeguard health information, the investigation also found that while a privacy impact assessment on privacy policies and procedures was developed in 2006, and updated in 2013, one of the employees admitted that the PIA was "never opened". Despite the PIA stating that employees were "educated" on privacy policies and procedures, the investigation also found none of the employees had received training.

In response to these findings, the Commissioner said:

> I have frequently said that one of the most effective proactive measures in Alberta's privacy laws is the requirement under HIA for custodians to complete PIAs and submit them to my office for review. This helps to ensure that custodians develop and implement rigorous privacy management programs that include delegated responsibilities, policies and procedures, training and awareness, and safeguards to protect health information. However, there is no value in this exercise if a custodian

considers completing a PIA to be a checklist activity, and that once the "box is ticked", the PIA can be shelved, never to be communicated, implemented, revisited or revised. When my office accepts a PIA submitted by a custodian it is with the expectation that the controls described to protect patient privacy will be implemented immediately.

Not only does my office expect more of custodians when protecting patient privacy, Albertans do too. Protection of health information is consistently rated among the most important of privacy issues in public opinion surveys.

The investigation made four recommendations, including for the clinic to develop or reinstate privacy and security policies and procedures and ensure all physicians practicing at the clinic adopt them, and all staff receive regular updated, documented privacy training.

Investigation Report H2019-IR-01: Investigation into alleged unauthorized accesses and disclosures of health information at Consort and District Medical Society Clinic

> "I have frequently said that one of the most effective proactive measures in Alberta's privacy laws is the requirement under HIA for custodians to complete PIAs and submit them to my office for review... However, there is no value in this exercise if a custodian considers completing a PIA to be a checklist activity, and that once the 'box is ticked', the PIA can be shelved, never to be communicated, implemented, revisited or revised."
>
> *- Commissioner Jill Clayton, May 21, 2019*

Alleged Destruction of Records Responsive to Access Requests

On May 1, May 14 and June 21, 2018, the Commissioner received applications from Alberta Justice and Solicitor General (JSG), made under section 55(1) of the FOIP Act, requesting authorization to disregard five access requests made by an inmate to the Calgary Remand Centre (CRC). The requests were for CCTV video recordings.

On June 28, 2018, the OIPC's review of the three requests to disregard found they each contained wording similar to the following:

> Please note that the video records that are requested are on a 30-day loop and have not been secured. The Public Body requests the OIPC to advise if they want the Public Body to secure the video records. A response is required by [...] in order to ensure that the video records are secured before the 30-day loop.

On June 29, 2018, the Commissioner wrote to JSG and requested immediate confirmation as to whether the records responsive to the access requests had been destroyed. The Commissioner stated:

> I should not have to tell Alberta Justice and Solicitor General that it is required to preserve and not destroy any and all records that are responsive to these access requests while these matters are before me.

The former Deputy Minister for JSG responded:

> We have conducted inquiries and have confirmed that the videos were on an analog recording system and that they were overwritten after 30 days. I have been advised that they are not recoverable. The approach taken by the public body was inappropriate. Requesting your office to take an active step to prevent the destruction of records subject to an access request is unacceptable and does not reflect JSG's guidance or corporate culture, or that of the GoA.

On July 31, 2018, the Commissioner issued decisions for the three section 55 files. One of the decisions stated:

> I am extremely concerned about Alberta Justice and Solicitor General's destruction of records that are responsive to an access request under FOIP. I am aware that this same destruction of responsive records has occurred in two other JSG applications under section 55(1)... My decisions in those matters are being issued concurrently.
>
> I have opened a new file to investigate Alberta Justice and Solicitor General's destruction of responsive records.

The subsequent investigation found that the information JSG provided in its requests to disregard was inaccurate. Three of the access requests were for records that never existed, and JSG did not know this at the time it submitted its requests. The investigator did, however, find that JSG did not preserve records as required for the remaining two access requests.

In response to these findings, the Commissioner said:

> The failure by JSG to ensure that responsive records were preserved compromised the integrity of the access to information process, and did not comply with the GoA's rules relating to the destruction of records (i.e. records must be preserved when subject to an access request). JSG also failed to respect my exclusive power under the FOIP Act to authorize a public body to disregard certain requests. Had I ordered JSG to process these requests, it would not be in a position to do so. Furthermore, as JSG acknowledges, when it makes a section 55(1) application, asking the Commissioner to take active steps to ensure that responsive records are preserved is inappropriate and unacceptable.

There were 10 recommendations made in the report, including six on the processing of access requests and four with respect to the administration of JSG's CCTV system at CRC.

Investigation Report F2019-IR-02: Investigation into Alberta Justice and Solicitor General's alleged destruction of records responsive to access request

Requests for Time Extensions by Public Bodies

A public body must make every reasonable effort to respond to an access request 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 (section 14). 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 treated as a decision to refuse access (section 11(2)).

In 2019-20, there were 231 requests for time extensions submitted by public bodies to the OIPC, representing an increase of 2% over 2018-19 (226). Of the 231 time extension requests received in 2019-20:

- 73% were made by provincial government departments
- 11% were made by municipalities
- 5% were made by post-secondary institutions
- 2% were made by school divisions
- 9% were made by other public bodies (e.g. commissions, law enforcement, boards, etc.)

The following decisions were made on time extension requests:

- 69% were granted
- 17% were partially granted (i.e. extension period permitted was less than what the public body requested)
- 11% were denied
- 3% were withdrawn by the public body

Deemed Refusals to Respond to Access Requests

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 and 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.

The OIPC issued only five deemed refusal orders in 2019-20, a significant decrease from the 30, 25 and 48 deemed refusal orders issued in the previous three years – 2018-19, 2017-18 and 2016-17, respectively. Four of the five deemed refusal orders in 2019-20 were issued to government departments.

Summary of Significant Decisions

Summary Information Not a Response under FOIP

An applicant requested records related to all retreats and/or meetings attended by principals of Edmonton Catholic School District No. 7 (school district) that took place outside of Edmonton. A similar request was also made for records relating to retreats and/or meetings attended by teachers. The applicant explained that the requests included all costs associated with any meetings or retreats in such places as Jasper Park Lodge or Kananaskis.

The school district responded by providing a summary it had created for the purpose of responding to the access request, and indicated it was "unable to perform an adequate search based on the initial criteria" provided in the applicant's request. The applicant argued that this "summary information" was not what had been requested.

During the inquiry, the Adjudicator noted that the school district "was able to describe the kinds of records that would be responsive and a method of searching for them". However, the school district did not search for responsive records or prepare a fee estimate regarding the costs of searching for and producing the records. It said the reason for not doing so was because it "would require sending emails to 2977 teachers and principals, and then reviewing the 'code series transactions' with the physical receipts in schools." Instead of processing the request, the school district asked the applicant to narrow the request. In doing so, the school district said it could not process the request until it received more information from the applicant about how the request would be narrowed, which the Adjudicator said "in essence" was the school district telling the applicant that it would not process the request until fewer records were requested.

The Adjudicator found that by providing summary information in response to the request, the school district had not responded to the applicant as required by section 11 of the FOIP Act.

The school district was ordered to respond to the applicant.

Following the issuance of this order, the OIPC took the extraordinary step of submitting a contempt application against the school district after it failed to inform the Adjudicator that it had complied with the order. The FOIP Act requires a public body to comply with an order within 50 days of receiving the order.

Order F2019-22, Edmonton Catholic School District No. 7

Inappropriate Access of Police Database

After receiving information from an access request, an individual submitted a complaint that Calgary Police Service (CPS) collected, used or disclosed his personal information in contravention of the FOIP Act. He complained that several accesses of his personal information – by a police officer (referred to as AB), now married to the complainant's former spouse, and other CPS staff who had relationships with AB or with the complainant's former spouse – contravened the FOIP Act.

The Adjudicator found that CPS already had custody and control of the complainant's personal information, and that AB's collection was not considered another collection of personal information. The Adjudicator also found that there was insufficient evidence to determine that AB disclosed the personal information without authority.

However, CPS acknowledged that AB had used the complainant's personal information by accessing it from a CPS database and that this use was unauthorized. CPS stated that audit records show AB, on two occasions, searched for and viewed reports in a case file relating to the complainant and his child custody dispute.

AB acknowledged he did not have a valid police reason to access the information. CPS Professional Standards Section investigated the improper accesses and disciplinary action was taken against AB. CPS further stated it "engaged in a service wide educational and informational campaign", including a training video on informational privacy, across the police service to reinforce the "absolute prohibition on accessing CPS databases and other information resources for any purpose other than lawful police business". The Adjudicator said, "I am satisfied with the remedial action taken by CPS to address the officer's actions directly and to provide additional training and safeguards more broadly (discussed at paragraph 19 of this Order). Therefore, I have nothing further to order to address the unauthorized use."

Order F2019-40, Calgary Police Service

Disclosure Authorized to Avert Risk of Harm to an Employee

An individual complained that Alberta Health Services (AHS) improperly disclosed his personal and health information to the Lethbridge Police Department (LPD). The disclosure related to a complaint an AHS employee made about the individual to LPD.

The Adjudicator explained:

> The evidence before me establishes that an employee of AHS provided three binders of the Complainant's correspondence written to AHS to the Lethbridge Police Service. The purpose of these disclosures of the Complainant's personal information was to obtain an assessment as to whether the Complainant posed a threat to AHS employees and whether the Lethbridge Police Service could provide any advice to assist AHS to mitigate any risk it identified. The information discussed did not include information gathered in the course of providing medical services or information about the Complainant's health or treatment.

The Adjudicator determined, as a result, that the FOIP Act applied to the information at issue, and that health information was not disclosed by AHS to LPD.

With respect to the disclosure of the complainant's personal information by AHS to LPD, the Adjudicator found "that the disclosure was authorized, rather than unauthorized, as the employee who disclosed the information had responsibilities in relation to both the information disclosed, and employee safety, which was the reason for which [the] Complainant's personal information was disclosed." In finding that the disclosure was authorized, the Adjudicator said:

> I am satisfied that the employee provided the Complainant's correspondence to the Lethbridge Police Service for the purpose of averting a foreseeable risk of harm to the mental and physical health of employees. The view that the Complainant was a potential risk to health and safety was based on numerous verbal altercations involving the Complainant and employees, and the Complainant's correspondence to employees, which could reasonably be viewed as threatening, even though the Complainant may not share this perception of events or his correspondence.

The Adjudicator also determined that AHS had not disclosed any more personal information than was reasonably necessary for meeting its purpose in disclosing the information.

Order F2020-01, Alberta Health Services

Reconsideration of Order after Privilege Claim Withdrawn

This order was a reconsideration of Order F2017-54, which examined the response of the Alberta Emergency Management Agency (AEMA) to an access request under the FOIP Act. On judicial review of that order, the Court of Queen's Bench directed certain records be provided to the OIPC for assessment by a different adjudicator.

There were two sets of records in this reconsideration.

With respect to the first set of records, on judicial review of Order F2017-54, and before the day of the judicial proceeding, AEMA withdrew its privilege claim over the records. Those records were not before the court in the proceeding. The court directed that the records be provided for review by a different adjudicator for a review of other exceptions AEMA had applied to those records. AEMA applied sections pertaining to disclosure harmful to personal privacy (section 17), advice from officials (section 24(1)) and privileged information (sections 27(1)(b) and/or (c)) to information in several pages of records. The Adjudicator found AEMA had properly applied exceptions to access, except for a limited amount of information to which section 24(1)(a) did not apply, and the Adjudicator ordered that information to be disclosed to the applicant.

With respect to the second set of records, in Order F2017-54, AEMA argued that the records were excluded from the FOIP Act under section 4(1). The Adjudicator rejected this argument, and ordered AEMA to respond to the applicant with respect to these records, including the appropriate application of any exception in the Act. AEMA complied with that part of the order, and applied sections 27(1)(a), (b) and (c), as well as section 24(1), to the information in these pages.

During the reconsideration, AEMA objected to producing records over which it claimed section 27(1)(a); however, it had previously provided the records to the OIPC when AEMA was not claiming privilege over the information in them. In coming to a finding, the Adjudicator said:

> Had the Public Body not provided the records for my review, and had the Public Body's description of pages 186-187 been the only information before me about the records, I likely could not have upheld the claim of solicitor-client privilege. As noted, correspondence to a third party adverse in interest to the client often cannot be subject to solicitor-client privilege. In this case, the records themselves provided the necessary evidence to show that privilege was correctly claimed.
>
> This illustrates the importance of providing accurate and sufficient submissions regarding records over which privilege is claimed. This is especially the case where those records are not provided for review.

The Adjudicator found that section 27(1)(a) applied to the information in the second set of records, and therefore did not need to consider whether sections 27(1)(b) and (c) were properly applied.

Order F2020-R-01, Alberta Emergency Management Agency

Use of Health Information to Defend the Provision of a Health Service

An individual complained that her former psychiatrist, Dr. Gendemann, accessed her health information on Netcare after he had ceased being her doctor in contravention of HIA.

Dr. Gendemann acknowledged that he had accessed the complainant's health information in Netcare, and argued that the information was accessed for the purpose of responding to a complaint being investigated against him by the College of Physicians and Surgeons. The complainant made the complaint against Dr. Gendemann to the College of Physicians and Surgeons.

The Adjudicator applied the principles set out in an Alberta Court of Appeal decision to the use of health information for providing health services (section 27(1)(a)). The Adjudicator explained:

I interpret the Court's view to be that physicians ought to be permitted to use health information in the EHR/Netcare that is essential to respond to complaints made about the way they provided health services. However, if section 27(1)(c) is the authority to use the health information for this purpose, then the use is permitted only when physicians are providing health services as affiliates of specified custodians (for example, physicians working as affiliates of AHS). It is not permitted when the physician is providing the health service as a [custodian] in their own right. There is no clear justification for this disparity.

I prefer an interpretation relying on section 27(1)(a) of the HIA, which does not distinguish between physicians as affiliates of larger custodians and physicians as custodians in their own right, and which is consistent with the conclusion in *Gowrishankar*.

Under the proposed analysis, defending the provision of a health service is an extension of providing that health service. Where a health care provider had authority under section 27(1)(a) to use health information to provide a health service, the health care provider is also authorized to continue to use that health information to defend themselves against a complaint about how they provided the health service. This interpretation would apply to complaints made to the College, to civil court actions, and other such proceedings arising out of the provision of the health service.

This interpretation also applies to information directly related to and emanating from the health service provided, such as the physician's report of the outcome of the health service, plans for ongoing care, and discharge reports that document the health service provided. In some cases, this information cannot be said to have been used by the health care provider when providing the health service in question, as it resulted from (i.e. came after) the service had concluded. However, such documentation is a direct result of and reports on the health service. It seems nonsensical to suggest that in a complaint or similar proceeding arising from the provision of a health service, a health service provider can use health information they reviewed when providing the service (e.g. lab results used to diagnose an illness), but cannot use the information generated from the service, such as a follow-up report.

Therefore, health information used by a health service provider while providing a health service under section 27(1)(a) can continue to be used under the same authority in later proceedings arising from the provision of that health service (e.g. defending against a complaint). The information that directly relates to and emanated from the provision of the health service, such as documentation of the service, can also be used in those proceedings under the same authority…

The interpretation of section 27(1)(a) that I have put forward cannot be taken as authority for a health care provider to undertake a general or wholesale review of any of an individual's health information in the EHR/Netcare for the purpose of finding something useful or relevant. Rather, this interpretation of section 27(1)(a) extends the authority to use the health information that was used by the health service provider when they provided the health service, in a later complaint or proceeding that arose from the provision of the health service, as well as the information directly relating to and emanating from the service.

The Adjudicator noted that this interpretation does not limit other authorities, such as section 27(1)(c) contemplated in *Gowrishankar*, or processes for accessing health information in the context of a complaint, investigation, court proceeding, etc.

The Adjudicator determined that Dr. Gendemann had authority to access the complainant's health information in Netcare under section 27(1)(a) to defend the provision of a health service.

Order H2020-03, Dr. Klaus D. Gendemann

Company's Vehicle GPS Tracking Device Authorized by PIPA

Individuals complained that NAL Resources Management Ltd. (NAL) contravened PIPA when it instituted a policy that required contractors, including the complainants, to have a GPS tracking device installed on their vehicles.

NAL indicated the default setting of the tracking device would be "on", but a vehicle operator could turn it off when not performing services for the organization. NAL said the purpose of the tracking device was to "promote good driving behaviour" and for occupational health and safety purposes, such as to "minimize the real risks of physical harm inherent to working alone around upstream oil and gas assets in remote areas". NAL added that, "Without the Telemetry Data, it would be practically impossible for NAL to safely manage the Complainants' employment relationship, because they would not have guaranteed working alone coverage."

The Adjudicator noted that PIPA "creates a class of personal information called 'personal employee information' which is subject to different rules than 'personal information'." Sections 15 and 18 of PIPA establish the circumstances in which an organization may collect and use "personal employee information". The Adjudicator noted that neither section requires the consent of an individual "for the sole purpose of managing an employment relationship, provided that it is reasonable to collect or use the personal employee information for the particular purpose, and reasonable notification of the Organization's intention has been provided."

The Adjudicator found that the information collected by the GPS tracking device was personal employee information within the terms of PIPA, as the organization collected and used it for the purpose of managing the employment relationship. In making this finding, the Adjudicator noted that previous orders found "that information in respect of the relationship between an organization and a contractor is to be viewed as information in respect of an employment relationship for the purposes of PIPA."

The Adjudicator also found that the collection and use of personal employee information was reasonable and the complainants were notified in accordance with PIPA, stating that NAL's:

> ...purpose in collecting and using data obtained from the GPS tracker is to comply with its regulatory occupational health and safety obligations to its workers. I find that complying with occupational health and safety requirements is an example of managing an employment relationship. I also find that this collection and use is solely for this purpose and that it is reasonable to collect the data for this purpose. Finally, I find that the Organization provided notice to the Complainants regarding its intent to collect and use data with the GPS tracker and its purposes in doing so.

The Adjudicator confirmed that the organization was not in contravention of PIPA when it collects and uses information obtained from a GPS tracking device installed on the complainants' vehicles. The Adjudicator also found that NAL had a privacy officer (section 5(3)), had privacy policies and practices in place and provides information about them (sections 6(2)(a) and (b)), and had reasonable security arrangements for personal information in its custody and control (section 34).

Order P2019-04, NAL Resources Management Ltd.

Fees Refunded in Request for Expense Claims

An individual made an access request to the County of Two Hills No. 21 for records related to expense claims made by county council members during a specified period of time. The county provided the applicant with a fee estimate in the amount of $1,000.

The applicant requested that the county waive the fee on the basis that the records were in the public interest. The county declined to waive the fee.

The applicant paid the fee but requested a review of the county's decision to charge the fee.

The Adjudicator found the county failed to substantiate that the $0.25 per page that it charged to the applicant for photocopying did not exceed the county's actual costs as required by the FOIP Act.

The Adjudicator said:

> Given that the Public Body in this case has said it relied on its Fee [Bylaw] as its authority to charge $0.25 per page for photocopying; that it did not provide me with any information about its actual costs for photocopying; that it did not provide me with any information as to how many hours or days it spent searching for, locating and retrieving the records; that it did not provide me with any information about the hourly rate of the employee(s) who performed the services; and that it said it could not accurately provide me with any further information, I do not think this is an appropriate situation to order the Public Body to recalculate its fees using its actual costs to provide these services...
>
> Accordingly, given the lack of evidence provided by the Public Body to support that the fee it estimated and charged the Applicant complied with the FOIP Act and the Regulation, I have decided the appropriate result in this case is to order the Public Body to refund all fees to the Applicant that were paid by the Applicant in relation to his access request.

The Adjudicator ordered the county to refund all fees paid by the applicant, due to the lack of evidence supporting its actual costs in responding to the applicant. Consequently, it was not necessary for the Adjudicator to determine whether payment of any of the fee should be refunded on the basis that the records related to a matter of public interest.

Order F2019-21, County of Two Hills No. 21

Requests to Disregard

A "request to disregard" is made by public bodies, health custodians or private sector organizations under section 55 of the FOIP Act, section 87 of HIA or section 37 of PIPA, respectively. These provisions provide the Commissioner with the power to authorize a public body, health custodian or private sector organization to disregard access requests in certain circumstances. The public body, health custodian or private sector organization must meet their burden in proving that the access request should be disregarded.

The OIPC began publishing more request to disregard decisions to assist public bodies, health custodians and private sector organizations in submitting requests to disregard to the Commissioner. In 2019-20, three request to disregard decisions, involving seven access requests, were made available on the OIPC's website.

Request to Disregard F2019-RTD-02 & H2019-RTD-01, Alberta Health Services
Request to Disregard F2019-RTD-03, Calgary Police Service
Request to Disregard F2019-RTD-04, University of Lethbridge

Tobacco Inquiries

An applicant made two separate access requests to Alberta Health (AH). The first access request was for the Contingency Fee Agreement (CFA) and the second for documents related to the CFA, in particular, records regarding the arrangements the Government of Alberta (GoA) made with outside counsel to pursue litigation to recoup smoking-related health care costs. The External Adjudicator made several determinations in this part of the inquiry, and ordered the release of certain records.

Two applicants made separate access requests to Alberta Justice and Solicitor General (JSG). The first applicant made two requests and the second applicant made one request. The first request from the first applicant was for the CFA and the second for documents related to the CFA, in particular, records regarding the arrangements the GoA made with outside counsel to pursue litigation to recoup smoking-related health care costs. The second applicant's request was for all records related to the contract tendering process, the selection process of counsel and any requests for proposals and bids submitted connected to the CFA litigation. However, the second applicant withdrew their request for inquiry during the inquiry. The External Adjudicator made several determinations in this part of the inquiry, and ordered the release of certain records.

Two applicants each made one access request to JSG. The first applicant's access request was for any requests for proposals from and agreements entered into by JSG regarding external legal services, and without limiting the request, naming three specific law firms, with respect to the recovery of health care costs associated with the use of tobacco. The second applicant's access request was for all records related to the awarding of the CFA between JSG and the law firm group retained and the CFA itself. In addition, the request was for records related to the process of awarding the tobacco litigation legal work as to how the firm selected was chosen over its competitors. The External Adjudicator made several determinations in this part of the inquiry, and ordered the release of certain records.

AH and JSG applied for judicial review on these orders. In total, there have been 10 applications for judicial review on orders regarding access requests made for the CFA and related records.

Order F2019-26, Alberta Health
Order F2019-27, Alberta Justice and Solicitor General
Order F2019-28, Alberta Justice and Solicitor General

Judicial Reviews and Other Court Decisions

JUDICIAL REVIEWS

Alberta (Municipal Affairs) v Alberta (Information and Privacy Commissioner)

2019 ABQB 274 – Judicial Review of Order F2017-54 (Reasons for Privilege Determination)

In Order F2017-54, the applicant had requested records containing information relating to the construction of berms during the flooding in High River in 2013 and records regarding an arbitration that had taken place in relation to the flooding. The Alberta Emergency Management Agency (AEMA) provided some responsive records and withheld others under various exceptions, including solicitor-client privilege (section 27(1) of the FOIP Act).

In this decision, the court dealt solely with the claims of solicitor-client privilege over some records at issue. At inquiry, the Adjudicator was not provided with the records over which solicitor-client privilege had been claimed. On the basis of the evidence provided by AEMA, the Adjudicator was unable to determine whether solicitor-privilege had been correctly claimed and ordered AEMA to produce the records to the applicant.

On judicial review, pursuant to a consent procedural order, AEMA provided the records over which it had asserted solicitor-client privilege to the court as new evidence. The court reviewed the records and applied an eight-part test to determine whether the privilege had been correctly claimed 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 any privileged information, can it be reasonably severed from the rest of the record, without revealing the privilege?

After reviewing the new evidence (the actual records over which solicitor-client privilege had been claimed), the court determined that all of the records were subject to solicitor-client privilege.

2019 ABQB 436 – Judicial Review of Order F2017-54

Following the release of its privilege determination, the court issued reasons for the remainder of the judicial review. The court quashed the portions of Order F2017-54 dealing with sections 10 and 27 of the FOIP Act. The records over which AEMA had claimed section 24 exceptions were remitted to the Commissioner for reconsideration by a different adjudicator. On January 27, 2020, Order F2020-R-01 was issued.

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

2019 ABQB 587 – Judicial Review of Order F2017-87

Order F2017-87 found that Edmonton Police Service (EPS) had accessed information regarding two criminal investigations in which the complainant had been the subject as a youth in addition to other information regarding police investigations of which he had been the subject, and had disclosed this information to his employer. At inquiry, the complainant also raised the issue that EPS had used information of this kind to create a police information check (PIC) and a vulnerable sector check (VSC), and that the PIC and VSC created by EPS resulted in the termination of his employment, even though he did not have a criminal record and had never been convicted of a criminal offence.

The Adjudicator determined that EPS had not established that it had identified the information it would use or obtained the consent of the complainant to use his personal information to create the PIC and VSC within the terms of section 39(1)(b) of the FOIP Act and section 7 of the FOIP Regulation. The Adjudicator held the disclosure of the complainant's personal information had not been authorized by Part 2 of the FOIP Act and directed EPS not to use and disclose the complainant's personal information contrary to the terms of the Act in the future.

The court upheld Order F2017-87. It stated, at paragraph 193, that a public body does not have discretion on how it can use personal information collected by it, as use is determined by the FOIP Act. The court pointed out that in Alberta PICs and VSCs are entirely unregulated other than under the FOIP Act (excluding vulnerable sector checks by the RCMP under the *Criminal Records Act*), and encouraged the Alberta Law Reform Institute to consider the potential for legislation in Alberta similar to the *Police Record Checks Reform Act* in Ontario.

2019 ABQB 864 – Ruling on Costs

The court ordered EPS to pay costs to the complainant.

JK v Gowrishankar

2019 ABCA 316 – Appeal of 2018 ABQB 70

In Order H2016-06, an individual complained that two physicians accessed her health information from Alberta Netcare in contravention of HIA. The Adjudicator held that the physicians had not been authorized by HIA to use and disclose the complainant's health information. This order was quashed on judicial review, and that decision was subsequently appealed by the complainant.

On appeal, the court stated that HIA permits the use of health information by custodians and affiliates for various purposes and that use of health information is permitted so long as it is for a purpose provided by HIA and only health information essential to carrying out the intended purpose is used. The court held that the disclosure had been done with the consent of the complainant in accordance with section 34. The court dismissed the appeal, holding that Order H2016-06 was unreasonable and that the complainant's health information had been used and disclosed in accordance with HIA.

University of Calgary v Alberta (Information and Privacy Commissioner)

2019 ABQB 950 – Judicial Review of Order F2018-15

The applicant requested copies of the University of Calgary's (U of C) legal bills associated with a judicial review application, an appeal, and a leave to appeal action in which he and the U of C were adverse parties. The U of C withheld portions or in full some records as being subject to solicitor-client privilege under section 27(1) of the FOIP Act.

At inquiry, the Adjudicator was not provided with the records over which solicitor-client privilege had been claimed. The Adjudicator held the U of C had not met its burden and she was unable to determine whether solicitor-privilege had been correctly claimed. The U of C was ordered to disclose the records to the applicant.

On judicial review, in recognition of the high public interest in maintaining the confidentiality of the solicitor-client relationship and the integrity of the administration of justice, the court stated that solicitor-client privilege is all but absolute. The court further held that the wording in section 71(1) of the FOIP Act was not clear enough to exclude the presumptive privilege pertaining to solicitor's accounts.

The court quashed Order F2018-15 and remitted the matter to the Commissioner to be determined in accordance with the court's reasons.

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

2020 ABQB 10 – Judicial Review of Orders F2013-13, F2017-57 and F2017-58

The three orders under judicial review, broadly, involved access requests by the Criminal Trial Lawyers' Association to the Edmonton Police Service (EPS) for records relating to complaints about and investigations of a police officer. Given the similarity of parties and issues, the three judicial reviews were consolidated by consent of all parties. The main issues before the court included the applicable standard of review, claims of solicitor-client privilege over crown opinion records and external counsel records, and the interpretation of sections 27(1)(b) and (c) and section 17 of the FOIP Act. The resulting decision was 135 pages and discusses each issue in detail.

The court confirmed that a public body bears the burden to prove that an exception under the FOIP Act applies. Pursuant to a consent procedural order, EPS provided the records over which it had asserted solicitor-client privilege to the court as new evidence. The court applied the eight-part test to determine whether solicitor-client privilege had been correctly claimed over each record.

In summary, the court determined:

- The crown opinion records were protected by solicitor-client privilege. The Adjudicator's findings to the contrary were wrong.
- The external counsel records were protected by solicitor-client privilege, with one exception. The Adjudicator's findings to the contrary were wrong.
- With some minor exceptions, the Adjudicator's interpretive approach to sections 27(1)(b) and (c) was reasonable, although the application of these provisions did not affect the withholding or disclosure of any records.
- The Adjudicator's determinations under section 17(5) were not reasonable as the Adjudicator failed to take into account some factors relating to whether the disclosure of records would constitute an unreasonable invasion of the officer's personal privacy.

The court remitted a portion of the records back to the Commissioner for reconsideration.

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

2020 ABQB 207 – Judicial Review of Order F2018-36

The Criminal Trial Lawyers' Association requested all records from Edmonton Police Service (EPS) relating to its YouTube series "The Squad". The applicant requested records relating to the planning and implementation of the series, criticism of the series, any reviews of criticism and EPS' response to criticism, and records containing information about why the series was cancelled. EPS located 1,448 pages of responsive records, and severed or withheld information under various exceptions, including solicitor-client privilege (section 27(1) of the FOIP Act).

At inquiry, the Adjudicator was not provided with the records over which solicitor-client privilege had been claimed. On the basis of the evidence provided by EPS, the Adjudicator concluded that two records were properly withheld on the basis of solicitor-client privilege, but that EPS had failed to establish that section 27(1)(a), (b) or (c) applied to the remaining records. EPS was ordered to disclose the remaining records.

The sole issue before the court on judicial review was EPS' application of section 27(1) to records. Pursuant to a consent procedural order, EPS provided the records over which it had asserted solicitor-client privilege to the court as new evidence. The court reviewed the records and, as in previous judicial reviews involving claims of solicitor-client privilege, applied the eight-part test to determine whether the privilege had been correctly claimed.

After reviewing the new evidence (the records over which solicitor-client privilege had been claimed), the court determined that all of those records were subject to solicitor-client privilege. The court quashed the portion of the order requiring disclosure of the records over which solicitor-client privilege had been claimed.

OTHER COURT DECISIONS

Makis v Alberta Health Services

2019 ABCA 288

The Commissioner was granted leave to intervene in the appeal of the decision cited as 2018 ABQB 976. In that decision, the court had declared the appellant to be a vexatious litigant and stayed all matters involving him before any non-judicial body, including the Commissioner.

Carter v Alberta (Ministry of Justice and Solicitor General)

2019 ABQB 491

As reported in the 2018-2019 Annual Report, in Action No. 1801 05226 the court had, on its own motion and under its inherent jurisdiction, initiated a process to determine whether the applicant should be subject to litigation gatekeeping through court access restrictions.

After reviewing submissions from all parties, the court determined that on the facts of this case, court access restrictions, and restrictions to information and privacy related processes were appropriate. The applicant was declared to be a vexatious litigant. As is set out in a detailed order within the decision, the applicant is required to obtain leave from the court prior to making any information or privacy related request.

John Doe v Edmonton Public School District No. 7

2019 ABQB 952

The applicant's application to use a pseudonym in his judicial review of Order F2019-25 and his request for a publication ban was dismissed. The court ordered that the style of cause be amended to reflect the applicant's full legal name and that the court file would remain open to the public.

EDUCATION & OUTREACH

Speaking Engagements

The Commissioner and staff made 55 presentations in 2019-20. To focus on daily operations and increasing caseloads, the OIPC has declined more speaking engagement requests over the past two years.

RIGHT TO KNOW WEEK FORUM

The OIPC hosted forums in Calgary and Edmonton to commemorate Right to Know Day, which is recognized on September 28 by the United Nations Educational, Scientific and Cultural Organization (UNESCO) as the "International Day for Universal Access to Information".

At both events, Sean Holman, Associate Professor of Journalism at Mount Royal University, presented on the history of access to information based on research he has been undertaking, and Katie Cuyler, Public Services and Government Information Librarian at the University of Alberta, discussed archiving digital government records.

In Calgary, the City of Calgary presented on routine disclosures of information. In Edmonton, Service Alberta presented on its government-wide content management program.

As always, both events were well attended, and provide an opportunity for networking among access and privacy professionals, among other attendees.

AI, ETHICS AND SOCIETY CONFERENCE

The University of Alberta's Kule Institute hosted a multidisciplinary conference to discuss the societal and ethical implications of artificial intelligence and machine learning.

The Commissioner was invited to present, and spoke on the fundamental role of privacy and ethics in responsible technology development. The presentation was adapted for publication in the "International Review of Information Ethics", a scholarly journal. The abstract of that article reads:

> For years, privacy regulators have said that privacy is good for business. Strong privacy management programs and accountability mechanisms build trust with consumers. In the public sector, privacy regulators have seen massive information sharing projects fail when public input or consultation, or independent oversight is not considered. After a sequence of events in 2018, society as a whole began asking questions about what is being done with personal information and questioned whether it is in our best interests. This presentation... provides an overview of the shifts that have taken place and how privacy regulators internationally have incorporated discussions about ethical assessments, in addition to traditional privacy impact assessments, as a way to guide current and future tech developments involving personal information in a way that is legal, fair and just.

The article was scheduled for publication in June 2020.

AccelerateAB

In April 2019, the Commissioner presented at A100's annual technology conference, AccelerateAB. A100 is a member-driven group of Alberta technology entrepreneurs with the mandate to support and strengthen Alberta's tech ecosystem. The Commissioner spoke on the topic of "Cybersecurity and Privacy" to an audience of approximately 700 technology entrepreneurs including both early-stage and late-stage startups, angel investors, and venture capitalists.

MEXICO'S NATIONAL TRANSPARENCY WEEK

The Commissioner was honoured to be invited by the National Institute for Transparency, Access to Information and Personal Data Protection, to participate in National Transparency Week 2019 in Mexico City, in November. Mexico's National Transparency Week facilitates the analysis and exchange of international experiences in transparency and access to public information, in order to contribute to the development of an integral system of accountability and to foster an open democratic society. Along with speakers from Mexico and Argentina, the Commissioner participated in a panel discussion on "Prospects for transparency and access to information at subnational authorities".

MLA ORIENTATION

Following the 2019 provincial election, the Commissioner joined her legislative officer colleagues in presenting about their respective mandates to new MLAs. In addition to the presentation, the OIPC joined legislative offices and the various support services of the Legislative Assembly Office in a "tradeshow" for MLAs to learn about the functions of the government's legislative branch.

ACCESS AND PRIVACY CONFERENCE

The OIPC once again was pleased to participate in the University of Alberta's annual Access and Privacy Conference in June 2019, a leading Canadian conference on access and privacy issues.

The Commissioner provided welcoming comments, participated in a Canadian Commissioners' roundtable discussion, and joined senior staff in discussing OIPC trends and issues. The OIPC also led a workshop on breach response and reporting, and presented in partnership with Alberta Health on the first year of mandatory breach reporting under HIA.

Collaboration with Other Jurisdictions

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

JOINT RESOLUTION ON MODERNIZING LEGISLATION

The federal, provincial and territorial Information and Privacy Ombudspersons and Commissioners urged governments in November 2019 to modernize access to information and privacy laws in a joint resolution. The resolution says, in part:

> Most Canadian access and privacy laws have not been fundamentally changed since their passage, some more than 35 years ago. They have sadly fallen behind the laws of many other countries in the level of privacy protection provided to citizens.

Canada's access to information and privacy guardians also noted that along with its many benefits, the rapid advancement of technologies has had an impact on fundamental democratic principles and human rights, including access to information and privacy.

The resolution calls for:

- A legislative framework to ensure the responsible development and use of artificial intelligence and machine learning technologies
- All public and private sector entities engaged in handling personal information to be subject to privacy laws
- Enforcement powers, such as legislating order-making powers and the power to impose penalties, fines or sanctions
- The right of access to apply to all information held by public entities, regardless of format

INTERNATIONAL CONFERENCE OF INFORMATION COMMISSIONERS

The OIPC's application for membership in the International Conference of Information Commissioners was accepted in September 2019. The Commissioner also continued as a member of the ICIC Governance Working Group, established to develop the governance processes for ICIC.

The ICIC is a forum that connects member Information Commissioners responsible for the protection and promotion of access to information laws globally.

ACTIVITY SHEETS AND LESSON PLANS FOR STUDENTS

Canada's privacy authorities issued a number of activity sheets to assist in teaching Grades 1 to 3 students about various privacy issues by presenting them in a visually appealing, easy-to-understand format. The following activity sheets were published in 2019-20:

- Privacy Snakes and Ladders
- Connect the Dots
- Learning About Passwords / Colour the Tablet
- Word Search

The OIPC issued a news release announcing the publication of the activity sheets, and took the opportunity to draw awareness to previously issued lesson plans for students in Grades 6 to 12.

Media Awareness

TRADITIONAL MEDIA

The OIPC saw an uptick in media requests in 2019-20, receiving 95 in 2019-20 compared to 72 in 2018-19.

The following three topics generated the most media requests:

- Alcanna and Patronscan's identification-scanning pilot project after the organizations said publicly that it had been "approved" by the OIPC, despite the OIPC being unaware of the project when it was announced.
- The announcement of a joint investigation into Clearview AI, the facial recognition company. The joint investigation was opened by the OIPC, Office of the Privacy Commissioner of Canada, OIPC for British Columbia and Commission d'accès à l'information du Québec. The use of Clearview AI by the Edmonton Police Service and Calgary Police Service also received media attention.
- The OIPC's "Advisory on Disclosing a Student's Participation in a School Club" and associated news release issued to assist school boards, charter schools and private schools in understanding their obligations to student privacy when deciding whether to disclose a student's participation in a school club, including a gay-straight alliance.

SOCIAL MEDIA

Twitter is used by the OIPC to share orders, investigation reports, publications and news releases, and promote events or raise awareness about access and privacy laws.

The following topics received among the most views or engagements on Twitter:

- The "Advisory on Disclosing a Student's Participation in a School Club" (mentioned above).
- The news release announcing that the Commissioner had opened an investigation under PIPA into Alcanna and Patronscan's pilot project (mentioned above).
- A news release about the publication of lesson plans and activity sheets to help start conversations about privacy with students in younger grades.
- An "Advisory for Phishing" that was released in response to a surge in privacy breaches reported to the OIPC caused by sophisticated phishing attacks.
- Messages about the University of Alberta's Access and Privacy Conference, including one recognizing the presence of other Canadian Commissioners in Alberta and another about a presentation the OIPC made with Alberta Health about the first year of mandatory breach reporting under HIA.

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

Publications

The OIPC issued the following resources in 2019-20:

- Advisory for Phishing (June 2019)
- Advisory for Communicating with Patients Electronically (June 2019)
- Advisory on Disclosing a Student's Participation in a School Club (June 2019)
- Activity Sheets, Lesson Plans for Students (August 2019)
  - Privacy Snakes and Ladders
  - Connect the Dots
  - Learning About Passwords
  - Word Search
- Privacy in a Pandemic (March 2020)

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 (the OIPC), which comprise the statement of financial position as at March 31, 2020, 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 OIPC as at March 31, 2020, 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 OIPC 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 OIPC'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 OIPC'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 OIPC'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 OIPC'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 OIPC 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 16, 2020
Edmonton, Alberta

Financial Statements

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
STATEMENT OF OPERATIONS

Year ended March 31, 2020

	2020		2019
	Budget	Actual	Actual
Revenues			
Prior Year Expenditure Refund	$ -	$ 33	$ 533
Other Revenue	-	1,075	157
	-	1,108	690
Expenses – Directly Incurred (Note 3b)			
Salaries, Wages, and Employee Benefits	$ 6,342,243	$ 5,469,871	$ 5,151,582
Supplies and Services	1,235,428	1,309,299	1,672,129
Amortization of Tangible Capital Assets (Note 5)	51,000	22,369	50,591
Total Program-Operations	7,628,671	6,801,539	6,874,302
Net Cost of Operations	$ (7,628,671)	$ (6,800,431)	$ (6,873,612)

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, 2020

	2020	2019
Financial Assets		
Cash	$ 200	$ 200
Accounts Receivable	112	10
	312	210
Liabilities		
Accounts Payable and Accrued Liabilities	313,897	190,440
Accrued Vacation Pay	493,589	461,903
	807,486	652,343
Net Debt	(807,174)	(652,133)
Non-Financial Assets		
Tangible Capital Assets (Note 5)	97,255	63,615
Prepaid Expenses	9,509	30,538
	106,764	94,153
Net Liabilities	$ (700,410)	$ (557,980)
Net Liabilities at Beginning of Year	$ (557,980)	$ (678,503)
Net Cost of Operations	(6,800,431)	(6,873,612)
Net Financing Provided from General Revenues	6,658,001	6,994,135
Net Liabilities at End of Year	$ (700,410)	$ (557,980)

Contractual obligations (Note 7)

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, 2020

	2020		2019
	Budget	Actual	Actual
Net Cost of Operations	$ (7,628,671)	$ (6,800,431)	$ (6,873,612)
Acquisition of Tangible Capital Assets (Note 5)		(56,009)	-
Amortization of Tangible Capital Assets (Note 5)	51,000	22,369	50,591
Decrease/(Increase) in Prepaid Expenses		21,029	(16,932)
Net Financing Provided from General Revenues		6,658,001	6,994,135
(Increase)/Decrease in Net Debt		(155,041)	154,182
Net Debt, Beginning of Year		(652,133)	(806,315)
Net Debt, End of Year		$ (807,174)	$ (652,133)

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, 2020

	2020	2019
Operating Transactions		
Net Cost of Operations	$ (6,800,431)	$ (6,873,612)
Non-cash Items Included in Net Cost of Operations		
Amortization of Tangible Capital Assets (Note 5)	22,369	50,591
	(6,778,062)	(6,823,021)
(Increase)/Decrease in Accounts Receivable	(102)	2,480
Decrease/(Increase) in Prepaid Expenses	21,029	(16,932)
Increase/(Decrease) in Accounts Payable and Accrued Liabilities	155,143	(156,662)
Cash Applied to Operating Transactions	(6,601,992)	(6,994,135)
Capital Transactions		
Acquisition of Tangible Capital Assets (Note 5)	(56,009)	-
Financing Transactions		
Net Financing Provided from General Revenues	6,658,001	6,994,135
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, 2020

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 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

Reporting Entity

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.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2020

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.

Basis of Financial Reporting

a) Revenue

All revenues are reported on the accrual basis of accounting.

b) Expenses

Expenses are reported on an accrual basis. 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.

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.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2020

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

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 includes 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, 2020.

Note 4 Future Accounting Changes

The Public Sector Accounting Board has approved the following accounting standards:

- PS 3280 Asset Retirement Obligations (effective April 1, 2021)
  This standard provides guidance on how to account for and report liabilities for retirement of tangible capital assets.
- PS 3400 Revenue (effective April 1, 2022)
  This standard provides guidance on how to account for and report on revenue, and specifically, it addresses revenue arising from exchange transactions and unilateral transactions.

Management is currently assessing the impact of these standards on the financial statements.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2020

Note 5 Tangible Capital Assets

	Office Equipment and Furniture	Computer Hardware and Software	2020 Total	2019 Total
Estimated Useful Life	5 years	5 years		
Historical Cost				
Beginning of Year	$ 83,318	$ 452,343	$ 535,661	$ 535,661
Additions	15,681	40,328	56,009	-
Disposals	(12,553)	-	(12,553)	
	$ 86,446	$ 492,671	$ 579,117	$ 535,661
Accumulated Amortization				
Beginning of Year	$ 79,639	$ 392,407	$ 472,046	$ 421,455
Amortization Expense	3,941	18,428	22,369	50,591
Disposals	(12,553)	-	(12,553)	
	$ 71,027	$ 410,835	$ 481,862	$ 472,046
Net Book Value at March 31, 2020	$ 15,419	$ 81,836	$ 97,255	$
Net Book Value at March 31, 2019	$ 3,679	$ 59,936	$	$ 63,615

Financial Statements

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2020

Note 6 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 $660,040 for the year ended March 31, 2020 (2019 – $666,011).

At December 31, 2019, the Management Employees Pension Plan reported a surplus of $1,008,135,000 (2018 - surplus $670,700,000) and the Public Service Pension Plan reported a surplus of $2,759,320,000 (2018 – surplus $519,218,000). At December 31, 2019 the Supplementary Retirement Plan for Public Service Managers had a deficit of $44,698,000 (2018 - deficit $70,310,000).

The Office also participates in a multi-employer Long Term Disability Income Continuance Plan. At March 31, 2020, the Management, Opted Out and Excluded Plan reported an actuarial surplus of $11,635,000 (2019 – surplus $24,642,000). The expense for this plan is limited to employer's annual contributions for the year.

Note 7 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.

	2020	2019
Obligations under operating leases and contracts	$ 11,681	$ 18,955

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

	Total
2020-21	$ 10,501
2021-22	1,180
	$ 11,681

Note 8 Comparative Figures

Certain 2019 figures have been reclassified to conform to the 2020 presentation.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2020

Note 9 Budget

The budget shown on the statement of operations is based on the budgeted expenses that the all-party Standing Committee on Legislative Offices approved on November 30, 2018. The following table compares the office's actual expenditures, excluding non-voted amounts such as amortization, to the approved budgets:

	Voted Budget	Actual	Unexpended (Over-expended)
Operating expenditures	$ 7,577,671	$ 6,779,170	$ 798,501
Capital investment	-	56,009	(56,009)
	$ 7,577,671	$ 6,835,179	$ 742,492

Note 10 Approval of Financial Statements

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

Financial Statements

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

SCHEDULE 1 - SALARY AND BENEFITS DISCLOSURE

Year ended March 31, 2020

	2020			2019
	Base Salary [a]	Other Non-cash Benefits [b][c]	Total	Total
Senior Official				
Information and Privacy Commissioner	$ 244,610	$ 60,836	$ 305,446	$ 304,471

[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 $6,891 (2019: $6,248) being the lease, fuel, insurance and maintenance expenses for an automobile provided by the Office.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
SCHEDULE 2 - RELATED PARTY TRANSACTIONS

Year ended March 31, 2020

Related parties are those entities consolidated or accounted for on the modified equity basis in the Government of Alberta's Consolidated financial statements. Related parties also include key management personnel and close family members of those individuals in the Office. The Office and its employees paid or collected certain taxes and fees set by regulations for premiums, licenses and other charges. These amounts were incurred in the normal course of business, reflect charges applicable to all users, and have been excluded from this schedule.

The Office of the Information and Privacy Commissioner had the following transactions with related parties recorded on the Statement of Operations and the Statement of Financial Position at the amount of consideration agreed upon between the related parties:

	Other Entities	
	2020	2019
Expenses - Directly Incurred		
Alberta Risk Management Fund	$ 3,709	$ 3,758
Postage	11,395	10,937
Information Services	62	-
Technology Services	28,400	17,200
Consumption	3,149	2,937
Fleet vehicle	5,412	5,412
	$ 52,127	$ 40,244

Financial Statements

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

SCHEDULE 2 - RELATED PARTY TRANSACTIONS *(continued)*

Year ended March 31, 2020

The Office of the Information and Privacy Commissioner also had the following transactions with related parties for which no consideration was exchanged. The amounts for these related party transactions are estimated based on the costs incurred by the service provider to provide the service. These amounts are not recorded in the financial statements but are disclosed in Schedule 3.

	Other Entities	
	2020	2019
Expenses - Incurred by Others		
Accommodation Costs	$ 447,481	$ 500,790
Telephone Costs	16,680	18,620
Business Services	51,000	42,000
	$ 515,161	$ 561,410

SCHEDULE 3 - ALLOCATED COSTS

Year ended March 31, 2020

	2020					2019
	Expenses - Incurred by Others					
Program	Expenses [a]	Accommodation Costs [b]	Telephone Costs [c]	Business Services [d]	Total Expenses	Total Expenses
Operations	$ 6,801,539	$ 447,481	$ 16,680	$ 51,000	$ 7,316,700	$ 7,435,712

[a] Expenses - Directly Incurred as per Statement of Operations which include related party transactions as disclosed in Schedule 2.
[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, 2019 to March 31, 2020

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 Collect Indirectly	Request for Information	Request for Review	Request for Review 3rd Party	Request Time Extension	Self-reported Breach	Total
Agencies																	**0**
Boards			6					19		3			12	1	2	6	**49**
Colleges								1					1			10	**12**
Commissions			2							2		3	4	1	1	1	**14**
Committees																	**0**
Federal Departments																	**0**
Foundations																	**0**
Government Ministries/Departments			8			3	1			9		2	76	12	177	24	**312**
Health Quality Council of Alberta																	**0**
Hospital Board (Covenant Health)																	**0**
Law Enforcement Agencies		3	8			1	7	8		1		2	43		3		**76**
Legislative Assembly Office																	**0**
Local Government Bodies												1	2			15	**18**
Municipalities		3	13			1	1			5		5	62	7	25	15	**137**
Nursing Homes																	**0**
Office of the Premier/ Alberta Executive Council													5		6		**11**
Officers of the Legislature			1									1					**2**
Panels																	**0**
Regional Health Authorities (Alberta Health Services)			2							2			8	1			**13**
School Districts	1	1	5			1		1					14	1	4	16	**44**
Universities										1			15		11	1	**28**
Other						1							9		2	7	**19**
Total	**1**	**7**	**45**	**0**	**0**	**7**	**9**	**29**	**0**	**23**	**0**	**14**	**251**	**23**	**231**	**95**	**735**

Note: The statistics do not include Intake cases.

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

Statistics are from April 1, 2019 to March 31, 2020

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)														**0**
Associations, Boards, Councils, Committees, Commissions, Panels or Agencies, created by Custodians												1		**1**
Chiropractors								124				2		**126**
Dental Hygienists								15				1		**16**
Dentists			2					309		1		1		**313**
Denturists														**0**
Government Ministries/Departments									1					**1**
Health Professional Colleges and Associations								3	2			2		**7**
Health Quality Council of Alberta														**0**
Hospital Board (Covenant Health)			3					2	1			19		**25**
Long Term Care Centres								1				3		**4**
Midwives								9						**9**
Minister of Health (Alberta Health)						1		15				35		**51**
Nursing Homes														**0**
Opticians														**0**
Optometrists								39						**39**
Pharmacies/Pharmacists			9					217	3	1		231		**461**
Physicians			26			1		542	23	5		167		**764**
Podiatrists								1						**1**
Primary Care Networks								15	1			13		**29**
Regional Health Authorities (Alberta Health Services)			21			3		96	3	10		414		**550**
Registered Nurses								35				1		**36**
Research Ethics Boards														**0**
Researchers												1		**1**
Subsidiary Health Corporations			2				2	1				40		**45**
Universities/Faculties of Medicine								1						**1**
Other			1			2	13	3	4			7		**30**
Total	**0**	**0**	**64**	**0**	**0**	**7**	**0**	**18**	**1,428**	**38**	**17**	**0**	**938**	**2,510**

Note: The statistics do not include Intake cases.

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

Statistics are from April 1, 2019 to March 31, 2020

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			2										6		**8**
Admin & Support Services									1				5		**6**
Agriculture, Forestry, Fishing & Hunting													1		**1**
Arts, Entertainment & Recreation			4							1			11		**16**
Child Daycare Services													2		**2**
Collection Agencies													4		**4**
Construction			1										7		**8**
Credit Bureaus													1		**1**
Credit Unions											1		15		**16**
Dealers in Automobiles											1		2		**3**
Educational Services													2		**2**
Finance			3			2			1		1		40		**47**
Health Care & Social Assistance			1			2			1		1	1	19		**25**
Information & Cultural Industries			7							1			12		**20**
Insurance Industry			2							1	2		29		**34**
Investigative & Security Services															**0**
Legal Services			4								1		11		**16**
Management of Companies & Enterprises													1		**1**
Manufacturing													7		**7**
Medical & Diagnostic Laboratories						1							2		**3**
Mining, Oil & Gas			2								3		13		**18**
Nursing Homes/Home Health Care													1		**1**
Private Health Care & Social Assistance			1								3		5		**9**
Professional, Scientific & Technical			2			1				3	1		15		**22**
Public Administration			1							2			2		**5**
Real Estate, Rental, Leasing			11								3		6		**20**
Retail			3			2				1	2		28		**36**
Trades/Contractors													1		**1**
Transportation													11		**11**
Utilities			1								1		3		**5**
Wholesale Trade													13		**13**
Other		1	7							3	5		36		**52**
Total	**0**	**1**	**52**	**0**	**0**	**8**	**0**	**0**	**3**	**1**	**11**	**25**	**1**	**311**	**413**

Note: The statistics do not include Intake cases.

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

Statistics are from April 1, 2019 to March 31, 2020

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 Collect Indirectly	Request for Information	Request for Review	Request for Review 3rd Party	Request Time Extension	Self-reported Breach	Total
Agencies																	**0**
Boards			9					19		1			4	2	2	3	**40**
Colleges			1					1		1			3			8	**14**
Commissions			2							1		2	3			1	**9**
Committees																	**0**
Federal Departments										1							**1**
Foundations													1				**1**
Government Ministries/Departments			12			4	1		2	7		1	81	30	166	21	**325**
Health Quality Council of Alberta																	**0**
Hospital Board (Covenant Health)																	**0**
Law Enforcement Agencies		1	8					8				2	39		5		**63**
Legislative Assembly Office																	**0**
Local Government Bodies			1									2	1			8	**12**
Municipalities			17			4	1			3		2	60	13	26	15	**141**
Nursing Homes																	**0**
Office of the Premier/Alberta Executive Council													6		6		**12**
Officers of the Legislature			1										1				**2**
Panels																	**0**
Regional Health Authorities (Alberta Health Services)		2	5										13	2			**22**
School Districts	1		5					1				1	20		5	11	**44**
Universities													3		10	5	**18**
Other										1			4		2	12	**19**
Total	**1**	**3**	**61**	**0**	**0**	**8**	**2**	**29**	**2**	**15**	**0**	**10**	**239**	**47**	**222**	**84**	**723**

Note: The statistics do not include Intake cases.

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

Statistics are from April 1, 2019 to March 31, 2020

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)														**0**
Associations, Boards, Councils, Committees, Commissions, Panels or Agencies, created by Custodians														**0**
Chiropractors								97						**97**
Dental Hygienists								9						**9**
Dentists			1					276		2		5		**284**
Denturists														**0**
Government Ministries/Departments														**0**
Health Professional Colleges and Associations														**0**
Health Quality Council of Alberta														**0**
Hospital Board (Covenant Health)								3	1	2		6		**12**
Long Term Care Centres												2		**2**
Midwives														**0**
Minister of Health (Alberta Health)								5	2	1		24		**32**
Nursing Homes														**0**
Opticians														**0**
Optometrists								13						**13**
Pharmacies/Pharmacists			5			1		196	1			164		**367**
Physicians			11			3		386	29	5		134		**568**
Podiatrists								2						**2**
Primary Care Networks								16	2			13		**31**
Regional Health Authorities (Alberta Health Services)		1	14		1	1		26	2	5		313		**363**
Registered Nurses								20				1		**21**
Research Ethics Boards														**0**
Researchers												1		**1**
Subsidiary Health Corporations												26		**26**
Universities/Faculties of Medicine														**0**
Other							9	1	7			6		**23**
Total	**0**	**1**	**31**	**0**	**1**	**5**	**0**	**9**	**1,050**	**44**	**15**	**0**	**695**	**1,851**

Note: The statistics do not include Intake cases.

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

Statistics are from April 1, 2019 to March 31, 2020

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			2								1		9		**12**
Admin & Support Services			1						1		1		5		**8**
Agriculture, Forestry, Fishing & Hunting													1		**1**
Arts, Entertainment & Recreation			1							1	1		12		**15**
Child Daycare Services			3								2		4		**9**
Collection Agencies			1										2		**3**
Construction											2		3		**5**
Credit Bureaus			1										1		**2**
Credit Unions			3										10		**13**
Dealers in Automobiles											2		3		**5**
Educational Services										3	1		4		**8**
Finance			1			1			1		2		27		**32**
Health Care & Social Assistance			3						1			1	23		**28**
Information & Cultural Industries	1		6							1			8		**16**
Insurance Industry			6						1		2	4	19		**32**
Investigative & Security Services															**0**
Legal Services			6								1		9		**16**
Management of Companies & Enterprises													1		**1**
Manufacturing										1			10		**11**
Medical & Diagnostic Laboratories											1		2		**3**
Mining, Oil & Gas			9								5		10		**24**
Nursing Homes/Home Health Care			1										1		**2**
Private Health Care & Social Assistance			2								3				**5**
Professional, Scientific & Technical			3						1	2	1		14		**21**
Public Administration			1							1					**2**
Real Estate, Rental, Leasing			10								3		5		**18**
Retail			3			1				2			29		**35**
Trades/Contractors			1								1		1		**3**
Transportation			5										6		**11**
Utilities			1												**1**
Wholesale Trade			1										12		**13**
Other			12						1	2	4		20		**39**
Total	**1**	**0**	**83**	**0**	**0**	**2**	**0**	**0**	**6**	**1**	**14**	**35**	**1**	**251**	**394**

Note: The statistics do not include Intake cases.

APPENDIX C: ORDERS, DECISIONS AND PUBLIC INVESTIGATION REPORTS ISSUED

Statistics are from April 1, 2019 to March 31, 2020

FOIP Respondent	Orders	Decisions	Public Investigation Reports	Total
Alberta Emergency Management Agency	1			1
Alberta Health Services	2			2
ATB Financial	1			1
Calgary Police Service	3			3
City of Edmonton	1			1
Community and Social Services	2			2
County of Two Hills	1			1
Edmonton Catholic School District No. 7	1			1
Edmonton Public School District No. 7	1			1
Grande Prairie School Division	1			1
Health	4			4
Infrastructure	1			1
Justice and Solicitor General	7		1	8
Labour and Immigration	1			1
Municipal Affairs	1			1
Municipal District of Opportunity No. 17	1			1
NorQuest College	1			1
Peace River School Division No. 10	2			2
Regional Municipality of Wood Buffalo	1			1
Service Alberta	1			1
Thorhild County	1			1
Workers' Compensation Board	2			2
Subtotal	37	0	1	38

HIA Respondent	Orders	Decisions	Public Investigation Reports	Total
Alberta Health Services	3			3
Covenant Health	1			1
Dr. Klaus D. Gendemann	1			1
Dr. Peter Idahosa			1	1
Saeed Sattari	1			1
Somayeh Pharmacy Ltd.	1			1
Subtotal	7	0	1	8

PIPA Respondent	Orders	Decisions	Public Investigation Reports	Total
De Beers Canada Inc.	1			1
Manulife Financial	1			1
Nal Resources Management Ltd.	1			1
Primco Dene (EMS) Ltd.	1			1
Servus Credit Union Ltd.	2			2
The Co-operators Group Limited	1			1
Worley Parsons Canada	1			1
YWCA Calgary	1			1
Subtotal	9	0	0	9
Total	53	0	2	55

Total of number of Orders, Decisions, and Investigation Reports Issued:
FOIP Orders: 37 (41 cases)
FOIP Decisions: 0
HIA Orders: 7 (7 cases)
HIA Decisions: 0
PIPA Orders: 9 (12 cases)
PIPA Decisions: 0
FOIP Investigation Reports: 1 (1 case)
HIA Investigation Reports: 1 (1 case)

Notes:

(1) This table contains all Orders and Decisions released by the OIPC whether the issuance of the Order or Decision concluded the matter or not.

(2) 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.

(3) 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.

(4) Only Investigation Reports that are publicly released are reported.

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

www.oipc.ab.ca