

2021/2022



Office of the
Saskatchewan Information
and Privacy Commissioner

Annual Report

Time for a Digital ID

WWW.OIIPC.SK.CA



Office of the
Saskatchewan Information
and Privacy Commissioner

June 28, 2022

Hon. Randy Weekes
Speaker of the Legislative Assembly
129 Legislative Building
Regina, Saskatchewan
S4S 0B3

Dear Mr. Speaker:

I am pleased to present my eighth Annual Report as Information and Privacy Commissioner for Saskatchewan. I have prepared this Annual Report in accordance with the provisions of section 62(1) of *The Freedom of Information and Protection of Privacy Act*, section 52(1) of *The Local Authority Freedom of Information and Protection of Privacy Act* and section 60(1) of *The Health Information Protection Act*.

As we return to near normal, my office is attempting to provide citizens with the same level of service that they were used to receiving, although I note we have shifted to more emails, virtual meetings and staff working from office or home.

I would like to thank you and the Board of Internal Economy for their support in the past year and I look forward to working with them to provide citizens with a high level of service.

As volumes have increased in my office, my goal for the coming year is to provide citizens, public bodies, and trustees with reports much sooner. My office has a target of issuing a report within 180 calendar days and it is my hope that by March 31, 2023, we have met that target.

I thank the Members of the Legislative Assembly for their support of my office. Going forward, I ask for their assistance in modernizing legislation to recognize that we have changed from a paper-based society to a database society. Now we really do live in a digital world.

I also thank the staff of my office for their hard work over the last year in a much more challenging remote work environment.

Respectfully submitted,

Original signed by
Ronald J. Kruzeniski, Q.C.
Information and Privacy Commissioner

Table of Contents

04 Commissioner's Message

05 About Us

07 Accomplishments 2021-2022

09 The Plan 2022- 2023

11 Files and Reports

19 Time for a Digital ID

22 Virtual Health Care

23 Spotlight on Misdirected Faxes

24 Recommendations for Change

Commissioner's Message



Ronald Kruzeniski, Q.C.
Information and Privacy Commissioner

It has become clear there is a need for each of us, who want one, to have a Digital ID. As more of us get our services online, there is a need to prove we are who we say we are. Governments across Canada are looking at this. British Columbia and Alberta are in the lead. In Saskatchewan, government has been studying this, but at the moment the matter is on “pause”. Later in this report, I discuss the need for the development of a [Digital ID](#) for Saskatchewan residents.

During COVID-19 many things were done online that weren't done that way before. As a result, more and more data exists about us and our organizations in the digital realm. For example, many meetings were held by zoom and recorded and some of those recordings would have contained personal information or personal health information. See Review Report 181-2020, [RM of Rosthern](#). We also know that health care was at times delivered virtually. As we hope to leave COVID-19 behind, some of those practices will continue and we will find other ways of providing service to citizens online. It is important that organizations, public and private, consider the issues of collection, storage, use and protection of that data.

One change that might stay with us is the use of virtual platforms to deliver health care. It was necessary during

COVID-19, but many found it was also convenient. It was of assistance to seniors, those with disabilities or those having to travel long distances. Several service providers entered the market. Later in this report, I suggest ten things that trustees, service providers and patients should consider when utilizing a [virtual platform for health care](#).

In this fiscal year my office spent considerable time looking at the issue of misdirected faxes. This matter was dealt with in Investigation Report [H-2014-001](#) by the former commissioner in 2014. The issue has persisted ever since that time and in 2021 it rose to the forefront again. Later in this report, I discuss the complex issue of [misdirected faxes](#).

Since I was appointed, my office has issued over 845 review and investigation reports, some of which consist of recommendations for legislative change. Later in this report, I outline the reports and the [recommendations](#) for legislative change.

Ronald J. Kruzeniski, Q.C.
Information and Privacy Commissioner

About Us

The Office of the Saskatchewan Information and Privacy Commissioner (IPC) is an independent office of the Saskatchewan Legislative Assembly. It oversees three Saskatchewan statutes:

1

The Freedom of Information and Protection of Privacy Act (FOIP)

2

The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP)

3

The Health Information Protection Act (HIPA)

FOIP, LA FOIP and HIPA establish the access to information and privacy rights of citizens.

OUR MISSION

To ensure that access to information and privacy rights in Saskatchewan are respected.

OUR MANDATE

The IPC ensures that public bodies respect the privacy and access rights of the citizens of Saskatchewan by:

- informing members of the public on their information rights.
- resolving access and privacy disputes between individuals and public bodies.
- investigating and resolving privacy complaints.
- making recommendations on public bodies' policies and practices and.
- commenting on proposed laws, policies and practices.

Accomplishments 2021-2022

Education and Awareness

Goals	Accomplishments
Update the IPC Guide to FOIP , the IPC Guide to LA FOIP and the IPC Guide to HIPA .	Updated Chapter 3 in FOIP and LA FOIP and updated Chapter 4 in FOIP.
Promote mandatory annual access and privacy training for employees within public bodies and health trustees.	This recommendation made in many IPC Reports. Staff participated in a webinar organized by others.
Develop and deliver a webinar during Right to Know Week. Develop and deliver a webinar for Data Protection Day.	Staff participated in a webinar organized by others.
Take part in the development of a Federal/Provincial/Territorial joint guidance document on facial recognition.	Joint guidance document on facial recognition posted.
Take part in the development of a Federal/Provincial/Territorial joint statement on vaccine passports.	Joint statement on vaccine passports posted.

Navigating in a Digital World

Goals	Accomplishments
Review of the office's website to determine what changes and what resources should be updated.	Review completed and website updated.

Advocating for Improvement

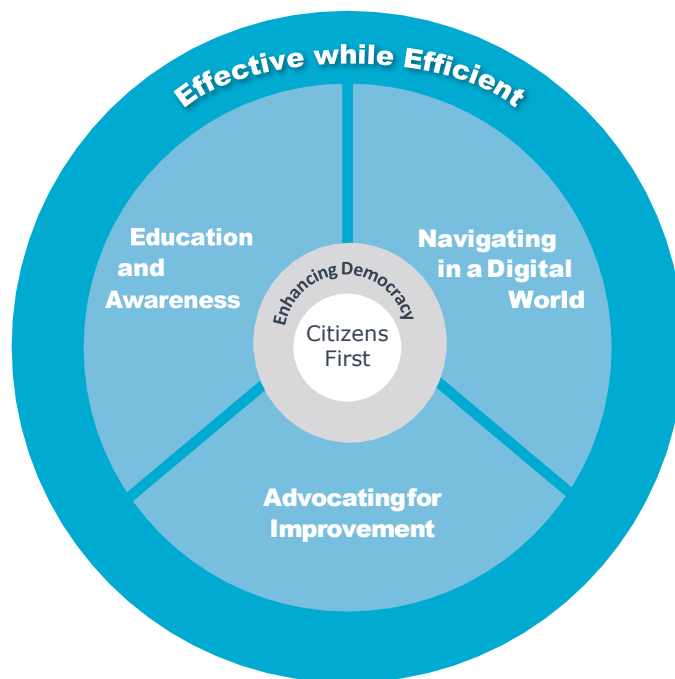
Goals	Accomplishments
Promote the modernization of FOIP and LA FOIP recognizing that we have moved from a paper to a digital society.	Recommendations made in Reports.
Promote regulation amendments to FOIP and LA FOIP including broadening the lists of government institutions or local authorities.	Recommendations made in Reports.
Promote that all non-governmental organizations who receive government or local authority funds will be subject to Part IV of FOIP or LA FOIP (Protection of Privacy).	Recommendations made in Reports.
Promote the modernization of HIPA recognizing that we have moved from a paper to a digital society.	Promoted in correspondence.
Promote updating <i>The Model Professions Act</i> template and promote that professional bodies will be subject to Part IV of FOIP or LA FOIP (Protection of Privacy).	Promoted in correspondence.
Promote HIPA Regulation amendments including broadening the definition of a "trustee".	Promoted in correspondence.

Effective While Efficient

Goals	Accomplishments
Resolve a matter by early resolution within 30 calendar days.	37 calendar days.
Issue a report or resolve a matter on review of an access request within 130 calendar days.	360 calendar days.
Issue a report or resolve a matter regarding breach of privacy within 130 calendar days.	319 calendar days.
Complete or close consultation files within 30 calendar days.	9 calendar days.
Complete or close an application to disregard within 30 calendar days.	23 calendar days.

The Plan 2022-2023

Core to our work is that we support access to records as requested by citizens in a timely manner and promote protection of the privacy of those citizens wherever required. The freedom of information legislation in the province enshrines the principle that citizens should have access to information collected and generated by organizations supported by taxpayer dollars. All other objectives in this document are intended to enhance and protect the rights of citizens to obtain information.



Education and Awareness

Goals

Complete and post to website Chapters 5 and 6 for Guide to FOIP.

Navigating in a Digital World

Goals

Review of the office's website to determine what changes and what resources should be updated.

Promote the need for a Digital ID initiative.

Advocating for Improvement

Goals

Promote the updating of *The Health Information Protection Regulations*.

Efficient while Effective

Goals

After initial contact setup file, explore informal resolution, and continue or discontinue within 30 calendar days.

Issue a Report or resolve a matter on review of an access request within 180 calendar days.

Issue a Report or resolve a matter regarding breach of privacy within 180 calendar days.

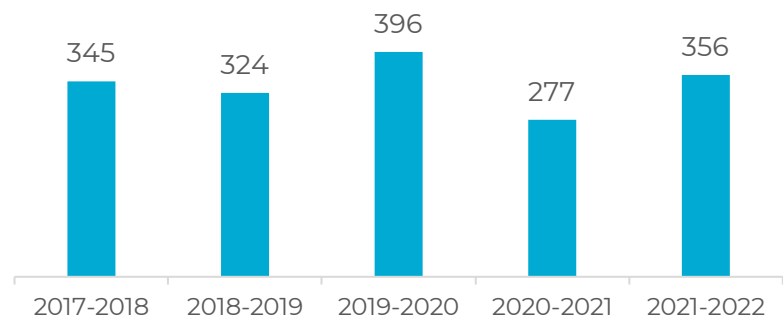
Complete or close consultation files within 30 calendar days.

Complete or close an application to disregard within 30 calendar days.

Files and Reports

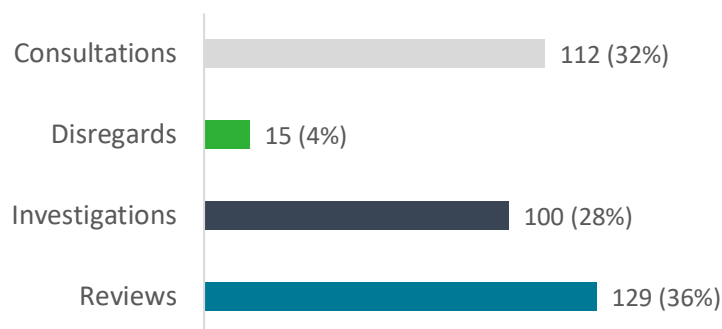
Files Opened

The office continues to have a high number of files opened which has impacted the time it takes to resolve or close a file.

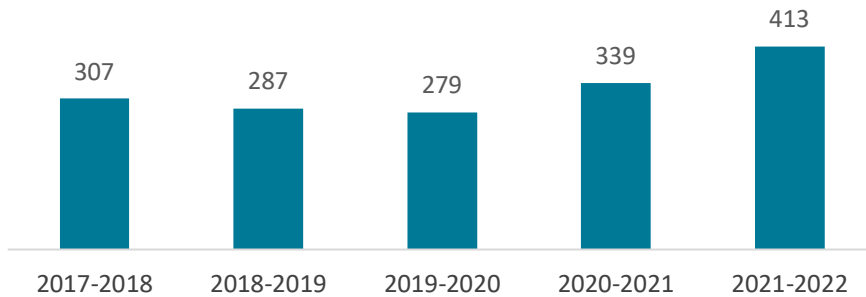


Types of Files Opened

36% of the files opened involved asking the office to do a review of the decision of a head to deny access.



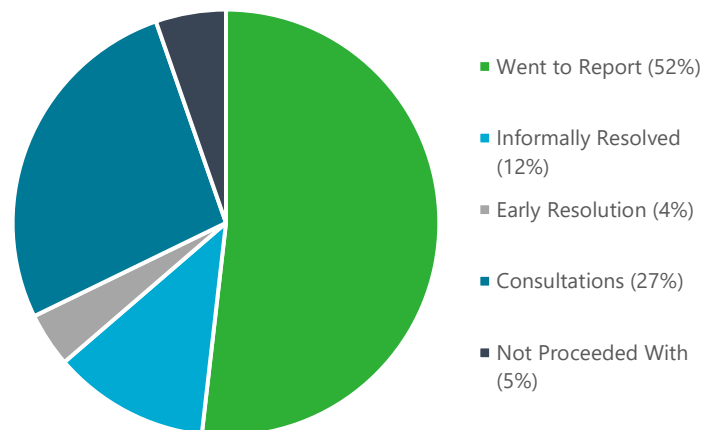
Files Closed



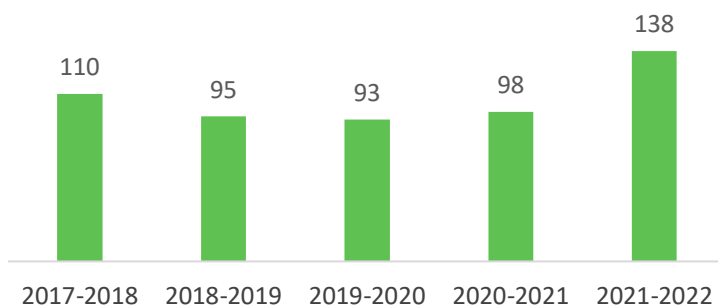
My office was able, to close more files than it opened and closed more this year than in past years.

Resolution of Files

52% of the files resulted in a report while the others were resolved in other ways.



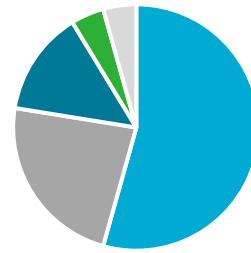
Reports Issued



My office, during this year, was able to significantly increase the number of reports issued. Please note that disregard decisions are included in this number.

Compliance with Recommendations

The office issued 138 reports in the 2021-2022 fiscal year. A public body or trustee is required to respond to the recommendations within 30 days of receiving the report. This is a chart showing the percentage of reports where there is full compliance, partial compliance, no compliance, and where no response was received.



■ Full Compliance (55%) ■ Partial Compliance (23%)
■ No Compliance (14%) ■ No Response (4%)
■ Other (4%)

My office is obligated to report on the recommendations that were not complied with - see FOIP, subsection 62(2); LA FOIP, subsection 52(2); and HIPA, subsection 60(2). Failure to respond to a report is considered to be non-compliance. On the following pages are three tables; the first table lists those public bodies and trustees that responded to a report with no compliance, the second table lists those public bodies and trustees that responded to a report with partial compliance, the third table lists those public bodies and trustees that did not respond at all.

NO COMPLIANCE

Government Institution	Report #	Recommendation(s) not complied with*
Ministry of Education	Review Report 281-2020	[22]
Ministry of Environment	Review Report 280-2020	[23]
Ministry of Health	Review Report 247-2020	[45]
Ministry of Highways	Review Report 196-2020	[62]
Ministry of Highways	Review Report 021-2021, 022-2021, 023-2021	[46]
Ministry of Justice and Attorney	Review Report 023-2020, 027-2020 - Part II	[20]
Ministry of Justice and Attorney	Review Report 197-2020	[33]
Ministry of Parks, Culture and Sport	Review Report 266-2020, 213-2021	[35]
Ministry of Social Services	Review Report 054-2020	[21]

NO COMPLIANCE (continued)

Ministry of Social Services	Review Report 145-2020	[22]
Ministry of Social Services	Review Report 003-2021	[22]
Ministry of Social Services	Review Report 137-2021	[37] , [38]
Ministry of Social Services	Review Report 141-2021, 192-2021	[44] , [45]
Ministry of Social Services	Review Report 142-2021, 193-2021	[44] , [45]
Saskatchewan Government Insurance	Investigation Report 087-2020	[32] , [33]
Saskatchewan Government Insurance	Investigation Report 199-2020	[25]
Local Authority	Report #	Recommendation(s) not complied with*
RM of Lumsden No. 189	Review Report 151-2020	[40]
RM of Lumsden No. 189	Review Report 070-2021	[26]
Saskatchewan Health Authority	Review Report 123-2020	[40]
Trustee	Report #	Recommendation(s) not complied with*
Dove House	Review Report 214-2020, 217-2020	[37]
Saskatchewan Government Insurance	Review Report 221-2020	[41]

PARTIAL COMPLIANCE

Government Institution	Report #	Recommendation(s) not or partially complied with*
Ministry of SaskBuilds and Procurement	Review Report 416-2019	[203]
Ministry of Education	Review Report 201-2020	[76] , [78]
Ministry of Finance	Review Report 044-2020	[135] , [136]

PARTIAL COMPLIANCE (continued)

Ministry of Government Relations	Review Report 026-2021	[126]
Ministry of Government Relations	Review Report 030-2020, 050-2020	[176], [177], [178], [179], [181], [182], [184], [185], [186], [188], [189], [190]
Ministry of Government Relations	Review Report 202-2020	[91], [92]
Ministry of Health	Review Report 101-2019, 192-2019, 193-2019, 194-2019	[107]
Ministry of Health	Review Report 195-2019	[109]
Ministry of Highways	Review Report 108-2021, 152-2021	[74], [75]
Ministry of Justice and Attorney General	Review Report 023-2020, 027-2020 - Part I	[79]
Ministry of Justice and Attorney General	Review Report 126-2020, 185-2020	[71], [75]
Saskatchewan Telecommunications	Review Report 078-2020	[75]
SaskPower	Review Report 129-2020	[119]
Saskatchewan Government Insurance	Review Report 009-2021	[62]
Local Authority	Report #	Recommendation(s) not or partially complied with*
Chinook School Division No. 211	Review Report 173-2020, 190-2020, 157-2021	[122], [123]
Chinook School Division No. 211	Investigation Report 234-2020	[50]
Regina Police Service	Review Report 115-2020, 116-2020, 117-2020	[288], [290], [291], [294], [299], [300]
Regina Police Service	Review Report 132-2020	[256], [258], [259], [262], [263], [264], [267], [270], [271], [272], [273], [274], [275], [276]

Partial Compliance (continued)

Regina Police Service	Review Report 206-2021	[52]
Resort Village of Candle Lake	Report 084-2020, 085-2020, 086-2020, 088-2020, 090-2020, 091-2020, 092-2020	[58] , [59]
RM of North Qu'Appelle No. 187	Investigation Report 166-2021	[45] , [46] , [47] , [48] , [49] , [50]
RM of McKillop No. 220	Review Report 121-2021	[87] , [88] , [89]
RM of McKillop No. 220	Review Report 132-2021	[43] , [44]
Saskatchewan Health Authority	Review Report 073-2020	[51]
Trustee	Report #	Recommendation(s) not or partially complied with*
Saskatchewan Health Authority, St. Anthony's Hospital	Investigation Report 037-2020, 183-2021	[72] , [73] , [74]
Saskatchewan Health Authority University of Saskatchewan Saskatchewan Cancer Agency Dr. Raviqubal Basi	Investigation Report 045-2021, 064-2021, 071-2021, 074-2021, 075-2021, 078-2021, 080-2021, 086-2021, 098-2021, 116-2021, 117-2021, 120-2021, 149-2021, 153-2021, 162-2021, 165-2021, 169-2021, 175-2021, 076-2021, 078-2021, 209-2021, 229-2021, 232-2021, 251-2021	[27] , [52] , [53] , [54] , [55] , [56]
Stonebridge Neurology Clinic	Investigation Report 413-2019, 414-2019, 415-2019	[45] , [46]

*Refers to paragraph number in the Report. Click on the link to go directly to the Report.

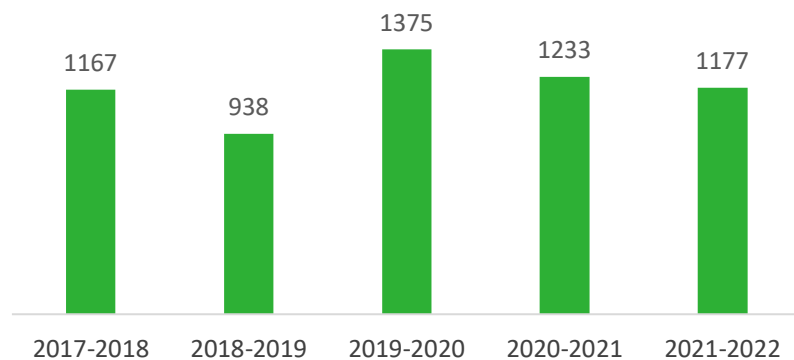
NO RESPONSE RECEIVED

Government Institution	Report #	Recommendation(s) not complied with*
Ministry of Health	Review Report 249-2021	[20]
Ministry of Highways	Review Report 130-2020	[25] , [26]
Local Authority	Report #	Recommendation(s) not complied with*
Northern Village of Sandy Bay	Review Report 019-2021	[30] , [31] , [32]
Prairie Spirit School Division No. 206	Review Report 109-2020	[64]
RM of Lumsden No. 189	Review Report 261-2021, 001-2021 Part II	[47] , [48] , [46]
Rural Municipality of North Qu'Appelle No. 187	Review Report 212-2021	[18]

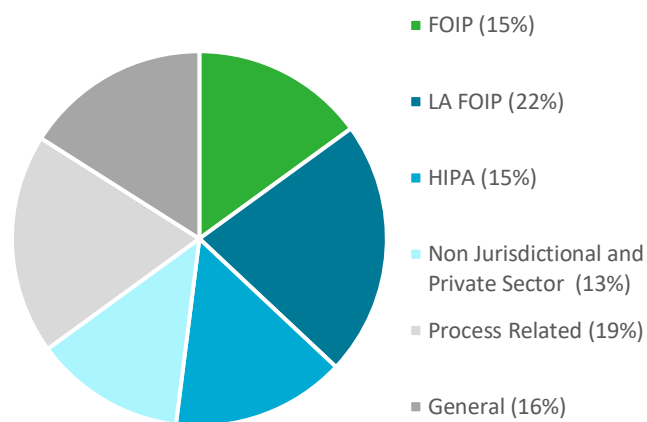
*Refers to paragraph number in the Report. Click on the link to go directly to the Report.

Summary Advice

There was a slight decrease in summary advice provided in the 2021-2022 fiscal year compared to the previous fiscal year.



From the chart to the right, it is clear that the office gives advice related to the three main statutes where the office has jurisdiction; 52% of summary advice was given related to these pieces of legislation.



Time for a Digital ID

Today one can have a driver's licence, a health card, a passport and/or other multiple physical credentials. We most likely always carry these on our person. The time has come where we need a credential that can be used online to prove one's identity. Whether you call it a digital credential, a digital ID or you give it some other name, it is something that would allow each of us the ability to prove who we are when necessary, particularly when we are online. The words "digital credential" and "digital ID" will be used interchangeably.

What is a Digital ID?

The [Government of Ontario](#) has defined a Digital ID as follows:

"Digital ID is an electronic version of trusted government identification that provides better safety, more security and stronger privacy than physical identification cards or documents."

We all have physical ID's such as a driver's licence and health card. My office encourages the development of a digital ID for Saskatchewan citizens as this would allow a citizen to engage with ministries, Crown corporations and other agencies.

Possible uses

Digital ID would be a convenient and easy identification solution that's made with the security and encryption we need to securely perform transactions and access services online. As an individual, you could use digital ID to prove your identity when you:

- make an age-sensitive purchase (like a lottery ticket)
- pick up a package at the post office
- apply for government assistance (such as disability support or EI)
- start a business
- apply for a hunting or fishing licence
- book a site in a provincial park
- sign up for an account at SaskPower or SaskEnergy
- obtain services at SaskTel
- obtain services at municipalities, post-secondary institutions and other agencies
- apply to open a bank account or apply for a personal loan
- make an insurance claim
- renew or replace a driver license
- sign a digital contract
- apply for a passport or other federal services

The possibilities are extensive. Of course, this would depend on government ministries and agencies making it possible and each citizen deciding to request a digital ID and then providing it voluntarily to the ministry or agency.

Understandings

I encourage the development of a digital ID in Saskatchewan with certain understandings. They are:

1. The digital ID service would be subject to FOIP or LA FOIP.
2. A digital ID would be optional, in other words, a citizen would have to request such an ID. A citizen could choose to stay with the regular forms of physical ID, which exist now. **A digital ID would NOT be mandatory.**
3. Subject to FOIP, any personal information provided to the government to set up the digital ID, would be kept confidential and would not be shared with any other ministry or agency.
4. In setting up the citizen's digital ID, the minimum amount of personal information would be requested, and the minimum amount would be disclosed.
5. There would not be a central database containing all the digital ID information about a citizen.
6. The digital ID would be stored in a citizen's smart phone or on a service card and only the citizen would have control and determine who it is shown to.

7. The information collected from a citizen, would not be used to track locations or activities.
8. All security measures would be taken to protect a citizen's personal information from being hacked. There is no such thing as a guarantee but the government would need to take all necessary steps possible to protect the information collected.
9. The government could not collect the citizens' personal information from multiple databases to create a complete picture of a citizen.
10. Any public body who uses the digital ID will have to be transparent as to the data elements it collects and the length of time it retains those elements.
11. A citizen could check online and determine who had accessed their digital credential. If the citizen determined inappropriate access, they could request an investigation of the inappropriate use or cancel their digital ID.
12. If a citizen wanted to cancel their digital ID, there would be a clear easy to access mechanism to do so. Obtaining the digital ID is optional and a citizen has the right to cancel the digital ID, whenever the citizen wants to. If cancelled, the citizen's data would be deleted.

Other Provinces

Other provinces are looking at a digital ID.

British Columbia

British Columbia has a British Columbia Service Card which serves as a citizen's digital ID.
(<https://www2.gov.bc.ca/gov/content/governments/government-id/bc-services-card>)

Ontario

Ontario has announced that it is proceeding with a digital ID. (<https://www.ontario.ca/page/digital-id-ontario>). The Ontario Information and Privacy Commissioner has provided a submission regarding the IPC Comments on the Government's Policy Framework for [Ontario's Digital Identity Program](#).

Generally, the commissioner was supportive of the project and made suggestions under the following themes:

1. Protecting Ontarians' privacy and security
2. Governance and following expert advice
3. Ensuring equity and inclusion of all Ontarians

Alberta

Alberta has a digital ID initiative called [MyAlberta Digital ID](#). It has been in place since about 2017. The Alberta Information and Privacy Commissioner has reported on this in her 2016-2017 Annual Report as follows:

"Service Alberta submitted, and the OIPC accepted, a PIA on the MyAlberta Digital Identity project. The program was implemented by the Government of Alberta as a means to facilitate electronic delivery of services to Albertans. The intent of the project is to deliver services more efficiently while maintaining the security of personal information required for service delivery by government departments. The goal is for the program to be used by government departments, municipalities, post-secondary institutions, agencies, boards and commissions, and other public bodies as defined under the FOIP Act."

For more details see the Alberta government website at <https://account.alberta.ca/>

Quebec

The Quebec Digital Identity Service (SQIN) Program will provide citizens with a trusted digital identity and will simplify their use of government services. It involves seven phases. Work is being done on the first two phases.

The first one aims to modernize the current government authentication solution. This ensures its sustainability and evolution, in addition to allowing citizens easier access to online government services. The first delivery of the Government Authentication Service is scheduled for June 2022 with a public body. It will be deployed to other public bodies until June 2023 for complete offloading of the clicSÉCUR (Quebec's actual authentication solution).

The Quebec government aims to provide citizens with a secure digital identity based on a digital certificate that will simplify identity management. The digital certificate will become a privileged way to interact securely with the Government of Quebec, municipalities, the federal government, the provincial governments as well as private companies. Everything will be accessible via a digital wallet available on a smartphone. The first delivery is scheduled for winter 2022-2023.

Government of Canada

The Government of Canada is encouraging provinces and territories to develop a digital ID. Provincial digital IDs could be used to access federal services. Currently, BC and Alberta's digital ID's can be used to access federal services. The federal government has been considering and discussing with the airline sector a digital ID for travel.

The Risks

Of course, with every innovation there are benefits and risks. In order to obtain the benefits, it is important to reduce the risks wherever possible. That is why I outlined the understandings above. Taking all those steps would reduce the risks of misuse.

There is another risk and that is the federal government or other provinces taking the lead and developing their version of a digital ID and we in Saskatchewan end up having no choice but to do the same.

Finally, there is a risk that big tech companies from other countries develop their own digital ID and we in Saskatchewan lose total control of what we would want a digital ID to be. For example, Apple, Google and Microsoft have backed a password / sign-in standard created by the Fast Identity Online [FIDO] Alliance and the World Wide Web Consortium.

A statement issued by the FIDO Alliance claimed such a standard would make the Internet more secure and usable and users could sign in with a fingerprint or their face. Also, [Microsoft](#) has announced it will offer its customers a standardized online identity verification system beginning in August. Through [Microsoft's](#) Entra management systems, which include Verified ID, it offers users the ability to identify oneself to entities that require user verification.

The Future

In a research study, Juniper Research revealed that digital ID users worldwide will reach 6.5 billion by 2026. This is an increase of 50% from 4.2 billion users. Citizens in Saskatchewan need this service as will many around the world.

I would hope the Government of Saskatchewan continues to consult, educate and explain the benefits of a digital ID for citizens of our province. My hope is that Saskatchewan develops a digital ID that meets our province's needs, maximizes the benefits and minimizes the risks.

Virtual Health Care

My office is pleased that the Ministry of Health (Ministry) has taken the time to hold public consultations on the future of virtual care in Saskatchewan. As noted in the Ministry's "[Saskatchewan Expanding Virtual Health Care Options](#)", utilization of virtual care has increased over the pandemic as patients embraced this new virtual and digital way of engaging with the health care community. Also noted is that careful consideration will be required to ensure that personal health information is adequately protected. My office is in complete agreement with that statement.

Because of the pandemic, the shift to virtual care came quickly, maybe without enough time for a thorough examination of it that shift in service model could adversely impact access and privacy rights. In particular, new working relationships were forged with vendors/service providers/information management service providers (companies) that were at the heart of platform/application/service design, without necessarily ensuring that all of the pieces of the puzzle were in place in terms of ensuring compliance with HIPA or other applicable privacy laws (i.e., private sector privacy laws like the *Personal Information Protection and Electronic Documents Act*). The opportunity now, before forging ahead further, is to fully scrutinize those working relationships and data sharing models to ensure that accountability and transparency is fully integrated into the practices of all engaged parties to prevent surprises down the road in terms of how the data may be leveraged for commercial purposes.

Because of the potential commercial applications, when considering entering into these types of arrangements, it should be anticipated that these companies may try to work around the restrictions placed on use of the data by legal instruments like HIPA by categorizing the data in such a way in an attempt to sidestep privacy regulation. For instance, instead of treating registration information as personal health information, a company may view it as personal information that falls outside of the scope of HIPA. Alternatively, the company may assume that once the data is de-identified, it is free to use for its own purposes whether there are reidentification or other concerns. These concerns would need to be explored with what I understood to be approximately 62 commercial platform providers that will only grow in number as time passes.

To ensure due diligence is done, my office recommends the following as these virtual care initiatives move forward:

1. For each new virtual care service, a privacy impact assessment (PIA) be completed and reviewed by my office to ensure a thorough threat risk assessment is undertaken. This exercise should include clearly defining what constitutes personal health information, personal information and de-identified data and examine any secondary uses and disclosures of that data proposed by the company to prevent function creep.
2. That custody or control of personal health information of patients remains with the trustee, not the vendor/service provider.
3. That for every virtual care service, written agreements are entered into by the parties that are in compliance with HIPA, in particular section 18. These agreements need to clearly identify all third parties/sub-contractors and ensure that rules and expectations extend to all including any cloud service providers.
4. That technical requirements are fully analyzed before written agreements are entered into to ensure that necessary access restrictions, logging and audit capabilities are built into the system as retrofitting may prove too costly down the road to be pursued.
5. That a broad communication strategy that takes into consideration different constituency groups be implemented with each new initiative to ensure that patients receive timely information on what the service entails, what the complaint mechanisms are and how consent will be managed.
6. That stipulated in any written agreement/contract is the requirement for all parties engaged to have comprehensive policies and procedures to ensure compliance with HIPA in particular, sections 16 and 23.
7. That as another accountability mechanism, responsibility is clear in terms of how the parties will work together to manage patient access/correction requests and investigate privacy complaints and cybersecurity incidents in a timely fashion.
8. That the life cycle of information is taken into consideration including termination of any agreement to reflect the continuing duties of trustees as noted in section 22 of HIPA.
9. That built in as a contractual requirement of all parties, contractors and employees, is that access/privacy training be provided on an annual basis.
10. That all agreements entered into by the parties indicate that the patients' personal health information shall be deleted from the service providers systems at the request of the patient, the termination of the contract with the trustee or for longer if legally required.

To assist with the above, my office has a number of tools and resources which include the following:

Privacy Impact Assessment – A Guidance Document

<https://oipc.sk.ca/assets/privacy-impact-assessment-guidance-document.pdf>

eCommunications – Considerations for trustees to protect personal information when using eCommunication tools

<https://oipc.sk.ca/assets/eCommunication-guidelines.pdf>

Auditing and Monitoring Guidelines for Trustees

<https://oipc.sk.ca/assets/audit-and-monitoring-guidelines-for-trustees.pdf>

One last point that needs to be raised is what my office views as a troubling gap in the definition of trustee in HIPA. In a number of investigations over the years, my office has identified cases where although health care professionals were engaged, a non-trustee was found to have custody or control of the personal health information involved. This is unacceptable as in those cases, there is no access or privacy legislative regime or independent oversight to hold parties accountable. In order to address that gap, my office has recommended an amendment to the definition of trustee in HIPA as follows:

2(t)...

(xv) a person who operates a facility whose primary purpose is the provision of health services provided by health professionals licensed or registered pursuant to an Act.

My office once again is recommending that the Government of Saskatchewan amend HIPA to expand the definition of trustee as noted above.

Spotlight on Misdirected Faxes

This past year, my office issued [Investigation Report 045-2021 et al.](#), which was about 23 misdirected faxes. 19 of these faxes involved electronic systems with a faxing feature. For over 10 years, my office has attempted to put the spotlight on the systemic issue of faxes containing sensitive personal health information being sent astray to incorrect recipients. This issue not only impacts patient privacy but also the delivery of timely patient care.

In [2010](#), my office dealt with faxes being continuously missent to a business who inherited the former fax number of a medical clinic. In [2014](#), my office learned that electronic systems replacing the traditional fax machine only multiplied the issue of missent faxes to incorrect recipients. From 2017 to 2020, my office dealt with misdirected faxes resulting from the misdialing of fax numbers on the traditional fax machine to the mis-selection of similar physician names on electronic systems. Given the complexity of our province's health care system, there are no easy solutions to this systemic issue. However, we must continue working towards eliminating misdirected faxes and ensure patients' personal health information is delivered to intended recipients in a timely and accurate manner.

In my Investigation Report 045-2021 et al., I made several recommendations including that the Minister of Health amend HIPA so that trustees must complete privacy impact assessments. When proposing and designing new systems, the process of completing a privacy impact assessment will help trustees anticipate risks that lead to misdirected faxes and come up with ways to mitigate such risks. In terms of existing systems, I recommended that trustees such as the Saskatchewan Health Authority and Saskatchewan Cancer Agency find IT solutions such as prompts that could be added to existing systems so that users are prompted to verify data that has been entered. Finally, I also recommended that trustees work towards eliminating the use of traditional fax machines.

Recommendations for Change

As we finalized this Annual Report, I realized that we have issued over 845 review and investigation reports. They are all posted on our website. Many recommendations have been made for legislative change. [FOIP](#) is now 30 years old and recommendations for legislative change have been made since 2014. It seemed like the time to make a summary of recommendations for legislative changes. Below you will find a summary of the recommendations to amend FOIP, LA FOIP and HIPA. These reports can be found on our [website](#) or on [CANLII](#).

Amendments to FOIP		
Amendments	Report #	Explanation
Chief Coroners Office, amend Appendix [section 3] Part I	Review Report 056-2014 para [26]	Amendments made
Saskatchewan Regional Parks Assoc.	Review Report 266-2020, 213-2021 para [36]	paras [8] to [12]
Amend 7(2)(c) to reduce timeframe from 90 days to 30 days	Review Report 107-2018 para [21]	para [16]
Amend 7(4) to narrow scope and bring in line with other provinces	Review Report 035-2015 para [34]	paras [8] and [9]
Amend 7(4) to narrow scope and bring in line with other provinces	Review Report 223-2015, 224-2015 para [36]	paras [10] and [11]
Extend privacy protection of PI to member of Legislative Assembly or members of Executive Council	Investigation Report 092-2015 to 095-2015 para [108] point a)	Amendments made
Amend 23(3)(c) of FOIP: repeal section 23(3)(c) of FOIP so that section 74 of CFSa is no longer included in that section	Review Report 054-2020 para [21]	para [8] to [19]
	Review Report 254-2017 para [59]	paras [13] to [18]
	Review Report 150-2018 para [49]	paras [29] to [42]
	Review Report 145-2020 [22]	paras [10] to [20]
Amend 24(1) of FOIP	Review Report 146-2017 para [57]	paras [22] to [50]
	Review Report 063-2017 para [22]	paras [6] to [18]
	Investigation Report 190-2018 para [19]	para [3] to [11]

Amendments to FOIP (continued)

Amend 24 (1.2)	Review Report 169-2020 para [29]	paras [7] to [22]
	Investigation Report 087-2020 para [33]	paras [25] to [29]
	Investigation Report 199-2020 para [25]	paras [7] to [21]
Amend FOIP regulations allowing for provision of records electronically	Review Report 146-2015, 147-2015 para [49]	
Introduce new section that protects PI in possession and control of contractors, consultants and IT specialists which is modelled in part on section 18 of HIPA	Investigation Report 131-2015 para [31]	Amendment made see section 24.2
Amend FOIP Regulations to identify Physician Remuneration as information that should be released	Investigation Report 173-2015 para [29] Review Report 082-2019, 083-2019 para [130]	Amendment made see section 24.2 paras [86] to [120]
	Review Report 342-2019 para [73]	paras [49] to [66]
Amend FOIP to include in act or regulations a provision respecting datasets similar to 20(4) of Newfoundland's <i>Access to Information and Privacy Act, 2015</i>	Review Report 057-2019 para [33]	paras [8] to [16]
Amend definition of third party that excludes both Government Institutions and Local Authorities	Review Report 080-2018 para [95]	paras [51] to [53]
An amendment to clarify the rules for interagency sharing in FOIP, LA FOIP and HIPA including a requirement for partner agencies to enter into written information sharing agreements when they participate in common integrated program delivery.	Investigation Report 105-2014 para [80] , point 3	Amendments made in FOIP regulations s.17.1, LA FOIP s.10.1 and HIPA s.5.2

Amendments to LA FOIP

Amendments	Report #	Explanation
Make Watershed Associations a local authority	Review Report 019-2018 para [23]	paras [5] to [17]
Make Regional Parks local authorities	Review Report 184-2020 para [26]	para [22]
	Review Report 121-2019, 122-2019 para [32]	paras [8] to [21]
Make Development Appeals Board a local authority	Review Report 020-2018 para [46]	paras [28] to [30]
Amend 7(2)(c) to reduce timeframe from 90 days to 30 days	Review Report 107-2018 para [21]	paras [8] to [17]
Amend 7(4) to narrow scope and bring in line with other provinces	Review Report 035-2015 para [34]	paras [7] to [11]
	Review Report 223-2015, 224-2015 para [36]	paras [10] and [13]
Amend definition of third party that excludes both Government Institutions and Local Authorities	Review Report 080-2018 para [95]	paras [47] to [53]
An amendment to clarify the rules for interagency sharing in FOIP, LA FOIP and HIPA including a requirement for partner agencies to enter into written information sharing agreements when they participate in common integrated program delivery.	Investigation Report 105-2014 para [80] , point 3	Amendments made in FOIP regulations s.17.1, LA FOIP s.10.1 and HIPA s.5.2

Amendments to HIPA

Amendments	Report #	Explanation
Designate 3sHealth as a health care organization	Review Report 082-2015 para [68]	paras [40] and [41]
Amend legislation to include massage therapists as trustees	Investigation Report 161-2015 para [35]	Will occur when The Massage Therapist Act is proclaimed
Amend 2(t) to work on ways to protect PHI when a Physician leaves a practice, owner sells a facility, etc.	Investigation Report 183-2016, 186-2016, 187-2016 para [33]	paras [26] and [27]
Broaden the definition of trustee (section 2(t)) to include organizations whose primary purpose is the provision of health services	Investigation Report 022-2018 para [24]	paras [11] to [14]
Amend 4(4)(h) to have all or part of Part IV apply to WCB regarding collection of PHI	Investigation Report 046-2014 para [54]	Amendment in FOIP to deal with issue.

Amendments to HIPA (continued)

Amend 6.4(1) of HIPA Regulations	Investigation Report 008-2017 para [48]	Amendment made to HIPA Regulations
Amend 26(2) to include trustee authorization for the use of PHI about an individual for educating employees	Investigation Report 161-2018 para [171]	paras [138] and [139]
	Investigation Report 180-2018, 181-2018, 226-2018 para [45]	paras [29] and [30]
Amend HIPA Regulations regarding the disclosure of PHI to physicians for the purpose of complying with <i>The Workers' Compensation Act</i>	Investigation Report 255-2017, 256-2017 para [110]	paras [95] and [96]
Amend HIPA to require every trustee to have a written retention schedule for PHI	Review Report 201-2016 para [26]	paras [18] and [19]
Amend HIPA to exclude raw data from standardized testing	Review Report 027-2018 para [63]	paras [31] to [45]
Amend HIPA Regulations to clarify the rules for interagency sharing in FOIP, LA FOIP and HIPA including a requirement for partner agencies to enter into written information sharing agreements when they participate in common integrated program delivery.	Investigation Report 105-2014 para [80] , point 3	Amendments made in FOIP regulations s.17.1, LA FOIP s.10.1 and HIPA s.5.2
Amend HIPA so that trustee must complete PIA's with respect to proposed systems, projects, programs or activities	Investigation Report 045-2021 et al. [53]	para [13]
Amend HIPA so that trustees must notify my office of theft, loss, or unauthorized use or disclosure of personal health information.	Investigation Report 045-2021 et al. [54]	para [13]



Office of the
Saskatchewan Information
and Privacy Commissioner

503 - 1801 Hamilton Street
Regina SK S4P 4B4

Phone: 306-787-8350
Toll Free: 1-877-748-2298

Email: webmaster@oipc.sk.ca
Twitter: @SaskIPC

WWW.OIPC.SK.CA