



Office of the Information and  
Privacy Commissioner of Alberta

**ANNUAL REPORT**  
— 2021-22 —



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](mailto:generalinfo@oipc.ab.ca)  
Twitter: @ABoipc

**[www.oipc.ab.ca](http://www.oipc.ab.ca)**

NOVEMBER 2022

# Table of Contents

<b>Commissioner's Message</b> .....	<b>5</b>	<b>Regulation and Enforcement</b> .....	<b>32</b>
<b>About the Office</b> .....	<b>7</b>	Investigation Reports.....	32
Mandate .....	8	Mediation and Investigation.....	35
Organizational Structure .....	10	Requests for Time Extensions by Public Bodies .....	37
Request for Review and Complaint Process .....	11	Privacy Impact Assessment Reviews.....	38
OIPC as a Public Body .....	12	Privacy Breaches.....	39
Financial Overview.....	14	Offence Investigations under HIA .....	42
<b>Trends and Issues</b> .....	<b>15</b>	Summary of Significant Decisions .....	42
COVID-19 Pandemic.....	16	Judicial Reviews and Other Court Decisions.....	45
Synthetic Data.....	18	<b>Education and Outreach</b> .....	<b>47</b>
Open Banking and Fintech .....	20	Speaking Engagements.....	48
<b>By the Numbers</b> .....	<b>23</b>	Collaboration with Other Jurisdictions.....	48
Highlights Page .....	24	Media Awareness.....	49
Graph A: Total Cases Opened.....	25	<b>Financial Statements</b> .....	<b>51</b>
Graph B: Total Cases Closed .....	25	<b>Appendices</b> .....	<b>69</b>
Table 1: Cases Opened by Case Type .....	26	Appendix A: Cases Opened under FOIP, HIA, PIPA by Entity Type.....	70
Table 2: Cases Closed by Case Type .....	27	Appendix B: Cases Closed under FOIP, HIA, PIPA by Entity Type.....	73
Table 3: Cases Closed by Resolution Method.....	28	Appendix C: Orders, Decisions and Public Investigation Reports Issued.....	76
Graph C: Percentage of Cases Closed by Resolution Method.....	29		
Table 4: General Enquiries .....	29		

# Commissioner's Message



In last year's Annual Report message, I confirmed that my second five-year term as Alberta's Information and Privacy Commissioner was coming to an end on January 31, 2022, and I was not seeking reappointment.

Section 46 of FOIP, however, provides that, "A person holding office as Commissioner continues to hold office after the expiry of that person's term of office until... a successor is appointed or a period of 6 months has expired, whichever occurs first." As no successor had been appointed by the end of my term, I continued in the role into early 2022-23.<sup>1</sup>

As always, it was a busy year! OIPC staff closed a record number of files, with 3,989 total cases closed, representing a 13% increase over 2020-21.

For the first time since 2015-2016, however, the number of new cases opened decreased, mainly because fewer breaches were reported under HIA.

The decrease in HIA breach reports was expected, as custodians became more familiar with legislated reporting requirements. When mandatory breach reporting requirements were introduced in 2018, the OIPC noticed custodians were reporting health information breaches out of an abundance of caution and many that were sent to the OIPC may not have met the reporting requirements.

An advantage of fewer new cases was that it allowed OIPC staff to focus on reducing the backlog. Definite progress was made. For example, 1,000 HIA breach reports were closed, representing a 48% increase over the previous year.

<sup>1</sup> Commissioner Jill Clayton's term officially ended on July 31, 2022.

Time extension decisions issued to public bodies also increased the OIPC's closed case count. In total, 375 time extension decisions were made, representing a 24% increase over 2020-21. This is a satisfying statistic from my perspective as Commissioner. I am pleased we were able to turn these matters around quickly.

Time extension statistics, however, highlight that public bodies are not responding to access requests in a timely fashion. The OIPC saw a new high-water mark for time extension requests. There were 398 time extension requests received in 2021-22, representing a 35% increase over 2020-21.

The pandemic is an obvious factor contributing to delays, but likely not the only one. As I said in last year's message, public bodies are seeing staff shortages, unfilled vacancies, and large and complicated requests. In 2012-13, my first full year as Commissioner, the OIPC received 68 time extension requests. Clearly those days are long behind us.

If the number of time extension requests is the canary in the coal mine indicating an access to information system in crisis then the alarm has been sounded. These issues cry out for urgent attention.

There are also urgent issues in privacy.

Investigation reports issued by the OIPC in 2021-2022, including investigations completed in conjunction with our colleagues in other jurisdictions, highlight the revolutionary and disruptive impacts of technology. There are definite advancements with new technologies, but they also bring the potential to cause significant harms if not designed and implemented with respect for personal information at their core.

Last year I wrote about new health technology systems, and the rapid implementation of virtual care systems. This continued in 2021-22.

In my view, we are now seeing the start of one of the most significant trends of my decade as Commissioner. In particular, we are seeing situations where the purposes for which health custodians collect and use health information overlap and potentially conflict with the purposes of their private sector information managers and service providers. The Babylon by Telus Health investigations, completed under Alberta's HIA and PIPA, highlight these issues but are by no means a unique example.

These and other technology issues – de-identification, open banking, synthetic data, biometrics and artificial intelligence, to name a few continuing and emerging trends – reinforce the need to modernize privacy laws to ensure they are fit for purpose. Modern, rigorous privacy laws are a required foundation to support innovation and to generate public trust in governments and private sector.

The next years promise to be full of challenges and opportunities, with access and privacy matters front and centre throughout. I am sincerely honoured and grateful to have had the opportunity to serve 10 years as Information and Privacy Commissioner of Alberta, and I offer my support and best wishes to Alberta's fourth Commissioner, Diane McLeod, as well as all the staff of the OIPC. Albertans and regulated entities will be well served.

*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) applies to 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.

FOIP 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.

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

## ***Personal Information Protection Act***

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

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

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

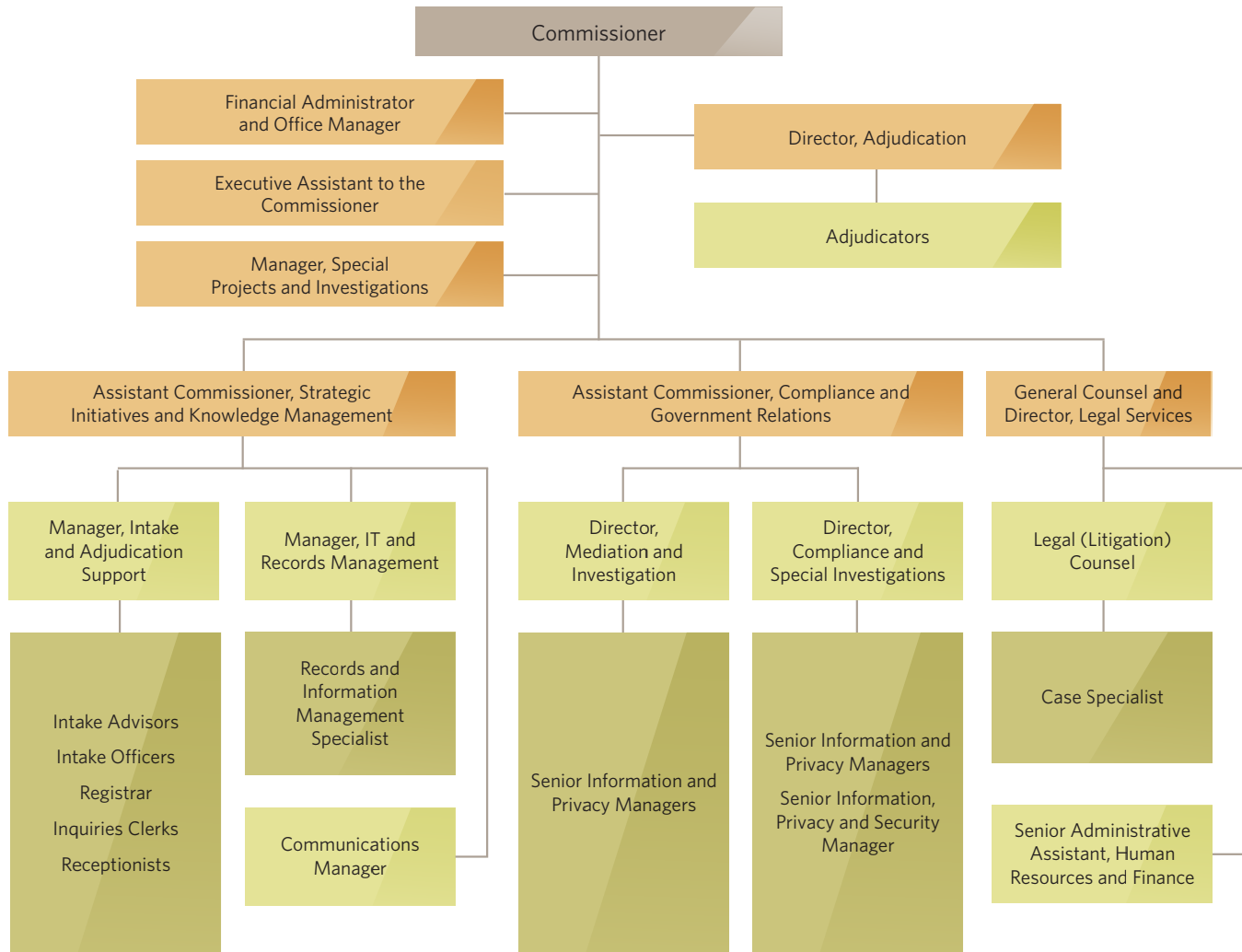
## MISSION

Our work toward supporting our vision includes:

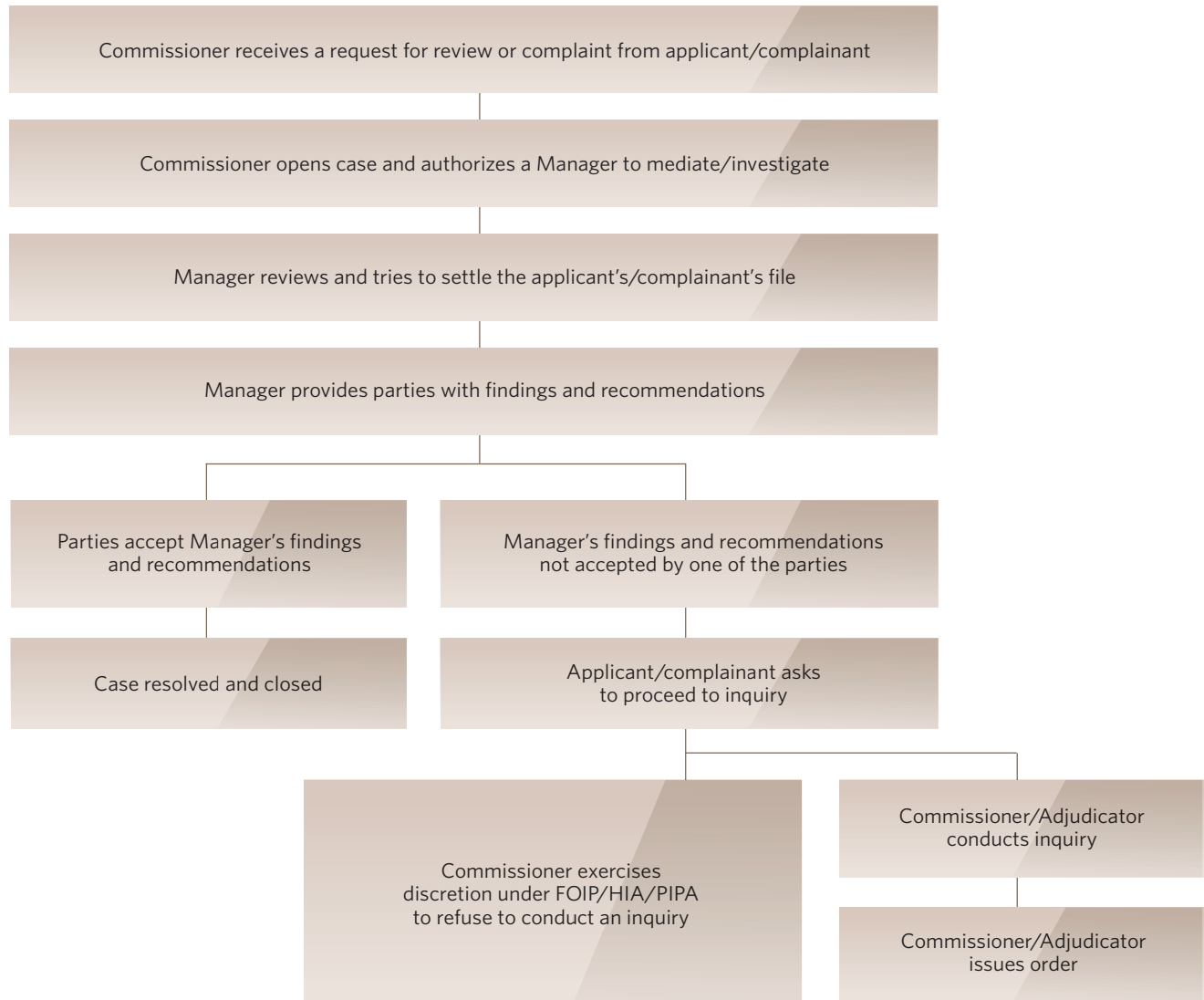
- Advocating for the access and privacy rights of Albertans
- Ensuring public bodies, health custodians and private sector organizations uphold the access and privacy rights contained in the laws of Alberta
- Providing fair, independent and impartial reviews in a timely and efficient manner



# Organizational Structure



# Request for Review and Complaint Process



# OIPC as a Public Body

## FOIP REQUESTS TO THE OIPC

As a public body under FOIP, the OIPC receives access requests on occasion. In 2021-22, the OIPC received two general information requests under FOIP. The OIPC responded to both 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 responded to the access request, such as properly excluding records subject to the access request.

On November 9, 2021, an External Adjudicator issued Adjudication Order #13, available at [www.oipc.ab.ca](http://www.oipc.ab.ca). The Commissioner was found to have properly excluded records requested by the applicant as the records related to the statutory functions of an Officer of the Legislature under FOIP.

As of March 31, 2022, there was one outstanding request for review awaiting the appointment of an External Adjudicator.

## OIPC PRIVACY MATTERS

In 2021-22, the OIPC conducted five investigations into internal incidents involving potential privacy breaches.

### Incident 1

The OIPC sent a request for review to the wrong public body. The request for review contained the applicant's personal information. The OIPC retrieved the request for review from the public body. As the public body was experienced in the requirements of FOIP not to disclose personal information, there was no real risk of significant harm, and no notification was required.

### Incident 2

The OIPC could not locate paper documents that a complainant delivered to the OIPC. The documents contained the complainant's personal information. The OIPC notified the complainant about the internal loss of the documents containing the complainant's personal information.

### Incident 3

The OIPC sent a request for review to the wrong organization. The request for review contained the requester's personal information. The OIPC retrieved the request for review from the organization. As the organization was experienced in the requirements of PIPA not to disclose personal information, there was no real risk of significant harm, and no notification was required.

#### Incident 4

The OIPC sent complaint documents in error to another individual. The documents contained the complainant's personal information. When the OIPC tried to retrieve the documents from the individual, the individual said that she had moved and had not received the documents. Canada Post did not return the documents to the OIPC. The OIPC notified the complainant about the loss of the documents containing the complainant's personal information.

#### Incident 5

The OIPC sent complaint documents to the wrong custodian. The documents contained the personal information of the complainant and the other custodian, as well as the first name of the other custodian's receptionist and the phone numbers of several persons contained in text messages from those individuals to the other custodian's receptionist.

When the OIPC tried to retrieve the documents, the custodian to whom the documents were sent in error said that he did not receive the documents. That custodian's receptionist could not remember seeing the package in which the documents were contained, but thought that she had probably shredded the documents. Canada Post did not return the documents to the OIPC.

The OIPC determined that if the documents had been shredded, there was no real risk of significant harm and no notification was required. Even if the documents had not been shredded, the custodian to whom the documents were sent in error would be aware of the requirements to maintain the privacy of the personal information contained therein, there would be no real risk of significant harm, and no notification was required.

Nevertheless, the OIPC apologized to the complainant and the other custodian when it provided acknowledgement packages to them that identified them as the correct parties to the review.

## 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 Commissioners and Directors every second month. The disclosures are available at [www.oipc.ab.ca](http://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 2020 calendar year, the threshold was adjusted to \$135,317. Other non-monetary employer-paid benefits and pension are also reported.

This disclosure is made annually by June 30 and is available at [www.oipc.ab.ca](http://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 (Whistleblower Protection) Act* in 2021-22.

# Financial Overview

In 2021-22, the total approved budget for the OIPC was \$7,053,000, including the supplementary estimate.<sup>2</sup> The total cost of operating expenses and capital purchases was \$7,047,413. The OIPC returned \$5,587 to the Legislative Assembly.

## TOTAL ACTUAL COSTS COMPARED TO BUDGET

	VOTED BUDGET	SUPPLEMENTARY ESTIMATE	ADJUSTED VOTED BUDGET	ACTUAL	DIFFERENCE
Operating Expenses*	\$ 6,998,000	\$ 55,000	\$ 7,053,000	\$ 7,015,537	\$ 37,463
Capital Purchases	-	-	-	31,876	(31,876)
<b>Total</b>	<b>\$ 6,998,000</b>		<b>\$ 7,053,000</b>	<b>\$ 7,047,413</b>	<b>\$ 5,587</b>

\*Amortization is not included

## TOTAL ACTUAL COSTS COMPARED TO PRIOR YEAR

	2021-2022	2020-2021	DIFFERENCE
Operating Expenses	\$ 7,015,537	\$ 7,059,127	\$ (43,590)
Capital Purchases	31,876	155,757	(123,881)
<b>Total</b>	<b>\$ 7,047,413</b>	<b>\$ 7,214,884</b>	<b>\$ (167,471)</b>

Total costs for operating expenses and capital purchases decreased by \$167,471 from the previous year.

<sup>2</sup> In December 2021, the Government of Alberta lifted salary restraint measures for non-union employees under the *Public Service Act*. This resulted in OIPC staff receiving a one-time in-range salary increase retroactive to December 1, 2021, which required a supplementary estimate from the OIPC for approval by the Standing Committee on Legislative Offices. The supplementary estimate was approved in January 2022.

# TRENDS & ISSUES





# COVID-19 Pandemic

Several and varied access to information and privacy issues arose and evolved throughout the COVID-19 pandemic.

Across all sectors, there were practical challenges in transitioning from the office to home. In particular, in the early days of the pandemic, retrieving records became more challenging for public bodies in responding to access requests. There were also several privacy and security concerns with staff transitioning to home en masse, such as increased risks of phishing and immediate deployment of connected technologies.

In the health sector, rapid adoption of virtual healthcare products occurred often without the privacy impact assessments expected when using a new system for interacting with patients.

Contact tracing drew much attention, particularly as many jurisdictions developed apps in an attempt to automate what was an otherwise labour intensive process. Businesses using customer lists to assist contact tracing efforts also raised novel privacy concerns.

While many of these topics faded as pandemic responses changed, virtual healthcare has remained a core component of the OIPC's work. (See the Regulation and Enforcement sections on Babylon by Telus Health and Privacy Impact Assessments for further analysis.)

In 2021-22, the discussion changed once again. Proof of vaccination programs became the primary pandemic privacy topic.

Recognizing the considerable attention on potential proof of vaccination programs and understanding the inherent privacy issues in introducing them, Canada's federal, provincial and territorial privacy commissioners issued in May 2021 a statement on privacy and COVID-19 vaccine passports.<sup>3</sup>

On the same day in May 2021, to assist Alberta businesses, the OIPC issued guidance under PIPA on proof of vaccination programs.<sup>4</sup> The advisory was for organizations that were considering asking for or requiring proof of vaccination from customers in order to receive discounts, access goods or services, or enter a store. The guidance addressed issues such as reasonable purpose for collection, reasonable extent of collection, notice of collection, consent and denial of service, among other privacy considerations. It also quickly became the most viewed OIPC resource on the website – ever.

3 Office of the Privacy Commissioner of Canada. "Privacy and COVID-19 Vaccine Passports: Joint Statement by Federal, Provincial and Territorial Privacy Commissioners". May 19, 2021. Available from [www.priv.gc.ca](http://www.priv.gc.ca).

4 Office of the Information and Privacy Commissioner of Alberta. "COVID-19 Pandemic: Proof of Vaccination". May 2021. Available from [www.oipc.ab.ca](http://www.oipc.ab.ca).

The proof of vaccination advisory preceded the Government of Alberta's Restrictions Exemption Program (REP) that came into effect in September 2021. REP was a version of a proof of vaccination requirement in that eligible businesses opted into REP to serve vaccinated customers in person legally. Many other jurisdictions also implemented versions of proof of vaccination programs.

In fall of 2021, employers began introducing proof of vaccination requirements for employment purposes, which also raised many privacy questions. Despite the debate about employers' vaccination requirements, there were few complaints made to the OIPC. There were, however, federal public servants who complained to the Office of the Privacy Commissioner of Canada about the COVID-19 vaccination requirement.<sup>5</sup>

As restrictions eased and vaccination programs were rescinded in the spring of 2022, the immediate attention on access and privacy issues also faded. What remained, however, were many files and cases making their way through various administrative tribunal, court or parliamentary processes across Canada. For the OIPC, this includes the hundreds of PIAs on virtual care products, the continued influx of time extension requests from public bodies and the various reviews of access request responses on pandemic topics.

5 The Canadian Press. "Privacy czar probing complaints about federal public service vaccination requirement". October 22, 2021. Available from [www.ctvnews.ca](http://www.ctvnews.ca).

# Synthetic Data

Discussion about privacy enhancing technologies to resolve common problems in data projects has increased in recent years, particularly as the calls grow louder to use publicly held information for data-driven innovations in the public, health and private sectors.

Synthetic data is one such privacy enhancing technology that has received plenty of attention. Generating synthetic data has itself become an artificial intelligence or machine learning enabled privacy protective method.<sup>6</sup>

Rather than masking, transforming or making more subtle changes to personal information in datasets – commonly called de-identification – the synthetic data process takes an original or “real” dataset, and creates a new or “fake” dataset with nearly identical statistical relationships. From a privacy standpoint, individual data points no longer relate to a real person. Consequently, the potential applications of synthetic data are numerous.

An area where the OIPC has observed real-world use of synthetic data in Alberta is in a Health Cities project.<sup>7</sup> Health Cities’ synthetic data project is a partnership among Alberta Innovates, Replica Analytics and the University of Alberta. The first phase of the project validated the first synthetic health dataset in Alberta. The second phase is underway and aims to establish use cases for synthetic data in the health system.

Given the highly sensitive nature of individually identifying health information, there is often a reluctance by healthcare professionals to share health information, even if mechanisms in established health information laws enable disclosing health information for research purposes or innovations in healthcare delivery.

Generally, the risk aversion to sharing health information is a good thing on an individual level. People who have their health information breached or disclosed improperly often feel violated and the information can be used against them maliciously.

However, the value of data in healthcare delivery cannot be overstated. Throughout the COVID-19 pandemic, discussion about data availability was paramount. Abroad, the United Nations noted that “insights drawn from aggregated data, which were made public and shareable, played a crucial role” in containing the Ebola outbreak in West Africa.<sup>8</sup>

This is where synthetic data offers promise. Once privacy can be assured – that is, the synthetic dataset cannot be linked back to specific individuals – those datasets can be shared widely, possibly publicly, to assist governments, businesses and healthcare organizations in coming up with innovative ways to think about and act with the data.

6 El Emam, Khaled. “Accelerating AI with synthetic data”. February 26, 2020. Available from [www.iapp.org](http://www.iapp.org).

7 Health Cities is a non-profit established by the City of Edmonton with a mission to deliver innovative healthcare solutions for use across Canada. Health Cities website is at [www.healthcities.ca](http://www.healthcities.ca).

8 United Nations. “Report of the Secretary General: Roadmap for Digital Cooperation”. June 2020. Available from [www.un.org](http://www.un.org).

Importantly, the promise of synthetic data does not mean that the accountability and oversight in privacy laws disappear. Rules remain for the collection, use and disclosure of health or personal information for the original datasets. Contractual parameters would also be required for the use or disclosure of original datasets to create synthetic datasets, which may include requirements on access, consent and notice, data minimization, incident response, information security, among other considerations. Involving independent information and privacy regulators is also encouraged to build public trust, and may be required such as through the submission of a privacy impact assessment under Alberta's HIA.

Many predictions exist about synthetic data's importance for information sharing and data analysis. It is too early to tell if synthetic data will realize its full potential as a privacy enhancing technology for data projects. For now, it remains a privacy topic to follow as governments, healthcare professionals and businesses continue to explore different ways to share information for data-driven innovations.

# Open Banking and Fintech

Over the past year, policy proposals progressed in Alberta and federally with the goal of advancing technology in the finance sector.

In March 2022, the Government of Alberta introduced the *Financial Innovation Act* to the legislature, and said:<sup>9</sup>

The *Financial Innovation Act* establishes a regulatory sandbox for financial services and fintech companies. A regulatory sandbox is a “safe space” in which companies can test innovative products or services, without immediately meeting all regulatory requirements. It also assists companies in collecting information on new products and services to determine if they have value for customers.

Among the changes, the *Financial Innovation Act* enables the Minister of Finance to issue a certificate of acceptance to approved companies, impose terms, conditions and restrictions to provide oversight, and requires public information about participants be published online.

PIPA is one of the laws from which approved participants in the “regulatory sandbox” may be temporarily exempt.

A key feature, however, is that a PIPA exemption requires the approval of the Commissioner and Minister of Service Alberta. Section 8(3) of the *Financial Innovation Act* reads:

8(3) The Minister may exempt a Sandbox Participant from any provision of the *Personal Information Protection Act* or any regulations under that Act

- (a) with the agreement of the Minister responsible for that Act,
- (b) with the prior written approval of the Information and Privacy Commissioner, and
- (c) on terms, conditions and restrictions agreed to jointly by both Ministers and the Information and Privacy Commissioner.

There are additional powers set out in sections 10(4) and 10(5) of the *Financial Innovation Act* with any addition, amendment or revocation of an exemption or certificate from a provision of PIPA requiring approval of the Commissioner, and the power of the Commissioner to revoke a written approval under section 8(3)(b).<sup>10</sup>

As University of Ottawa law professor Teresa Scassa noted in summarizing the *Financial Innovation Act*, “This is an interesting bill, and one to watch as it moves through the legislature in Alberta. Not only is it a model for a *legislated* regulatory sandbox its approach to addressing privacy issues is worth some examination.”<sup>11</sup>

<sup>9</sup> Bill 13, Financial Innovation Act, passed first reading on March 30, 2022 and received Royal Assent on April 29, 2022. The *Financial Innovation Act* came into force on July 1, 2022.

<sup>10</sup> The Government of Alberta started accepting applications on July 4, 2022 for the “Financial services and fintech regulatory sandbox”. Available from [www.alberta.ca](http://www.alberta.ca).

<sup>11</sup> Scassa, Teresa. “Alberta proposes a fintech regulatory sandbox with interesting privacy features”. April 12, 2022. Available from [www.teresascassa.ca](http://www.teresascassa.ca).

Around the same time in March 2022, the Government of Canada moved to the next phase of its open banking project by appointing a project leader tasked with engaging stakeholders to develop an accreditation framework, rules and technical standards, and providing advice to government for the future ongoing administration of an open banking system.<sup>12</sup>

Guided by the principle of data portability, the Government of Canada notes, “In the simplest terms, open banking is a system that allows consumers to share their financial data between financial institutions and accredited third party service providers.”<sup>13</sup>

Whereas the Government of Alberta’s regulatory sandbox is designed for fintech companies to experiment with new products, open banking is meant to facilitate connections between banks and fintech companies. Currently in Canada, regulatory mechanisms do not exist to allow for open banking. As the Government of Canada notes:

The establishment of an open banking system aims to give Canadians and businesses greater control over their financial data and be better equipped to manage their finances. Open banking, or consumer-directed finance, is a system that would enable consumers to transfer their financial data between financial institutions and accredited third parties in a secure and consumer-friendly way.

The appointment of a project lead marked the beginning of phase 3 in the Government of Canada’s pledge to implement open banking. It follows efforts to review open banking in other jurisdictions and with stakeholders in phase 1 and further consultations in phase 2 concluding with a final report to the federal Minister of Finance in April 2021 that provided recommendations on implementing open banking. Phase 3 is for acting on the recommendations set out in the final report and implementing an open banking system.<sup>14</sup>

One of the four open banking working groups involved in phase 3 is dedicated to privacy, “including how consumers provide and revoke consent to share their data, and how consumer data can be used pursuant to the consent provided.”<sup>15</sup> The other three working groups are focused on accreditation, liability and security.

Depending on what is required for successful implementation of these projects, many regulatory changes may soon follow, including much needed modernization of Canada’s privacy laws.

12 Government of Canada. “Open banking implementation”. October 2022. Available from [www.canada.ca](http://www.canada.ca).

13 Government of Canada. “Final Report – Advisory Committee on Open Banking”. April 2021. Available from [www.canada.ca](http://www.canada.ca).

14 Government of Canada. “Open banking”. August 2022. Available from [www.canada.ca](http://www.canada.ca).

15 See citation 12.





# BY THE NUMBERS



## Totals Opened/Closed

(excluding Intake cases)



3,768 total opened files in 2021-22; 4,166 in 2020-21

3,989 total closed files in 2021-22; 3,517 in 2020-21



## Privacy Impact Assessments (PIAs)



under FOIP, HIA and PIPA



## Requests for Review (RfRs) Opened under FOIP

21%

INCREASE IN OPENED RfRs

343 opened RfRs in 2021-22; 283 in 2020-21

## Self-Reported Breaches

957

SELF-REPORTED BREACHES OPENED

under FOIP, HIA and PIPA

1,400

SELF-REPORTED BREACHES CLOSED

under FOIP, HIA and PIPA

## Time Extension Requests under FOIP

35% INCREASE IN TIME EXTENSION REQUESTS UNDER FOIP

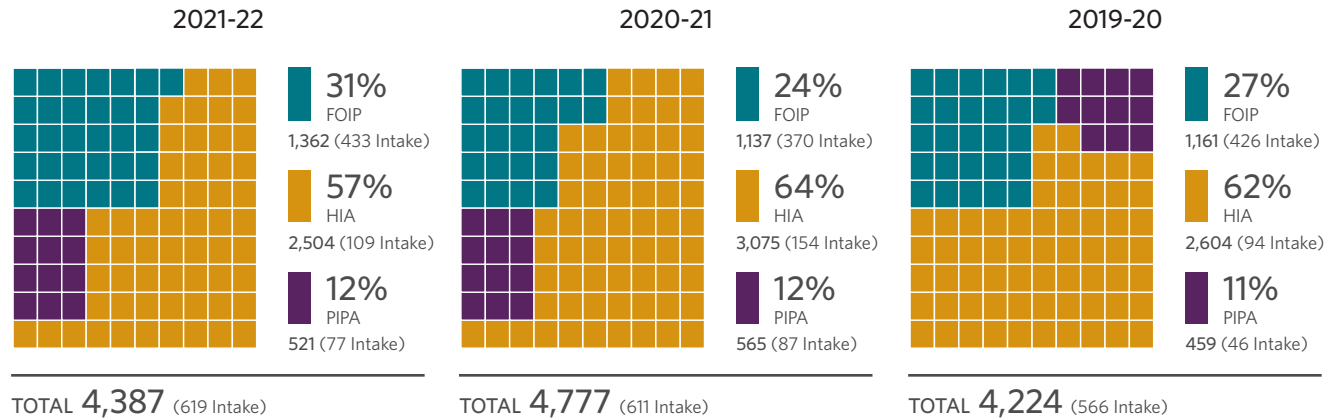
398

time extension requests in 2021-22; 294 in 2020-21



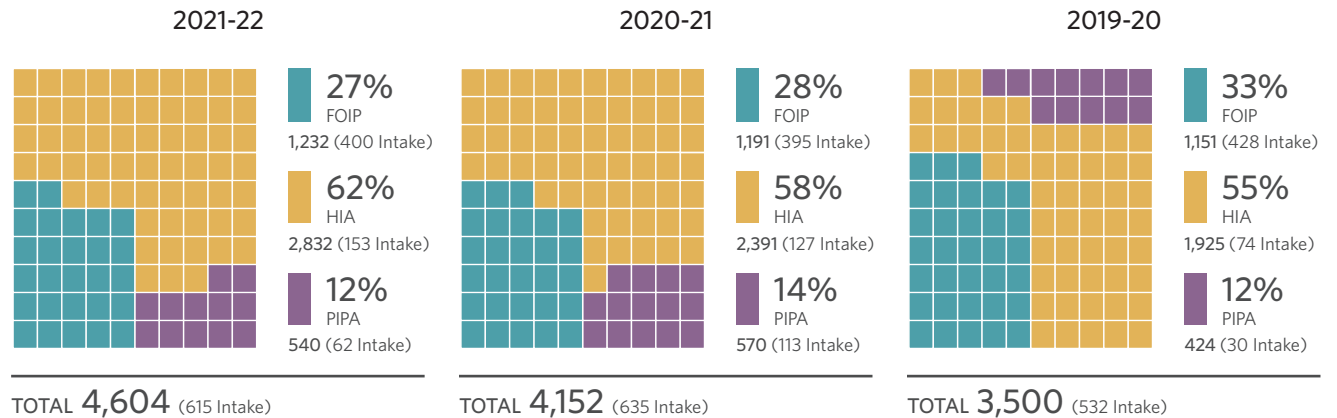
## GRAPH A: TOTAL CASES OPENED

Three Year Comparison



## GRAPH B: TOTAL CASES CLOSED

Three Year Comparison



## TABLE 1: CASES OPENED BY CASE TYPE

FOIP	2021-2022	2020-2021	2019-2020
Advice and Direction	0	0	1
Authorization to Disregard a Request	4	4	7
Complaint	38	28	45
Disclosure to Commissioner (Whistleblower)	0	0	0
Engage in or Commission a Study	0	0	0
Excuse Fee	5	2	7
Investigation Generated by Commissioner	2	4	9
Notification to OIPC	1	7	29
Offence Investigation	0	1	0
Privacy Impact Assessment	10	14	23
Request Authorization to Collect Indirectly	0	0	0
Request for Information	14	9	14
Request for Review	343	283	251
Request for Review 3rd Party	41	40	23
Request Time Extension	398	294	231
Self-reported Breach	73	81	95
<b>Subtotal</b>	<b>929</b>	<b>767</b>	<b>735</b>
Intake cases	433	370	426
<b>Total</b>	<b>1,362</b>	<b>1,137</b>	<b>1,161</b>

HIA	2021-2022	2020-2021	2019-2020
Advice and Direction	0	0	0
Authorization to Disregard a Request	1	0	0
Complaint	48	33	64
Engage in or Commission a Study	0	0	0
Excuse Fee	0	1	0
Investigation Generated by Commissioner	6	19	7
Notification to OIPC	0	0	0
Offence Investigation	17	11	18
Privacy Impact Assessment	1,730	1,888	1,428
Request for Information	23	19	38
Request for Review	19	19	17
Request Time Extension	0	1	0
Self-reported Breach	551	930	938
<b>Subtotal</b>	<b>2,395</b>	<b>2,921</b>	<b>2,510</b>
Intake cases	109	154	94
<b>Total</b>	<b>2,504</b>	<b>3,075</b>	<b>2,604</b>

PIPA	2021-2022	2020-2021	2019-2020
Advice and Direction	0	0	0
Authorization to Disregard a Request	0	1	1
Complaint	38	46	52
Engage in or Commission a Study	0	0	0
Excuse Fee	0	0	0
Investigation Generated by Commissioner	2	7	8
Notification to OIPC	0	0	0
Offence Investigation	0	0	0
Privacy Impact Assessment	11	6	3
Request for Advanced Ruling	0	0	1
Request for Information	7	4	11
Request for Review	52	37	25
Request Time Extension	1	0	1
Self-reported Breach	333	377	311
<b>Subtotal</b>	<b>444</b>	<b>478</b>	<b>413</b>
Intake cases	77	87	46
<b>Total</b>	<b>521</b>	<b>565</b>	<b>459</b>

### Notes

- 1 See Appendix A for a complete listing of cases opened in 2021-22.
- 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	2021-2022	2020-2021	2019-2020
Advice and Direction	1	0	1
Authorization to Disregard a Request	4	1	3
Complaint	36	53	61
Disclosure to Commissioner (Whistleblower)	0	0	0
Engage in or Commission a Study	0	0	0
Excuse Fee	6	11	8
Investigation Generated by Commissioner	3	6	2
Notification to OIPC	1	7	29
Offence Investigation	1	3	2
Privacy Impact Assessment	13	27	15
Request Authorization to Collect Indirectly	0	0	0
Request for Information	15	14	10
Request for Review	286	241	239
Request for Review 3rd Party	31	28	47
Request Time Extension	375	303	222
Self-reported Breach	60	102	84
<b>Subtotal</b>	<b>832</b>	<b>796</b>	<b>723</b>
Intake cases	400	395	428
<b>Total</b>	<b>1,232</b>	<b>1,191</b>	<b>1,151</b>

HIA	2021-2022	2020-2021	2019-2020
Advice and Direction	0	0	0
Authorization to Disregard a Request	0	0	1
Complaint	56	42	31
Engage in or Commission a Study	0	0	0
Excuse Fee	1	0	1
Investigation Generated by Commissioner	7	2	5
Notification to OIPC	0	0	0
Offence Investigation	13	12	9
Privacy Impact Assessment	1,560	1,491	1,050
Request for Information	18	24	44
Request for Review	24	17	15
Request Time Extension	0	1	0
Self-reported Breach	1,000	675	695
<b>Subtotal</b>	<b>2,679</b>	<b>2,264</b>	<b>1,851</b>
Intake cases	153	127	74
<b>Total</b>	<b>2,832</b>	<b>2,391</b>	<b>1,925</b>

PIPA	2021-2022	2020-2021	2019-2020
Advice and Direction	0	0	1
Authorization to Disregard a Request	1	1	0
Complaint	64	66	83
Engage in or Commission a Study	0	0	0
Excuse Fee	0	0	0
Investigation Generated by Commissioner	7	7	2
Notification to OIPC	0	0	0
Offence Investigation	0	0	0
Privacy Impact Assessment	6	4	6
Request for Advanced Ruling	0	1	1
Request for Information	7	4	14
Request for Review	52	36	35
Request Time Extension	1	0	1
Self-reported Breach	340	338	251
<b>Subtotal</b>	<b>478</b>	<b>457</b>	<b>394</b>
Intake cases	62	113	30
<b>Total</b>	<b>540</b>	<b>570</b>	<b>424</b>

### Notes

- 1 See Appendix B for a complete listing of cases closed in 2021-22.
- 2 A listing of all privacy impact assessments accepted in 2021-22 is available at [www.oipc.ab.ca](http://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).

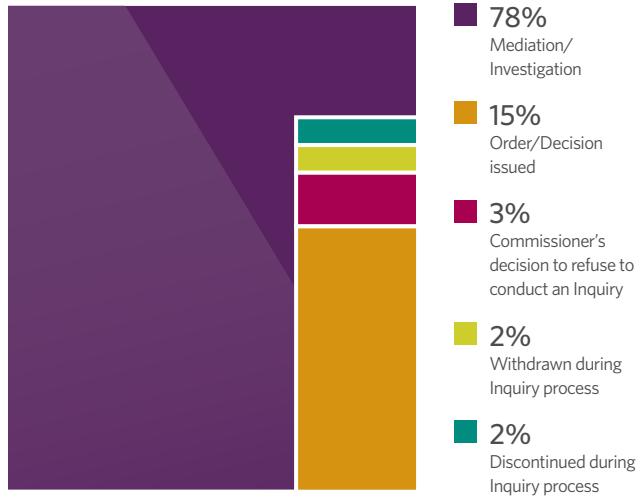
RESOLUTION METHOD	NUMBER OF CASES (FOIP)	NUMBER OF CASES (HIA)	NUMBER OF CASES (PIPA)	TOTAL	%
Mediation/Investigation	346	46	63	455	78%
Order or Decision	59	15	11	85	15%
Commissioner's decision to refuse to conduct an Inquiry	7	2	9	18	3%
Withdrawn during Inquiry process	10	0	2	12	2%
Discontinued during Inquiry process	5	4	5	14	2%
<b>Total</b>	<b>427</b>	<b>67</b>	<b>90</b>	<b>584</b>	<b>100%</b>

FOIP Orders: 57 (59 cases); HIA Orders: 14 (15 cases); PIPA Orders: 11 (11 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 2021-22. Copies of Orders, Decisions and public Investigation Reports are available at [www.oipc.ab.ca](http://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



Of the **584** cases that could proceed to Inquiry:  
**3%** were resolved within 90 days  
**6%** were resolved within 180 days  
**91%** were resolved in more than 180 days

## TABLE 4: GENERAL ENQUIRIES

TELEPHONE CALLS		
FOIP	Number	Percentage
Public Bodies	31	12%
Individuals	230	88%
<b>Total</b>	<b>261</b>	<b>100%</b>

HIA	Number	Percentage
Custodians	287	43%
Individuals	388	57%
<b>Total</b>	<b>675</b>	<b>100%</b>

PIPA	Number	Percentage
Organizations	80	12%
Individuals	598	88%
<b>Total</b>	<b>678</b>	<b>100%</b>

NON-JURISDICTIONAL	151
--------------------	-----

EMAILS FOIP/HIA/PIPA	420
----------------------	-----

<b>Total</b>	<b>2,185</b>
--------------	--------------





# REGULATION & ENFORCEMENT



# Investigation Reports

## BABYLON BY TELUS HEALTH REPORTS ISSUED UNDER HIA AND PIPA

The OIPC opened investigations into the Babylon by Telus Health virtual healthcare app after identifying concerns in separate privacy impact assessments (PIAs) that a physician and Babylon Health Canada Limited had submitted on the app.

The OIPC's investigations found that clinical services offered by physicians through the app were subject to Alberta's HIA, which applies to certain regulated healthcare professions.

Other features of the product – Symptom Checker, Healthcheck and clinical services provided by dietitians and mental health counsellors – were subject to PIPA, Alberta's private sector privacy law.

In total, there were 31 findings and 20 recommendations made in the investigations.

Of particular concern, the investigations found that the collection and use of individuals' government-issued ID and selfie photos through the app for identity verification and fraud prevention by using facial recognition technology was not compliant with PIPA and HIA. With respect to PIPA, Babylon did not establish that it was reasonable to collect this extent of personal information in order to verify identity, and detect and prevent fraud. With respect to HIA, collecting and using copies of government-issued ID and selfie photos from patients through the Babylon app went beyond what was essential to verify identity and provide health services. The OIPC noted that other simpler, effective methods existed for verifying identity that were consistent with provincial and national guidelines.

The HIA investigation also found that collecting (recording) and using audio and video consultations through the Babylon app went beyond what is essential to provide a health service and, again, was not consistent with provincial and national guidelines for providing virtual health care. (Babylon said video recording functionality was disabled in June 2020, but recording audio consultations remained available.) Policies and procedures implemented by the physicians also did not reflect the roles, responsibilities and accountabilities required by HIA.

Many of the findings from the PIPA investigation related to the app's privacy policy, which was found to be unclear, lengthy and contained inaccuracies. For example, the privacy policy did not clearly identify the purposes for which personal information was collected, and it was not clear what information was associated with each purpose. The privacy policy also referred to functionality that was not enabled or available to individuals.

Babylon also did not meet PIPA's requirements to develop policies and practices that included information regarding the countries in which personal information was collected, used, disclosed or stored, and the purposes for which service providers outside of Canada are authorized to collect, use or disclose personal information.

During the investigations, Babylon and the physicians implemented or started introducing some of the recommendations, including discontinuing the practice of recording video consultations. However, despite accepting many recommendations, Babylon said that "it cannot discontinue" its collection and use of government-issued ID and a selfie photo, and it continued to offer audio recordings of consultations with physicians.

In January 2021, the OIPC was advised that, “TELUS acquired the Canadian operations of Babylon Health. The acquisition includes all of the Canadian operations, including the clinic, and we have licensed from Babylon the software platform upon which the virtual service runs. From a privacy perspective, this means that the Babylon operations in Alberta are now part of TELUS and will now be operating under the TELUS privacy program.”

Despite this, the investigations were concerned with the operation and implementation of the app at the time the investigation was initiated in April 2020.

*Investigation Report H2021-IR-01: Investigation into the use of Babylon by TELUS Health by Alberta physicians*

*Investigation Report P2021-IR-02: Investigation into Babylon by TELUS Health’s compliance with Alberta’s Personal Information Protection Act*

“ I support virtual health care solutions and innovations, and I hope the lessons learned from this investigation help other healthcare professionals and organizations take the steps necessary to comply with Alberta’s privacy laws. ”

- Commissioner Jill Clayton, July 29, 2021

## LIQUOR STORE ID-SCANNING PROGRAM REVIEWED

The OIPC opened an investigation of Alcanna Inc.’s use of Servall Data Systems Inc.’s PatronsCan ID-scanning system after the organizations announced their partnership at a news conference. During the news conference and in subsequent media interviews, representatives for the organizations assured reporters that the technology had been “approved” by the OIPC. The OIPC, however, was not aware of the pilot project until it was announced and had not reviewed this use of the technology.

The OIPC learned that Servall relied on a 2009 privacy impact assessment review of its technology as evidence that the technology complied with PIPA, as well as previous investigations of the technology implemented in nightclubs.

However, the OIPC’s decade-old PIA review letter to Servall said, “As you know, the OIPC cannot endorse or even approve Servall’s product as ‘privacy-compliant.’” Additionally, findings from previous investigations of the technology implemented in nightclubs relied on representations by Servall that the system only collected personal information as authorized under the *Gaming, Liquor and Cannabis Act* (GLCA), which the investigation determined was not the case.

The investigation found that GLCA authorized Alcanna to collect and use “name, age and photograph” in order to decide whether to grant entry to an individual. Based on knowledge or belief about an individual’s past conduct, GLCA authorizes the disclosure of name, age and photograph to other licensees, and requires the information be disclosed to a police officer upon request.

Given GLCA’s provisions, the investigation found it was reasonable for Alcanna to collect and use name and age to identify someone involved in a criminal activity that needs investigating, and to identify someone involved in a prior incident of theft, robbery or violence, and it did not require consent for these purposes.

However, the investigation also found that Alcanna, through the PatronsCan system, examined all the information encoded in a driver’s licence barcode, and retained gender and partial postal code in addition to name and age, which contravened PIPA’s provisions on limited collection and use of personal information (sections 11(2) and 16(2)).

In arriving at this finding, the investigation noted that the legislature specifically considered the need to limit the collection and use of personal information to the extent that is reasonable to meet specific purposes when it amended GLCA in 2009.

The investigation also found that the privacy notice in Alcanna's stores was inaccurate and did not provide adequate contact information in case individuals had questions about the collection of their personal information, as required by PIPA (section 13(1)). The privacy notice did not accurately identify the personal information that was collected or the purposes for the collection.

There were 16 findings and five recommendations in the investigation. Alcanna and Servall committed to address each of the recommendations.

*Investigation Report P2021-IR-03: Investigation into Alcanna Inc.'s use of PatronsCan identification-scanning technology*

“ Overall, this investigation highlights two important issues. The first is that it is clear the legislature intended the 2009 amendments to the GLCA to authorize licensed premises to collect some limited personal information for specific purposes related to investigating and ultimately reducing crime. However, the current language of the GLCA presents a number of practical challenges, particularly when it comes to the use of ID-scanning technologies. I intend to follow-up with government and other stakeholders on this point to articulate these challenges and discuss possible solutions.

Secondly, this investigation serves as a reminder to all businesses that the way in which technology is implemented and what features are engaged, along with several other important considerations such as context, can have substantial implications for compliance. The findings from a review by my office are only as valid as the representations and information made available to us. Additionally, acceptance of a privacy impact assessment is not a 'seal of approval' for marketing purposes, particularly when a technology is implemented in a new and different way in a different context. ”

- Commissioner Jill Clayton, October 7, 2021

## LIFELABS' COMPLIANCE WITH PIPA REVIEWED

After LifeLabs Inc. notified the OIPC of a privacy breach, investigations were opened to review LifeLabs' compliance with HIA and PIPA.

In December 2019, LifeLabs publicly announced a cyberattack it incurred that resulted in unauthorized access to customer information. LifeLabs indicated that the information “could include name, address, email, logins, passwords, date of birth, health card numbers, gender, phone numbers, password security questions and lab test results.” LifeLabs said the information relating to approximately 15 million customers was potentially affected by this breach and that the “vast majority of these customers are in B.C. and Ontario”. LifeLabs also said that a relatively small number of customers in other provinces may have been affected, including Albertans.

The investigation determined that LifeLabs was subject to PIPA, not HIA. Therefore, the investigation's purpose was to review whether LifeLabs protected personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction in accordance with section 34 of PIPA.

The investigation found that LifeLabs did not meet its obligations under section 6(1) of PIPA to both develop and follow policies and practices that are reasonable to meet its obligations under section 34. It was unclear which security policies and practices were followed at the time of the incident. It was also unclear whether policies and practices were consistently followed.

The investigation also found that LifeLabs did not retain personal information only for as long as reasonably required for legal or business purposes, as required by section 35. As a result, it did not meet its obligations under section 34 to make reasonable security arrangements to protect against unauthorized access, use, disclosure or copying.

Ultimately, the investigation determined that LifeLabs did not make reasonable security arrangements to protect personal information as required by section 34 of PIPA.

The investigation resulted in five recommendations to LifeLabs.

*Investigation Report P2021-IR-04: Investigation into LifeLabs Inc.'s compliance with the Personal Information Protection Act*



# Mediation and Investigation

The mediation and investigation (MI) team, consisting of a director and seven Senior Information and Privacy Managers (SIPMs), reviews access request responses (requests for review) and responds to privacy complaints from Albertans under all three laws.

In 2021-22, 78% of files that could proceed to Inquiry were resolved at mediation and investigation. In total, 455 files were resolved by mediation and investigation, representing a 15% increase compared with 2020-21 (397).

## IMPACT OF THE PANDEMIC ON MI PROCESSES

There have been challenges on MI processes throughout the pandemic. For example, public bodies, custodians and organizations had challenges accessing responsive records and it took longer to provide records for review or submissions on complaints. The OIPC also had internal challenges responding to work from home realities. Overall, more than 90% of files are taking more than 180 days to resolve.

The OIPC has since moved its MI files to electronic records which was a positive shift accelerated by the pandemic. The MI team is now mostly paperless, which removed duplication of electronic and paper files.

## CASE TRENDS

### Pandemic Related Access Requests and Complaints

The OIPC received reviews concerning access requests made to public bodies with respect to various pandemic-related issues. For example, there are reviews concerning accessing records related to return to school plans, the efficacy of mask wearing in schools or the vaccination program.

Public bodies have a positive obligation to release information that is “clearly in the public interest” under section 32(1)(b) of FOIP. It appears, however, that section 32(1)(b) has not been used by public bodies for releasing information related to the pandemic.

With respect to privacy complaints about pandemic-related mandates, the OIPC received questions but did not receive complaints on the topic. The OIPC received relatively few complaints related to pandemic-related issues, overall.

### Condominium Corporations and PIPA

The past year saw a number of requests for review and complaints made by owners or tenants at condominium corporations.

A common misconception is what an individual considers as personal information when making a request for information under PIPA. For example, requesting an invoice from a condominium corporation related to fixing water damage is generally not considered personal information and PIPA does not apply. The OIPC receives requests to review responses to access requests related to these types of issues. PIPA permits someone to ask a condominium corporation for access to their personal information, but it does not have provisions for requesting access to information that is not personal information.

Common privacy complaints include disclosure of personal information during condominium board meetings, in meeting minutes or in notices concerning arrears for condominium fees. The collection, use or disclosure of personal information through the installation of video surveillance in common areas of the condominium is also the subject of several complaints.

Requests for review and complaints related to condominium boards are challenging. Condominium boards often change membership and are comprised of volunteers from the ownership pool making it difficult to establish consistent approaches for complying with PIPA.

The OIPC offers guidance on video surveillance at [www.oipc.ab.ca](http://www.oipc.ab.ca). Service Alberta also offers resources for condominiums' responsibilities under PIPA.

### **Access Requests for Different Mediums of Records**

For the past few years, the MI team has noticed applicants have asked for access to records in many different formats.

Some applicants have requested access to all instant messaging or entire email inboxes of employees or government officials. There have also been requests for access to records within personal email or messaging accounts of government officials, as the applicant alleges that government devices are not always used to conduct government business.

With the increased use of video conferencing, individuals have also raised concerns about the notice – or lack thereof – for recording meetings or have requested transcripts of meetings.

The various mediums available to employees in all sectors raise novel and complex issues under FOIP, including the duty to assist, determining custody or control of responsive records, following retention schedules and retrieving records subject to an access request.

### **Third Party Requests for Review – Disclosures Harmful to Business Interests**

Third party requests for review under section 16 of FOIP continue to make up a good portion of MI's work.

Section 16 requires a public body to refuse to disclose information that would harm the business interests of a third party. Businesses can request a review of a public body's decision to grant an applicant access to their companies' information by arguing that the criteria for the application of section 16 have been met.

The most common subjects of such reviews are information contained in contracts between the businesses and public bodies and submissions or bids in response to requests for proposals.

The OIPC has noticed businesses arguing that the format or methodology of their bids constitutes commercial or technical information, which should be protected under section 16.

A challenge at MI is getting businesses to provide sufficient evidence to establish that all three conditions are met for the application of section 16 to specific information. The three conditions are:

- Disclosure would reveal the commercial, financial, labour relations, scientific or technical information of a third party
- The information was supplied in confidence
- The disclosure would lead to one of the harms in section 16(1)(c)

### **Increased Requests for Police Misconduct Investigations and Disciplinary Decisions**

Several reviews are active concerning access requests for records related to alleged police or law enforcement misconduct investigations and disciplinary decisions. These include requests for internal police investigations as well as external reviews, such as by the Alberta Serious Incident Response Team.

These requests reflect the heightened public interest in police oversight and accountability, specifically the scrutiny of disciplinary investigation processes. Records relating to performance of job duties can have both personal and non-personal aspects. This often requires consideration of what is and is not personal information and whether disclosure would be an unreasonable invasion of a third party's privacy under section 17 of FOIP.

Section 17 requires public bodies to consider the privacy rights of the subjects of such records against many factors.

The factors include, but are not limited to, the:

- Nature of the records
- Seriousness of the allegations
- Manner in which the allegations are addressed and outcomes
- Existing oversight mechanisms and the desirability of additional public scrutiny
- Extent of prior public disclosure of information that relates to the affected party and records at issue

## Requests for Time Extensions by Public Bodies

A public body must make every reasonable effort to respond to an access request under FOIP 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(2)). 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 2021-22, there were 398 requests for time extensions submitted by public bodies to the OIPC, representing a 35% increase compared with 2020-21 (294).

Of the 398 time extension requests received:

- 78% were made by provincial government departments
- 9% were made by municipalities
- 7% were made by post-secondary institutions
- 2% were made by boards and commissions
- 2% were made by the regional health authority (Alberta Health Services)
- 1% were made by law enforcement
- 1% were made by other public bodies

In total, 75% of the time extension requests were granted to the public body. The remaining 25% were partially granted or denied, or the public body withdrew its request.



# Privacy Impact Assessment Reviews

Privacy impact assessments (PIAs) identify risks to personal information and put safeguards in place to protect privacy. A PIA is most often used for information systems, administrative practices and policy proposals.

There were 1,332 privacy impact assessments (PIA) accepted by the OIPC in 2021-22, representing a 2% decrease compared with 2020-21 (1,363). The OIPC will “accept”, not approve, a PIA. Acceptance acknowledges that there were reasonable efforts made to protect privacy and the custodian, public body or private sector organization has addressed relevant privacy considerations.

Nearly all PIAs are submitted by health custodians under HIA, with some occasionally submitted by public bodies under FOIP or private sector organizations under PIPA. Only health custodians under HIA are required to submit PIAs to the OIPC. Similar PIA requirements do not exist under FOIP and PIPA.

## HIA

Privacy impact assessments have been mandatory since 2001 for health custodians under HIA. During that time, the types of information systems implemented in the health sector have changed drastically.

Initially, health custodians submitted PIAs on locally installed, single purpose information systems, such as patient record directories or digital calendars. These information systems were often installed from a CD, and internet access was not required. Otherwise, the PIAs regarded paper-based policies and procedures for protecting health information.

More recently, health custodians are submitting PIAs on complex, multipurpose applications, such as cloud-based virtual healthcare products or multifaceted digital messaging systems. As with many apps, virtual healthcare products and digital messaging systems operate with the assistance of several third party service providers that offer a range of behind-the-scenes services, such as ID verification or multifactor authentication. These third parties also often operate in many different sectors and industries providing technological infrastructure support.

These significant changes in the way healthcare is delivered have created new risks to health information that must be considered and reasonably mitigated by health custodians. A PIA remains the best way for health custodians to analyze and mitigate risks to privacy before implementing a new system.

The ubiquitous use of digital healthcare tools has in turn led to a significant increase in the number of PIAs received by the OIPC. In the early 2000s, a few hundred PIAs were submitted by custodians each year. Over the past few years, the OIPC routinely receives from custodians more than 1,000 PIAs annually. Of those, a few notable PIAs are accepted by the OIPC each year, including:

- **Alberta COVID-19 Correction Request (ACCR) System:** The ACCR System is a web portal through which Albertans can report any issues or corrections to their COVID-19 records. The system was implemented by Alberta Health, in collaboration with Alberta Health Services. The OIPC conditionally accepted this PIA in February 2022.

- **AB COVID Records PIA:** The AB COVID Records application allows Albertans to access a secure, verifiable and trusted digital copy of their COVID-19 vaccination information. The AB COVID Records system facilitated the implementation of the Restrictions Exemption Program. The OIPC accepted this PIA in February 2022.
- **Central Fill Service:** The Central Fill Service, also known as Central Fill Pharmacy, is a “Shared Services Pharmacy” implemented by Shoppers Drug Mart Inc. It is used for

preparing and packaging prescription orders for participating Shoppers Drug Mart pharmacies. This service includes the filling and product verification steps of the prescription and dispensing workflow for Shoppers Drug Mart pharmacies. Central Fill Service interfaces with pharmacy practice management systems but it is not a patient facing application. The OIPC accepted this PIA in November 2021.

The OIPC received 957 breach reports in 2021-22 under all three laws, representing a 31% decrease compared with 2020-21 (1,388).

HIA and PIPA require health custodians and private sector organizations to report certain privacy breaches to the OIPC. Public bodies may report breaches voluntarily.

The OIPC closed 1,400 self-reported breach files in 2021-22 under all three laws, representing a 20% increase compared with 2020-21 (1,115).

Certain breaches are prioritized for review, including files where affected individuals have not yet been notified or when a significant number of Albertans have been affected.

## Privacy Breaches

### PIPA

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.

There were 340 breaches reported in 2021-22, a 9% decrease compared with 2020-21 (377).

The Commissioner issued 338 breach decisions in 2021-22, representing no change compared with 2020-21 (338). The following decisions were made in 2021-22:

- 266 were found to have a real risk of significant harm
- 44 were found to have no real risk of significant harm
- 28 where PIPA did not apply (that is, the Commissioner did not have jurisdiction to make a decision)

Of particular concern among the breaches reported is the continued increase in electronic system compromises. Breaches caused by phishing, in particular, are leading to massive and costly incidents. For example, when ransomware or malware is installed on an organization's systems, the breach is often initially caused by a successful phishing attempt against an employee. These breaches serve as important reminders to organizations of all sizes to train staff about suspicious emails, messages or requests, and to keep up to date with all IT security updates.

On that note, in the past year there were several notable breach decisions:

- The organization was the subject of a cyberattack that resulted in the exfiltration of personal information. The information was subsequently published on a dark web data marketplace. Nearly 20,000 individuals whose information was collected in Alberta were affected by the breach.

The organization provides employee wellness and employee and family assistance programs to a number of public and private sector clients. A number of client organizations also submitted breach reports to the OIPC, which highlighted the importance for organizations in these business relationships to clearly understand who controls what records, particularly in the case of a breach.

*P2021-ND-284, Homewood Health Inc.*

- The operator of a proof of vaccination app had a vulnerability that led to the exposure of personal information of approximately 17,500 individuals whose personal information was collected in Alberta.

After the incident was reported in the media, the OIPC received complaints that led to an investigation against the organization.

*P2021-ND-232, 2364920 Alberta LTD. o/a PORTpass Inc.*

- Threat actors exploited a vulnerability in the organization's website, which enabled them to upload a malicious payload and eventually access a customer database. Of the approximate 90,000 individuals affected, about 4,200 of them had their personal information collected in Alberta.

There was a notably wide scope of affected data elements, including bitcoin or financial information and physical location.

*P2021-ND-282, 8159181 Canada Inc. d/b/a Canadian Bitcoins*

- The organization discovered that an external backup drive was missing from the server room of its head office, despite the external backup drive being located in a server room that required a key code to access. The organization also discovered the encryption function on the scheduled daily backups of the server was disabled some time prior to the incident. The stolen drive affected 27,163 individuals.

The organization said it is incorporated under the *Societies Act* and therefore is a "non-profit organization" as defined in section 56(1)(b)(i) of PIPA. In this case, however, the organization operates a meal delivery service at a cost and is therefore engaging in commercial activities. As a result, PIPA applied to the personal information that was collected, used or disclosed in connection with the organization's commercial activities.

*P2022-ND-023, Edmonton Meals on Wheels*

- The organization discovered that it was a victim to ransomware. In the days prior to ransomware being installed on its systems, the attack began when a server was infected with malware. The attacker(s) then used several strains of malware and offensive tools to gain access to other systems before installing ransomware. The organization also discovered that stolen records were leaked on the dark web. The organization was not able to determine how the attackers initially compromised the organization's network. Of the 6,715 individuals affected, 1,100 had their information collected in Alberta.

*P2021-ND-339, Canpar Express Inc.*

- Online applications for professional development scholarships and bursaries were inadvertently publicly accessible on the organization's website. Applicants' contact information could be returned as part of search results when specific searches were entered. The organization investigated and found four other scholarship and bursary archives were on a default setting that made them visible to the public. The organization removed the information. In total, approximately 1,154 individuals whose information was collected in Alberta were affected. This situation serves as a reminder to triple check settings when interconnected information systems may leave personal information publicly exposed on websites.

*P2021-ND-298, The Alberta Teachers' Association*

## HIA

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(2) of HIA to notify the Minister of Health and the individuals affected by the privacy breach.

There were 551 breaches reported by custodians to the OIPC in 2021-22, representing a 41% decrease compared with 2020-21 (930).

The OIPC saw an increase in snooping breaches where someone with authorized access to health information viewed another person's COVID-19 vaccine results without an authorized purpose to do so. The highest proportion of breaches submitted under HIA, however, continue to be human error breaches where prescriptions and requisitions are provided to the wrong patient.

## FOIP

There were 73 breaches reported voluntarily by public bodies in 2021-22, representing a 10% decrease compared with 2020-21 (81).

FOIP is Alberta's only privacy law that does not require regulated entities to report privacy breaches to the Commissioner and notify affected individuals.

# Offence Investigations under HIA

---

There were two convictions for unauthorized access to health information and one conviction for unauthorized disclosure of health information in 2021-22.

A former Alberta Health Services employee in Calgary pleaded guilty in October 2021 to knowingly accessing health information in contravention of HIA. The individual illegally accessed the health information of 76 individuals 238 times over a two-year period. The individual was sentenced to 200 hours of community service and two years of probation, including not being employed in any capacity that allows access to health information.

A former Alberta Health Services employee in Calgary pleaded guilty in February 2022 to knowingly accessing health information in contravention of HIA. The individual illegally

accessed the health information of 189 individuals 985 times over a two-year period. The individual was fined \$5,000, plus a \$1,000 victim fine surcharge, for the infractions and given 18 months of probation, including not being employed in any capacity that allows access to health information.

A former Covenant Health employee in Vegreville pleaded guilty in March 2022 to knowingly disclosing health information in contravention of HIA. The individual also admitted to accessing health information of several people without a valid employment purpose.

There have been 21 convictions for offences under HIA as of March 31, 2022.

# Summary of Significant Decisions

---

## **Canadian Energy Centre Not Subject to FOIP**

The applicant sought copies of records from the Canadian Energy Centre Ltd. (CEC). In response, CEC advised that it was not a public body under FOIP. The applicant sought a finding that CEC qualifies as a public body despite the fact that it has not been designated as such.

The Adjudicator determined that CEC is not a public body within the meaning of the definitions set out in FOIP.

The Adjudicator found that the decision to subject CEC to public scrutiny and accountability under FOIP does not rest with the Commissioner. The Adjudicator concluded that only the government can decide to designate CEC as a public body covered by FOIP.

*Canadian Energy Centre Ltd., Order F2022-16*

## Clearview AI Ordered to Comply with PIPA

In Investigation Report P2021-IR-01, the OIPC found, among other things, that Clearview engaged in the collection, use and disclosure of personal information through the development and provision of its facial recognition application, without the requisite consent, contrary to section 7(1) of PIPA. The report was issued in conjunction with the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec and the Office of the Information and Privacy Commissioner for British Columbia. The report also found that Clearview's collection, use and disclosure of personal information through the provision of its facial recognition application was for a purpose that a reasonable person would find to be inappropriate, contrary to sections 11, 16 and 19 of PIPA.

As a result, the report recommended, among other things, that Clearview:

1. Cease offering the facial recognition services that have been the subject of this investigation to clients in Canada
2. Cease the collection, use and disclosure of images and biometric facial arrays collected from individuals in Canada
3. Delete images and biometric facial arrays collected from individuals in Canada in its possession.

The report also said at para. 123:

Should Clearview maintain its refusal to accept the findings and recommendations of four independent Canadian privacy enforcement authorities, we will pursue other actions available to us under our respective Acts to bring Clearview into compliance with federal and provincial privacy laws applicable to the private sector.

Following exchanges of correspondence, the Commissioner did not accept Clearview's position on recommendations 2 and 3, as it had come to the Commissioner's attention that Clearview had already agreed to do something similar in Illinois. Clearview described what it undertook to do in Illinois as a "very imperfect

proxy" for identifying individuals from Illinois. However, the Commissioner said, "In my view, there is nothing to prevent me from also directing a 'very imperfect proxy' that Clearview can pursue to comply with my order."

The Commissioner ordered Clearview under section 36(1)(b), section 52(3)(e) and section 52(3)(g) of PIPA to comply with the recommendations set out above.

To comply with this order, Clearview was directed to take similar good faith steps as those to which it referred in the Memorandum of Law in Illinois.

Clearview applied for judicial review of this order. The judicial review was not heard as of March 31, 2022.

*Clearview AI Inc., Order P2021-12*

## Responding to Applicant Via Email

In two separate orders, applicants said they did not receive a response to their access request, yet in both cases the public bodies had emailed the records within time limits set out in FOIP.

In Order F2021-30, the applicant made an access request to the Town of Ponoka. The applicant indicated that the time limit for responding to her request had expired and she had received no reply as required by FOIP.

The Town of Ponoka said that it responded to the applicant via email, and that its email records indicated that the response was delivered to the applicant, with no rejection notice.

The Adjudicator found that the Town of Ponoka made every reasonable effort to respond to the applicant's request not later than 30 days after it received the request, as required by section 11 of FOIP.

In Order F2021-31, the applicant made an access request to the Municipality of Crowsnest Pass. In a substantially similar situation as in the Town of Ponoka order described above, the Municipality of Crowsnest Pass emailed its response to the applicant's request.

The Adjudicator found that the applicant did not notify the Municipality of Crowsnest Pass that he had not received a response to the access request. The Adjudicator concluded, “It was reasonable for the [Municipality of Crowsnest Pass] to respond via the email address the Applicant included in his FOIP request, and that had been used to communicate with the Applicant during the processing of the request. In the circumstances, it was also reasonable for the [Municipality of Crowsnest Pass] to assume its response had been received by the Applicant. Without something to alert it, the [Municipality of Crowsnest Pass] cannot be expected to know or guess that there was an issue with its response and/or the Applicant’s receipt of its response. I find that the [Municipality of Crowsnest Pass] met its duties under section 11 of the Act.”

*Town of Ponoka, Order F2021-30*

*Municipality of Crowsnest Pass, Order F2021-31*

### **Disclosure of Health Information for Involuntary Admission to a Medical Facility**

An individual made a complaint that Alberta Health Services (AHS) disclosed her health information contrary to HIA when AHS provided the Edmonton Police Service (EPS) with a copy of an admission certificate regarding the complainant, completed pursuant to section 2 of the *Mental Health Act*.

AHS also disclosed to EPS examination notes from a physician about the complainant. AHS acknowledged that it disclosed the notes in error, and that the disclosure was not permitted under HIA. The Adjudicator ordered AHS to refrain from similar disclosures in the future.

The Adjudicator found, however, that disclosure of the admission certificate was permitted under section 35(1)(m)(ii) of HIA. AHS had reasonable grounds to believe that disclosing the full admission certificate to EPS would avert or minimize danger to the health or safety of any person. Specifically, it would enable EPS to apprehend and convey the complainant to a medical facility, after the physician had determined that she was likely to cause harm to herself or others.

*Alberta Health Services, Order H2021-07*

### **Corporations Are Not Individuals under PIPA**

Under PIPA, a corporation and an individual made complaints that Direct Energy Regulated Services (Direct Energy) contravened PIPA when it collected and used their information.

The complainants alleged that Direct Energy contravened PIPA when it used their information to contact them in relation to a property, 16 years after they ceased being involved with the property.

Direct Energy argued that a corporation was not an individual under Part 5 of PIPA, and therefore could not make a complaint. The Adjudicator considered that issue, and also whether collection and use of the information in question was exempt from PIPA as collection and use of “business contact information” under section 4(3)(d).

The Adjudicator found that a corporation is not an individual and therefore could not make a complaint under PIPA.

The Adjudicator found that the information in question was the individual complainant’s personal information and also business contact information used by him as a representative of the corporation when dealing with Direct Energy. The Adjudicator found that Direct Energy collected and used the business contact information for the purposes of contacting the individual complainant in relation to his business responsibilities. As a result, collection and use were exempt from PIPA as business contact information under section 4(3)(d).

The Adjudicator retained jurisdiction to consider the further issue of whether Direct Energy contravened section 35 of PIPA when it retained the individual’s personal information for so long after the complainant was no longer involved with the property in question.

*Direct Energy Regulated Services, Order P2021-10*

# Judicial Reviews and Other Court Decisions

## JUDICIAL REVIEWS

### ***Edmonton Police Service v Alberta (Information and Privacy Commissioner), 2021 ABQB 304***

In Order F2020-17, the applicant made an access request to the Edmonton Police Service (EPS), seeking records from an RCMP file. The applicant wanted to use the records to lay an information under the *Criminal Code*. EPS withheld all the information under section 21(1)(b) of FOIP. After later releasing portions of the records to the applicant, information was withheld by EPS under sections 17(1) and 21(1)(b).

The Adjudicator found that section 21(1)(b) did not apply to the records at issue. The information in the records was collected by the RCMP acting as a provincial police service under the *Police Act*. As a provincial police service, the RCMP are considered a representative of the Government of Alberta, and not an entity under section 21(1) with which the Government of Alberta has relations. The Adjudicator found that some information was correctly withheld under section 17(1) but that other information should be disclosed.

EPS requested judicial review of the Adjudicator's findings under section 21(1)(b) of FOIP. The court upheld the order as reasonable and dismissed the judicial review. The court's decision is currently under appeal.

### ***Edmonton Police Service v Alberta (Information and Privacy Commissioner), 2021 ABCA 428***

The Alberta Court of Appeal granted intervener status, with specified conditions, to the Attorney General of Alberta and the Attorney General of Canada in the appeal of *Edmonton Police Service v Alberta (Information and Privacy Commissioner)*, 2021 ABQB 304.

### ***AHS v Cardinal, 2021 ABQB 678***

In Order H2020-05, the applicant had been treated at a hospital in his community and then at the University of Alberta Hospital Emergency Department for a fracture. At his community hospital, a physician wrote the following statement on the applicant's chart: "supposedly was hit by a vehicle (whilst pointing a gun @ them)." A physician at the University of Alberta hospital also made a chart note regarding the complainant pointing a gun.

The applicant made a request to Alberta Health Services (AHS) that it delete both statements. He also complained that AHS had not collected the information that was the source of the statement directly, as required by HIA, and that it had not used his health information in accordance with the Act.

The Adjudicator found that AHS' collection and use of the complainant's information was in compliance with HIA given the emergency department setting in which the information was collected and used. However, the Adjudicator noted that if it were the case that the information could be used or disclosed in the future, and AHS was unable to establish the truth of the statements, AHS should take steps to ensure they were not accessible, or amend them to warn future users that the information may not be sufficiently reliable for use or disclosure unless reasonable steps are first taken to ensure their accuracy.

On judicial review, the court upheld Order H2020-05 as reasonable. The court agreed with the Adjudicator's finding that section 13(6) of HIA did not apply to the information at issue because it was not a professional opinion or observation of a health services provider. Because section 13 did not address the issue at inquiry, the Adjudicator considered the purpose of the Act, the duty to ensure information is accurate, and the scope of powers of the Commissioner under section 80. AHS' application for judicial review was dismissed.



***Blades v Alberta (Information and Privacy Commissioner), 2021 ABQB 725***

This case involved a judicial review of a time extension decision under FOIP. On July 3, 2020, the applicants requested disclosure of records from Alberta Energy (Energy) related to the government's decision to rescind a long-standing coal mining policy. This policy, the "1976 Coal Mining Policy" had previously restricted coal mining in the area where the applicants live and range. It was reinstated in February 2021.

Energy granted itself a series of time extensions, and then requested a time extension from the Commissioner, which was granted on January 6, 2021. On January 11, 2021, Energy advised the applicants by way of letter that the Commissioner had granted an additional 270 days to respond to the access request. The applicants requested a judicial review.

The court held that the manner in which the Commissioner had granted the time extension was procedurally fair. The court noted at paragraph 44 that the failure of Energy to properly communicate the full reasons to the applicant may be relevant to costs but was insufficient to quash the decision of the Commissioner.

In assessing the reasonableness of the time extension decision, the court stated at paragraph 80: "The Commissioner was attuned to the purposes of the Act and the importance of timely disclosure to applicants, as demonstrated when the Commissioner denied the 612 day extension requested by Alberta Energy. The Commissioner referred to the threshold of 500 records as a bench mark when determining whether the number of records in this case, being 6539, constituted a large number of records. The Commissioner acknowledged the average extension time it usually granted, consistent with that amount of records. The Commissioner also considered additional time that was needed to issue third party notices and complete possible public body consultations. The Commissioner, in granting the extension, properly relied upon only those enumerated factors that could be considered under [section] 14."

The time extension decision was upheld as reasonable and the application for judicial review was dismissed.

***University of Alberta v Alberta (Information and Privacy Commissioner), 2021 ABQB 795***

Following the Supreme Court of Canada's decision in *Alberta (Information and Privacy Commissioner) v University of Calgary*, 2016 SCC 53, the Commissioner decided to complete the inquiry. In Decision F2017-D-01, the Adjudicator held that the notice to produce that had been the subject of an earlier judicial review had been an interim step in the proceedings and the substantive question as to whether the University of Calgary had properly withheld records it claimed were subject to solicitor-client privilege had not been fully determined.

In Order F2017-84, the Adjudicator held that, as per the Supreme Court of Canada's decision, certain records were subject to solicitor-client privilege and could be withheld by the University of Calgary. However, the Adjudicator held there was a period of time which had not been addressed by the court, and in which the University of Calgary's claims of solicitor-client privilege had been challenged by the applicant. The Adjudicator ordered such records, if they existed, to be disclosed to the applicant.

The court reviewed the earlier decision by the Supreme Court of Canada and held it was unreasonable for the Adjudicator "to have parsed the Supreme Court's reasons so as to reject its findings regarding the validity of the privilege." The court held that the matter was not, however, moot. In the circumstances of this case, the court awarded costs against the Commissioner.

## OTHER COURT DECISIONS

***Roy v Roy, 2021 ABQB 788***

The plaintiff filed a statement of claim naming a number of defendants including an employee of the OIPC. In accordance with Civil Practice Note No. 7, the court struck the statement of claim, finding that it was a hopeless proceeding and an abuse of the court and its processes.

# EDUCATION & OUTREACH



## Speaking Engagements

---

The Commissioner and staff presented at 34 events in 2021-22. Among the topics, the OIPC spoke about facial recognition and privacy implications of new technologies, and virtual healthcare in response to the Babylon by Telus Health investigation. The Commissioner also recapped 10 years in the role with a variety of audiences.

The OIPC continued to participate in the School at the Legislature program. An opportunity for the office to speak to Grade 6 students in Alberta about digital privacy, privacy rights and the office's role in protecting personal information.

## Collaboration with Other Jurisdictions

---

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

### **COMMISSIONERS CALL ON GOVERNMENTS TO REINFORCE ACCESS AND PRIVACY RIGHTS**

In June 2021, Canada's information and privacy regulators in a joint resolution called on their respective governments to respect Canadians' quasi-constitutional rights to privacy and access to information. The Commissioners took note of the serious impact the COVID-19 pandemic has had on the right of access to information and privacy rights in Canada and requested governments to use the lessons learned during the pandemic to enhance these rights.

### **PRIVACY AND COVID-19 PASSPORTS**

Canada's federal, provincial and territorial privacy commissioners issued in May 2021 a joint statement on privacy and COVID-19 vaccine passports.

The statement recognized the potential value of a vaccine passport, or proof of vaccination program, "as a means of allowing a return to something more closely resembling normal life." However, the Commissioners cautioned that necessity, effectiveness and proportionality for vaccine passports must be established and "must be continually monitored to ensure that they continue to be justified."

## TRADITIONAL MEDIA

The OIPC had 63 media requests in 2021-22, a decrease of 27% compared with 2020-21 (86).

The following topics generated the most media requests:

- Proof of vaccination guidance and COVID-19 vaccine cards
- Complaints about the Canadian Energy Centre and how Alberta's laws apply to its operations
- Babylon by Telus Health investigation reports
- Edmonton Police Service's facial recognition program
- Liquor store ID-scanning investigation report

## 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:

- Canadian Energy Centre order finding that it is not subject to FOIP
- Babylon by Telus Health investigation reports
- Clearview AI ordered to comply with PIPA after its failure to implement recommendations made in an investigation report
- Proof of vaccination guidance
- Liquor store ID-scanning investigation report

The OIPC's Twitter account is available at [www.twitter.com/ABoipc](https://www.twitter.com/ABoipc).

## Publications

The OIPC issued the following resources in 2021-22:

- Proof of Vaccination (May 2021)
- Helping Municipal Councillors Understand FOIP (November 2021)



# FINANCIAL STATEMENTS



Independent Auditor's Report.....	52
Statement of Operations.....	54
Statement of Financial Position.....	55
Statement of Change in Net Debt.....	56
Statement of Cash Flows.....	57
Notes to the Financial Statements.....	58
Schedule 1 - Salary and Benefits Disclosure.....	65
Schedule 2 - Related Party Transactions.....	66
Schedule 3 - Allocated Costs.....	68



## 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, 2022, 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, 2022, 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 18, 2022

Edmonton, Alberta



# Financial Statements

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER STATEMENT OF OPERATIONS

Year ended March 31, 2022

	2022		2021
	Budget	Actual	Actual
<b>Revenues</b>			
Prior Year Expenditure Refund	\$ -	\$ 3,979	\$ 1,117
Other Revenue	-	135	1,131
	-	4,114	2,248
<b>Expenses – Directly Incurred (Note 3b)</b>			
Salaries, Wages, and Employee Benefits	\$ 5,726,000	\$ 5,750,518	\$ 5,805,608
Supplies and Services	1,272,000	1,265,019	1,253,519
Amortization of Tangible Capital Assets (Note 5)	-	45,613	29,435
<b>Total Program-Operations</b>	6,998,000	7,061,150	7,088,562
<b>Net Cost of Operations</b>	\$ (6,998,000)	\$ (7,057,036)	\$ (7,086,314)

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

# Financial Statements

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER STATEMENT OF FINANCIAL POSITION

As at March 31, 2022

	2022	2021
<b>Financial Assets</b>		
Cash	\$ 200	\$ 200
Accounts Receivable	-	57,884
	200	58,084
<b>Liabilities</b>		
Accounts Payable and Other Accrued Liabilities	319,314	454,277
Accrued Vacation Pay	621,434	536,172
	940,748	990,449
<b>Net Debt</b>	(940,548)	(932,365)
<b>Non-Financial Assets</b>		
Tangible Capital Assets (Note 5)	209,840	223,577
Prepaid Expenses	47,668	53,738
	257,508	277,315
<b>Net Liabilities</b>	\$ (683,040)	\$ (655,050)
Net Liabilities at Beginning of Year	\$ (655,050)	\$ (700,410)
Net Cost of Operations	(7,057,036)	(7,086,314)
Net Financing Provided from General Revenues	7,029,046	7,131,674
Net Liabilities at End of Year	\$ (683,040)	\$ (655,050)

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, 2022

	2022		2021
	Budget	Actual	Actual
<b>Net Cost of Operations</b>	\$ (6,998,000)	\$ (7,057,036)	\$ (7,086,314)
Acquisition of Tangible Capital Assets (Note 5)		(31,876)	(155,757)
Amortization of Tangible Capital Assets (Note 5)		45,613	29,435
Decrease/(Increase) in Prepaid Expenses		6,070	(44,229)
Net Financing Provided from General Revenues		7,029,046	7,131,674
<b>Increase in Net Debt</b>		(8,183)	(125,191)
<b>Net Debt, Beginning of Year</b>		(932,365)	(807,174)
<b>Net Debt, End of Year</b>		\$ (940,548)	\$ (932,365)

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

# Financial Statements

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER STATEMENT OF CASH FLOWS

Year ended March 31, 2022

	2022	2021
<b>Operating Transactions</b>		
Net Cost of Operations	\$ (7,057,036)	\$ (7,086,314)
Non-cash Items Included in Net Cost of Operations		
Amortization of Tangible Capital Assets (Note 5)	45,613	29,435
	(7,011,423)	(7,056,879)
Decrease/(Increase) in Accounts Receivable	57,884	(57,772)
Decrease/(Increase) in Prepaid Expenses	6,070	(44,229)
(Decrease)/Increase in Accounts Payable and Other Accrued Liabilities	(49,701)	182,963
Cash Applied to Operating Transactions	(6,997,170)	(6,975,917)
<b>Capital Transactions</b>		
Acquisition of Tangible Capital Assets (Note 5)	(31,876)	(155,757)
<b>Financing Transactions</b>		
Net Financing Provided from General Revenues	7,029,046	7,131,674
<b>Cash, Increase</b>	-	-
<b>Cash, at Beginning of Year</b>	200	200
<b>Cash, at End of Year</b>	\$ 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, 2022

### 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 PS3450 Financial Instruments. As the Office does not have any transactions involving financial instruments that are classified in the fair value category, there is no statement of remeasurement gains and losses.

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.

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

March 31, 2022

### **Note 3 Summary of Significant Accounting Policies and Reporting Practices (Cont'd)**

#### 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.

Accounts Receivable

Accounts receivable are recognized at the lower of cost or net recoverable value. A valuation allowance is recognized when recovery is uncertain.

# Financial Statements

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

March 31, 2022

### Note 3 Summary of Significant Accounting Policies and Reporting Practices (Cont'd)

#### (d) Liabilities

Liabilities are present obligations of the Office to external organizations and individuals arising from past transactions or events, the settlement of which is expected to result in the future sacrifice of economic benefits.

They are recognized when there is an appropriate basis of measurement and management can reasonably estimate the amounts.

#### (e) Non-financial assets

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

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

Non-financial assets of the Office includes tangible capital assets and prepaid expenses.

#### 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.

#### Prepaid expenses

Prepaid expenses is recognized at cost and amortized based on the terms of the agreement.

#### (f) Net debt

Net debt indicates additional cash required from General Revenues to finance the Office's cost of operations to March 31, 2022.

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

March 31, 2022

### **Note 4 Future Accounting Changes**

The Public Sector Accounting Board has approved the following accounting standard, which is effective for fiscal years starting on or after April 1, 2023:

- **PS 3400 Revenue**  
This accounting standard provides guidance on how to account for and report on revenue, and specifically, it differentiates between revenue arising from exchange and non-exchange transactions.

Management is currently assessing the impact of this standard on the financial statements.



# Financial Statements

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

March 31, 2022

### Note 5 Tangible Capital Assets

	Leasehold Improvements	Office Furniture and Equipment	Computer Hardware and Software	2022 Total	2021 Total
<b>Estimated Useful Life</b>	5 years	5 years	5 years		
<b>Historical Cost</b>					
Beginning of Year	\$ 43,142	\$ 105,217	\$ 586,515	\$ 734,874	\$ 579,117
Additions	-	8,542	23,334	31,876	155,757
Disposals	-	-	-	-	-
<b>Total Historical Cost</b>	\$ 43,142	\$ 113,759	\$ 609,849	\$ 766,750	\$ 734,874
<b>Accumulated Amortization</b>					
Beginning of Year	\$ 3,011	\$ 74,162	\$ 434,124	\$ 511,297	\$ 481,862
Amortization Expense	8,628	8,599	28,386	45,613	29,435
Disposals	-	-	-	-	-
<b>Total Accumulated Amortization</b>	\$ 11,639	\$ 82,761	\$ 462,510	\$ 556,910	\$ 511,297
<b>Net Book Value at March 31, 2022</b>	\$ 31,503	\$ 30,999	\$ 147,339	\$ 209,840	
<b>Net Book Value at March 31, 2021</b>	\$ 40,131	\$ 31,055	\$ 152,391		\$ 223,577

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

March 31, 2022

### 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 \$549,125 for the year ended March 31, 2022 (2021 - \$598,030).

At December 31, 2021, the Management Employees Pension Plan reported a surplus of \$1,348,160,000 (2020 - surplus \$809,850,000) and the Public Service Pension Plan reported a surplus of \$4,588,479,000 (2020 - surplus \$2,223,582,000). At December 31, 2021 the Supplementary Retirement Plan for Public Service Managers had a deficit of \$20,982,000 (2020 - deficit \$59,972,000).

The Office also participates in a multi-employer Long Term Disability Income Continuance Plan. At March 31, 2022, the Management, Opted Out and Excluded Plan reported an actuarial surplus of \$6,597,000 (2021 - surplus \$7,858,000). 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.

	2022	2021
Obligations under operating leases and contracts	\$ 7,808	\$ 12,600

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

	Total
2022-23	\$ 6,246
2023-24	1,562
	\$ 7,808

# Financial Statements

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

March 31, 2022

### Note 8 Contingent liabilities

The Office is named in one (2021 - None) legal matter where legal costs are being sought and the outcome of this claim is not determinable.

### 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 December 4, 2020. The following table compares the office's actual expenditures, excluding non-voted amounts such as surplus sales and amortization, to the approved budgets:

	Voted Budget	Supplementary Estimate	Adjusted Voted Budget <sup>(1)</sup>	Actual	Unexpended (Over-expended)
Operating expenditures	\$ 6,998,000	\$ 55,000	\$ 7,053,000	\$ 7,015,537	\$ 37,463
Capital investment	-	-	-	31,876	(31,876)
	\$ 6,998,000	\$ 55,000	\$ 7,053,000	\$ 7,047,413	\$ 5,587

(1) As per *Appropriation (Supplementary Supply) Act, 2022*, approved March 17, 2022.

### Note 10 Approval of Financial Statements

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

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER SCHEDULE 1 - SALARY AND BENEFITS DISCLOSURE

Year ended March 31, 2022

	2022			2021
	Base Salary <sup>(a)</sup>	Other Non-cash Benefits <sup>(b)(c)</sup>	Total	Total
<b>Senior Official</b>				
Information and Privacy Commissioner	\$ 241,289	\$ 55,471	\$ 296,760	\$ 312,513

<sup>(a)</sup> Base salary is comprised of pensionable base pay.

<sup>(b)</sup> 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.

<sup>(c)</sup> Other non-cash benefits for the Information and Privacy Commissioner paid by the Office includes \$7,735 (2021: \$7,056) being the lease, fuel, insurance and maintenance expenses for an automobile provided by the Office.

# Financial Statements

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

Year ended March 31, 2022

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	
	2022	2021
<b>Expenses - Directly Incurred</b>		
Alberta Risk Management Fund	\$ 4,332	\$ 3,830
Postage	11,240	10,314
Technology Services	10,500	13,900
Consumption	775	6,441
Fleet vehicle	5,412	5,412
	<b>\$ 32,259</b>	<b>\$ 39,897</b>
Receivable from	\$ -	\$ 57,287
Payable to	\$ -	\$ 15,532

# Financial Statements

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER SCHEDULE 2 - RELATED PARTY TRANSACTIONS *(Cont'd)*

Year ended March 31, 2022

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.

### Expenses - Incurred by Others

Accommodation Costs

Business Services

Other Entities	
2022	2021
\$ 457,345	\$ 460,620
74,000	164,000
<u>\$ 531,345</u>	<u>\$ 624,620</u>

# Financial Statements

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER SCHEDULE 3 - ALLOCATED COSTS

Year ended March 31, 2022

	2022				2021
	Expenses - Incurred by Others				
<b>Program</b>	Expenses <sup>(a)</sup>	Accommodation Costs <sup>(b)</sup>	Business Services <sup>(c)</sup>	Total Expenses	Total Expenses
Operations	\$ 7,061,150	\$ 457,345	\$ 74,000	\$ 7,592,495	\$ 7,713,182

<sup>(a)</sup> Expenses - Directly Incurred as per Statement of Operations which include related party transactions as disclosed in Schedule 2.

<sup>(b)</sup> Costs shown for Accommodation (includes grants in lieu of taxes), allocated by square meters.

<sup>(c)</sup> Business services includes charges for shared services, finance services, technology services, 1GX, and Corporate Overhead.

# APPENDICES



Appendix A: Cases Opened under FOIP, HIA, PIPA by Entity Type.....	70
Appendix B: Cases Closed under FOIP, HIA, PIPA by Entity Type.....	73
Appendix C: Orders, Decisions and Public Investigation Reports Issued.....	76



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

Statistics are from April 1, 2021 to March 31, 2022

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																
Boards			1										8	1	5			15
Colleges										1			3			7		11
Commissions		1	1									1	4		2			9
Committees																		0
Federal Departments												1						1
Foundations															1			1
Government Ministries/Departments			8			3				2		4	136	19	303	5		480
Health Quality Council of Alberta																		0
Hospital Board (Covenant Health)										1								1
Law Enforcement Agencies			6			1		1		1		2	64		4	1		80
Legislative Assembly Office												1	1					2
Local Government Bodies															3	2		5
Long Term Care Centres																		0
Municipalities		2	7			1	1					2	66	17	35	20		151
Nursing Homes																		0
Office of the Premier/Alberta Executive Council													10		8			18
Officers of the Legislature													2					2
Panels																		0
Regional Health Authorities (Alberta Health Services)			3				1			4			17	3	7	1		36
School Divisions		1	5									2	10		1	26		45
Universities			4										15		29	6		54
Other			3							1		1	7	1		5		18
<b>Total</b>		<b>0</b>	<b>4</b>	<b>38</b>	<b>0</b>	<b>0</b>	<b>5</b>	<b>2</b>	<b>1</b>	<b>0</b>	<b>10</b>	<b>0</b>	<b>14</b>	<b>343</b>	<b>41</b>	<b>398</b>	<b>73</b>	<b>929</b>

Note: The statistics do not include Intake cases.

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

Statistics are from April 1, 2021 to March 31, 2022

HIA	Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Engage in or Commission a Study	Excuse Fee	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
	Affiliates and Information Managers (Electronic Medical Record Vendors, Consultants)									1					1
	Associations, Boards, Councils, Committees, Commissions, Panels or Agencies, created by Custodians														0
	Chiropractors								103				6		109
	Dental Hygienists								19						19
	Dentists								198				2		200
	Denturists								1						1
	Government Ministries/Departments														0
	Health Professional Colleges and Associations									4					4
	Health Quality Council of Alberta								1						1
	Hospital Board (Covenant Health)								4		2		13		19
	Long Term Care Centres												1		1
	Midwives								6				1		7
	Minister of Health (Alberta Health)		1						17		3		39		60
	Nursing Homes									1			2		3
	Opticians								1						1
	Optometrists								37				2		39
	Pharmacies/Pharmacists		7						342	2	1		235		587
	Physicians	1	12			1		3	869	4	5		125		1,020
	Podiatrists								1						1
	Primary Care Networks								30				10		40
	Regional Health Authorities (Alberta Health Services)		22			4		1	40	6	7		103		183
	Registered Nurses								58				1		59
	Research Ethics Boards									1					1
	Researchers								1						1
	Subsidiary Health Corporations												1		1
	Universities/Faculties of Medicine									3					3
	Other		6			1		13	2	1	1		10		34
	<b>Total</b>	<b>0</b>	<b>1</b>	<b>48</b>	<b>0</b>	<b>0</b>	<b>6</b>	<b>0</b>	<b>17</b>	<b>1,730</b>	<b>23</b>	<b>19</b>	<b>0</b>	<b>551</b>	<b>2,395</b>

Note: The statistics do not include Intake cases.

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

Statistics are from April 1, 2021 to March 31, 2022

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 Ojpc	Offence Investigation	Privacy Impact Assessment	Request for Advanced Ruling	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
	Accommodation & Food Services											4		3		7
	Admin & Support Services			2								3		4		9
	Arts, Entertainment & Recreation			1							1			2		4
	Child Daycare Services											1		5		6
	Construction			1								1		2		4
	Credit Bureaus			1												1
	Credit Unions			1								1		13		15
	Dealers in Automobiles			1								1		2		4
	Educational Services			1								3		14		18
	Finance											1		42		43
	Health Care & Social Assistance			2		1			6				1	25		35
	Information & Cultural Industries			5					2		2			8		17
	Insurance			3								2		34		39
	Legal Services											2		13		15
	Management of Companies & Enterprises													1		1
	Manufacturing											1		23		24
	Medical & Diagnostic Laboratories										1			1		2
	Mining, Oil & Gas			1								1		10		12
	Motor Vehicle Parts & Accessorie											1				1
	Other Services			7		1			3		1	12		44		68
	Private Health Care & Social Assistance										1	2		4		7
	Professional, Scientific & Technical			1							1	1		23		26
	Public Administration													1		1
	Real Estate, Rental, Leasing			7								10		12		29
	Retail			3								3		23		29
	Trades/Contractors													5		5
	Transportation			1										4		5
	Utilities													2		2
	Wholesale Trade											2		13		15
	<b>Total</b>	<b>0</b>	<b>0</b>	<b>38</b>	<b>0</b>	<b>0</b>	<b>2</b>	<b>0</b>	<b>0</b>	<b>11</b>	<b>0</b>	<b>7</b>	<b>52</b>	<b>1</b>	<b>333</b>	<b>444</b>

Note: The statistics do not include Intake cases.

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

Statistics are from April 1, 2021 to March 31, 2022

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	Self-reported Breach	Total	
	Agencies																0	
	Boards		5							1			7		1		14	
	Colleges												1			4	5	
	Commissions									3		2	1		2		8	
	Committees																0	
	Federal Departments											1					1	
	Foundations												1				1	
	Government Ministries/Departments		10			2				1		5	109	12	292	4	435	
	Health Quality Council of Alberta																0	
	Hospital Board (Covenant Health)									1			1				2	
	Law Enforcement Agencies	1	2	1		2		1				1	43		3		54	
	Legislative Assembly Office											1					1	
	Local Government Bodies												4		3	3	10	
	Long Term Care Centres																0	
	Municipalities		1	13		1	2			4		1	67	15	31	21	156	
	Nursing Homes												1				1	
	Office of the Premier/Alberta Executive Council												3		8		11	
	Officers of the Legislature																0	
	Panels																0	
	Regional Health Authorities (Alberta Health Services)			1						2			10	3	6		22	
	School Divisions		1	2		1	1					2	13		1	19	40	
	Universities			4						1			19		28	2	54	
	Other								1			2	6	1		7	17	
	<b>Total</b>	<b>1</b>	<b>4</b>	<b>36</b>	<b>0</b>	<b>0</b>	<b>6</b>	<b>3</b>	<b>1</b>	<b>1</b>	<b>13</b>	<b>0</b>	<b>15</b>	<b>286</b>	<b>31</b>	<b>375</b>	<b>60</b>	<b>832</b>

Note: The statistics do not include Intake cases.

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

Statistics are from April 1, 2021 to March 31, 2022

Entity Type	HIA													Total
	Advice and Direction	Authorization to Disregard a Request	Complaint	Engage in or Commission a Study	Excuse Fee	Investigation Generated by Commissioner	Notification to OI/PC	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	
Affiliates and Information Managers (Electronic Medical Record Vendors, Consultants)										1				1
Associations, Boards, Councils, Committees, Commissions, Panels or Agencies, created by Custodians										1				1
Chiropractors									111				6	117
Dental Hygienists									16					16
Dentists									66				2	68
Denturists														0
Government Ministries/Departments														0
Health Professional Colleges and Associations										2			2	4
Health Quality Council of Alberta									2					2
Hospital Board (Covenant Health)			2						6		1		22	31
Long Term Care Centres											1		2	3
Midwives									4				1	5
Minister of Health (Alberta Health)									14		3		56	73
Nursing Homes									1				3	4
Opticians														0
Optometrists									36					36
Pharmacies/Pharmacists			4			1			300	1			355	661
Physicians			20			2			903	3	10		192	1,130
Podiatrists									1					1
Primary Care Networks									19				16	35
Regional Health Authorities (Alberta Health Services)			27			3			39	4	8		324	405
Registered Nurses									39				1	40
Research Ethics Boards										1				1
Researchers														0
Subsidiary Health Corporations			2							1			4	7
Universities/Faculties of Medicine									1	3				4
Other			1		1	1		13	2	1	1		14	34
<b>Total</b>	<b>0</b>	<b>0</b>	<b>56</b>	<b>0</b>	<b>1</b>	<b>7</b>	<b>0</b>	<b>13</b>	<b>1,560</b>	<b>18</b>	<b>24</b>	<b>0</b>	<b>1,000</b>	<b>2,679</b>

Note: The statistics do not include Intake cases.

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

Statistics are from April 1, 2021 to March 31, 2022

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		1			1						3		8		13
	Admin & Support Services											2		4		6
	Agriculture, Forestry, Fishing and Hunting													1		1
	Arts, Entertainment & Recreation		1								1	1		8		11
	Child Daycare Services															0
	Construction		1									1		3		5
	Credit Bureaus													2		2
	Credit Unions										1			11		12
	Dealers in Automobiles															0
	Educational Services		1			1								3		5
	Finance		5								1	2		47		55
	Health Care & Social Assistance		4			1		4			1	1		31		42
	Information & Cultural Industries		8					2		1				16		27
	Insurance		2									6		21		29
	Legal Services		4									5		12		21
	Management of Companies & Enterprises															0
	Manufacturing					1								15		16
	Medical & Diagnostic Laboratories					1					1			2		4
	Mining, Oil & Gas		1									3		8		12
	Motor Vehicle Parts & Accessories															0
	Nursing Homes/Home Health Care													2		2
	Private Health Care & Social Assistance		4								1			3		8
	Professional, Scientific & Technical		4								1			24		29
	Public Administration		1											2		3
	Real Estate, Rental, Leasing		10									6		13		29
	Retail		7			2						4		31		44
	Trades/Contractors		1											1		2
	Transportation											2		8		10
	Utilities											1		1		2
	Wholesale Trade		2									1		17		20
	Other	1	7									14		46		68
	<b>Total</b>	<b>0</b>	<b>1</b>	<b>64</b>	<b>0</b>	<b>0</b>	<b>7</b>	<b>0</b>	<b>0</b>	<b>6</b>	<b>0</b>	<b>7</b>	<b>52</b>	<b>1</b>	<b>340</b>	<b>478</b>

Note: The statistics do not include Intake cases.

## APPENDIX C: ORDERS, DECISIONS AND PUBLIC INVESTIGATION REPORTS ISSUED

Statistics are from April 1, 2021 to March 31, 2022

FOIP Respondent	Orders	Decisions	Public Investigation Reports	Total
Alberta Energy Regulator	1			1
Brazeau Seniors Foundation	1			1
Calgary Police Service	6			6
Canadian Energy Centre Ltd.	1			1
CapitalCare	1			1
Children's Services	2			2
City of Calgary	2			2
City of Edmonton	5			5
City of Spruce Grove	1			1
Edmonton Catholic Separate School Division	2			2
Edmonton Police Service	2			2
Energy	1			1
Environment and Parks	8			8
Health	7			7
Justice and Solicitor General	7			7
Kensington Business Revitalization Zone	1			1
Labour and Immigration	1			1
Municipality of Crowsnest Pass	2			2
Municipality of Wood Buffalo	1			1
Rocky View County	1			1
Strathcona County	1			1
Summer Village of South View	1			1
Town of Ponoka	1			1
University of Alberta	1			1
Workers' Compensation Board	3			3
Subtotal	61	0	0	61

HIA Respondent	Orders	Decisions	Public Investigation Reports	Total
Alberta Health Services	8			8
Covenant Health	1			1
Dr. Alherbish	1			1
Dr. Charles B. Metcalfe	1			1
Dr. Colin Lywood	1			1
Dr. John Dushinski	1			1
Dr. Ryan Yau	1			1
Babylon Health Canada Limited, et al.			1	1
<b>Subtotal</b>	<b>14</b>	<b>0</b>	<b>1</b>	<b>15</b>

PIPA Respondent	Orders	Decisions	Public Investigation Reports	Total
Lifelabs Inc.			1	1
Alcanna Inc. and Servall Data Systems Inc.			1	1
Babylon Health Canada Limited			1	1
ATB Financial	1			1
Canadian Natural Resources Ltd.	1			1
Clearview AI, Inc.	1			1
College of Physicians & Surgeons of Alberta	2			2
Direct Energy Regulated Services	1			1
Grosvenor House Condominium Plan 772-2911	1			1
Industrial Alliance Insurance and Financial Services Inc.	1			1
Little A Accounting	1			1
Luminos Consulting & Production Inc.	1			1
Rogers Insurance Ltd.	1			1
Weinrich Contracting Ltd.	1			1
<b>Subtotal</b>	<b>12</b>	<b>0</b>	<b>3</b>	<b>15</b>
<b>Total</b>	<b>87</b>	<b>0</b>	<b>4</b>	<b>91</b>

**Total number of Orders, Decisions and public Investigation Reports issued:**

FOIP Orders: 61 (63 cases)  
FOIP Decisions: 0  
FOIP Investigation Reports: 0  
HIA Orders: 14 (15 cases)  
HIA Decisions: 0  
HIA Investigation Reports: 1 (15 cases)  
PIPA Orders: 12 (12 cases)  
PIPA Decisions: 0  
PIPA Investigation Reports: 3 (5 cases)

**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 public Investigation Reports are counted by the number of Order, Decision or public Investigation Report numbers assigned. A single Order, Decision or public 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) Public Investigation Reports are recorded by the date they were publicly issued.
- (5) Copies of all Orders, Decisions and public Investigation Reports are available at [www.oipc.ab.ca](http://www.oipc.ab.ca).







