



Office of the
Saskatchewan Information
and Privacy Commissioner

ANNUAL REPORT 2019-2020

Issues in a
Pandemic



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
Fax: 306-798-1603

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

June 29, 2020

Hon. Mark Docherty
Speaker of the Legislative Assembly
129 Legislative Building
Regina, Saskatchewan
S4S 0B3

Dear Mr. Speaker:

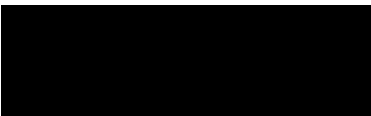
I am pleased to present my sixth Annual Report as Information and Privacy Commissioner for Saskatchewan. I have prepared this Annual Report in accordance with the provisions of subsection 62(1) of *The Freedom of Information and Protection of Privacy Act*, subsection 52(1) of *The Local Authority Freedom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

The pandemic in Saskatchewan, Canada and the World has shifted our focus and caused many of us to make significant changes to our lives at work. On March 20, 2020, my office was closed and we quickly developed a plan to have all staff working from home. Our front door was closed but the work of the office through telephone, email, conference calls and video conferences has continued. We have had to become more flexible with timelines but continue to insist that access and privacy legislation is still in force. As of the date of filing this report, my office is still closed and staff continue to work from home.

I thank the Members of the Legislative Assembly for their support of the Office of the Information and Privacy Commissioner. Going forward, I ask for their cooperation 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 the office for their hard work over the last year in accomplishing some ambitious goals and continuing to complete our three-year plan. My office has also been faced with increased requests for reviews or investigations which continue to put pressure on the office to get reports out in a timely manner. Finally, I thank staff for their willingness to adjust their lives and work lives to provide services to Saskatchewan residents even though our front doors were closed.

Respectfully submitted,



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

Table of Contents

Commissioner's Message	1
About Us	2
Accomplishments 2019-2020	3
The Plan 2020-2021	7
Files and Reports	9
Issues in a Pandemic	14

Commissioner's Message



This year, 2019-2020, is the third year in our three year plan and in this Report, I will report on our progress on the goals in the plan. In the spring of 2020, my office will be developing its next three year plan.

In my Annual Report for 2016-2017, I addressed the issues relating to “Navigating in a Digital World”. So much of what we do today is now electronic and my office and society needs to continue to adjust its approaches to access and privacy in this digital world.

In the *2017-2018 Annual Report*, “Reducing the Risks”, I focused further on how, in our digital world, organizations may reduce the risk of privacy breaches. Breaches can occur with paper files, but most of the noteworthy breaches today involve electronic files that generally impact thousands of people.

When *The Freedom of Information and Protection of Privacy Act* and *The Local Authority Freedom of Information and Protection of Privacy Act* (1992-1993) were implemented, we as a society were aware of the internet but weren’t really using it. Databases existed but weren’t in use to the extent they are now and generally were not accessible by the internet. We were a paper based society. In 2020, for the most part, we are no longer a paper based society. A vast amount of information about each of us is housed in databases, some of which are accessible by the internet. We look up information, we order things, and we pay bills and communicate with one another through the utilization of these databases and the internet. It is time that we modernize our access and privacy legislation to take this into account. The remainder of my term will really be focused on modernizing this legislation to take into account the database/internet world we now live in.

There continues to be a need to focus on continuous education on access and privacy issues. My office issued 16 reports regarding the Village of Pinehouse and 14 of those reports dealt with the process under the legislation. I have heard the message that there is a real need for training and education in the municipal sector. Municipal administrators come and go and elected officials come and go. This to me suggests that education must be continuous and offered regularly.

Security experts will say that many breaches in an organization occurred because of staff. In other words, the breach is from the inside or staff actions internally make breaches from the outside easier. It had been indicated that a good proportion of breaches are caused or facilitated by actions from the inside. The main solution is continuous education of employees in an organization.

I am looking forward to my seventh year as Commissioner and to the development of a new three year plan.

I want to express my appreciation to the staff of the office for their hard work, dedication and commitment to ensuring access and privacy rights are afforded to the citizens of Saskatchewan. I also want to thank our many stakeholders including applicants, complainants, public bodies, and health trustees for their continued cooperation with our office.

The fiscal year, 2019-2020, ended in a dramatic fashion. On March 20, 2020, my office closed its doors and switched to operating with all staff working from home. It took a week to get organized but after that, the office has been able to provide good service to the citizens of Saskatchewan.

Finally, I want to thank the members of the board of internal economy and the Members of the Legislative Assembly for their continued support.

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

About Us

Our Mandate

The Office of the Saskatchewan Information and Privacy Commissioner (IPC) is an independent office of the Saskatchewan Legislative Assembly. It oversees three Saskatchewan statutes: *The Freedom of Information and Protection of Privacy Act* (FOIP); *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP); and *The Health Information Protection Act* (HIPA).

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

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

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

Our Mission

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

Accomplishments 2019-2020

Education and Awareness

Goals	Accomplishments
Update the online <i>Dictionary</i> .	The online <i>Dictionary</i> was updated.
Redesign the <i>IPC Guide to Exemptions</i> as a guide to FOIP.	Launched in December 2019.
Participate in/develop an event with the media to promote Right to Know week in Saskatchewan.	Organized an event in Saskatoon in September 2019.
Update <i>The Rules of Procedure</i> regarding solicitor-client privilege.	<i>The Rules of Procedure</i> are up to date.
Promote annual access and privacy training for employees within public bodies and health trustees.	Has been promoted in speeches and presentations and made as a recommendation in reports investigating privacy breaches.
Support a conference sponsored by the Ministry of Justice in 2019.	Supported that conference in June 2019.
Work with SUMA, SARM and the SSBA to provide education and training to elected officials, including attendance at either convention.	Worked with SUMA, UMASS and RMAA on six regional workshops with a segment on access and privacy.
Develop a Sample policy for processing access requests for towns, villages and municipalities.	<i>Sample Operational Policy for Municipalities</i> completed and posted.
Participate in a webinar with SUMA for villages, towns and municipalities on the application of and obligations imposed by LA FOIP.	A webinar entitled, <i>LA FOIP 101: What Municipalities Need to Know</i> , was delivered on April 29, 2019.
Update the <i>IPC Guide to HIPA</i> and post to the website.	The <i>IPC Guide to HIPA</i> was updated.
Update Q&A resources for MLAs and Ministers and post to the website.	The <i>Q&A resources for MLAs and Ministers</i> were updated.

Navigating in a Digital World

Goals	Accomplishments
Implement a process that can be used by public bodies to send electronic files securely to the IPC.	Liquid files licensed and made operational to securely send and receive documents or records.
Promote government having a new approach and system for the retention and archiving of emails where retrieval is possible at a low cost.	Government has developed such a system.
Promote and work with the Ministry of Central Services to develop a government strategy regarding the use and destruction of backup tapes.	Investigation Report 072-2018 was issued with recommendations dealing with backup tapes and Central Services has developed a plan to deal with backup tapes.
Develop eCommunication guidelines.	This eCommunication tool was posted to our website April 2019 and is intended to provide general advice to trustees on how to protect personal health information.

Advocating for Improvement

Goals	Accomplishments
Promote and work with the Ministry of Justice to develop further proposals for amendments to FOIP and LA FOIP and their regulations.	Proposals have been given for FOIP and LA FOIP regulation amendments.
Promote and work with the Ministry of Health to develop further proposals for amendments to HIPA and its regulations.	Proposals have been given for amendments to HIPA regulations.
Implement regulations for <i>The Data Matching Agreements Act</i> .	Worked with the Ministry of Justice regarding the regulations under this Act (it is not yet in force).
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).	Continue to promote.
Promote that all organizations who contract with government or local authorities will be subject to Part IV of FOIP or LA FOIP (Protection of Privacy).	Continue to promote.

Advocating for Improvement (cont'd)

Goals	Accomplishments
Promote that all publicly funded bodies who are landlords be under FOIP or LA FOIP.	Continue to promote and propose that housing authorities be local authorities under LA FOIP regulations.
Promote a broader definition of “trustee” under HIPA or other legislation.	Continue to promote.
Work with the Ministry of Justice to develop regulations under <i>The Interpersonal Violence Disclosure Protocol Act</i> (Clare’s Law).	Worked with the Ministry of Justice regarding the regulations and protocol under this Act.
Promote an amendment to <i>The Education Act</i> similar to section 117 of <i>The Municipalities Act</i> .	Continue to promote.
Promote the updating of <i>The Model Professions Act</i> and promote that professional bodies will be subject to Part IV of LA FOIP or HIPA (Protection of Privacy).	Continue to promote.
Promote and work with the Ministry of Justice to ensure lists of government institutions and local authorities are up to date.	Have requested FOIP and LA FOIP regulation amendments to include government institutions and local authorities.
Implement amendments to <i>The Workers’ Compensation Amendment Act, 2019</i> (Bill 141).	Amendments implemented on November 15, 2019.

Effective While Efficient

Goals	Accomplishments
Issue a notification letter or resolve a matter within 20 calendar days.	25 calendar days.
Issue a Report or resolve a matter on review of an access request within 130 calendar days.	210 calendar days.
Issue a Report or resolve a matter regarding a breach of privacy within 130 calendar days.	264 calendar days.
Complete or close consultation files within 30 calendar days.	13 calendar days.

Effective While Efficient (cont'd)

Goals	Accomplishments
Complete or close applications to disregard within 20 calendar days.	15 calendar days.
Implement Data by Design releases 3, 4 and 5.	Release 4 implemented. Requirements for Release 5 defined.
Recruit and train two Analysts.	Completed.
On the website complete a project to convert all pdf documents to HTML and develop a categories function.	All pdf documents of 10 pages or less have been converted to HTML and a categories function was developed.
Develop forms related to the office's policies and guidelines.	75% of forms have been developed.
Review and update policies and guidelines.	Completed and policies submitted to the Board of Internal Economy.

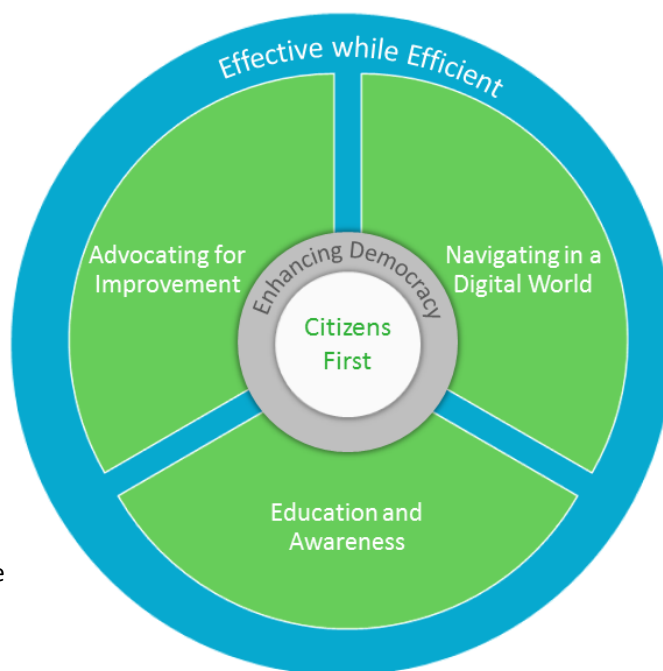
The Plan 2020-2021

Citizens First

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. All other objectives in this document are intended to enhance and protect the rights of citizens to obtain information.

Enhancing Democracy

The freedom of information legislation in the province enshrines the principle that citizens should have access to information 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

- Update resources to ensure that amendments to FOIP, LA FOIP and HIPA are captured in educational material.
- Continue to update and expand the *IPC Guide to FOIP* and the *IPC Guide to HIPA*. Develop a similar guide for *LA FOIP*.
- Promote mandatory annual access and privacy training for employees within public bodies and health trustees.
- Develop and post a [Pandemic Binder](#) containing the access and privacy issues caused by the Pandemic.

Navigating in a Digital World

- Develop and post to the website a document on [Best Practices for the Management of Non-work Related Personal Emails in Work-Issued Email Accounts: A Guide for Public Bodies](#).
- Promote ways for public bodies and health trustees to deliver electronic information securely.
- Promote a workshop in Regina, Saskatoon and Prince Albert that is lived streamed for municipal officials and administrators involving Government Relations, SUMA, SARM, UMAAS and RMAA.

Advocating for Improvement

- Promote and work with the Ministry of Justice to modernize access and privacy legislation recognizing that we have moved from a paper to a digital society.
- Promote and work with the Ministry of Health to modernize HIPA recognizing that we have moved from a paper to a digital society.
- Promote and work with the Ministry of Health to develop HIPA Regulation amendments including broadening the definition of a “trustee”.
- Promote and work with the Ministry of Justice to develop regulation amendments to FOIP and LA FOIP including updating the lists of government institutions or local authorities.
- Promote and work with the Ministry of Justice on updating *The Model Professions Act* and promote that professional bodies will be subject to Part IV of LA FOIP or HIPA (Protection of Privacy).
- Promote an amendment to *The Education Act* similar to section 117 of *The Municipalities Act*.
- 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).

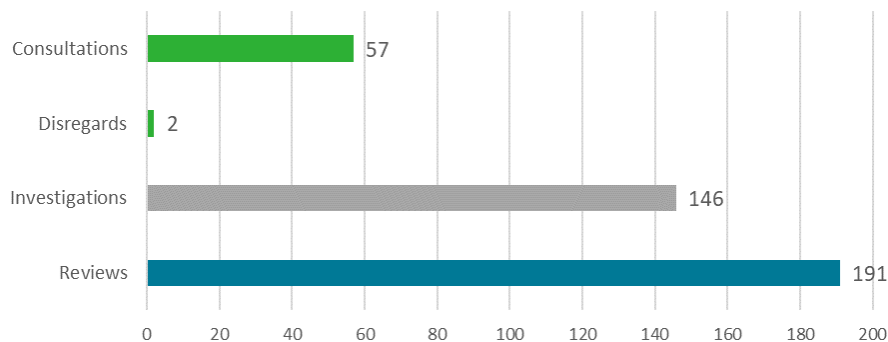
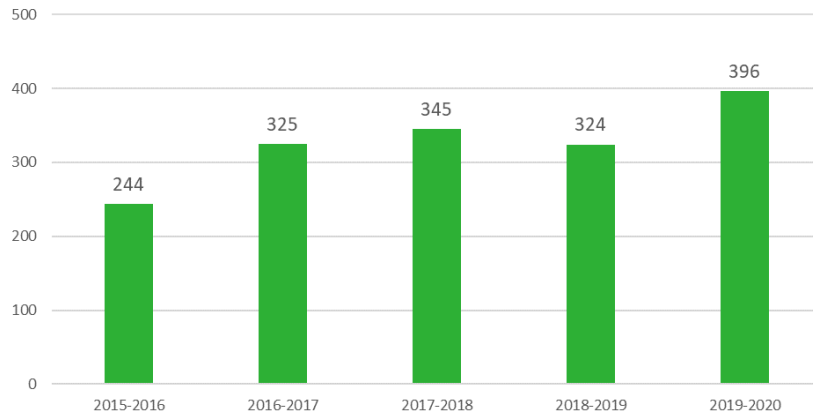
Effective While Efficient

- Manage the increasing caseload so that citizens obtain results in a reasonable period of time.
- Resolve a matter by early resolution within 30 calendar days.
- Complete or close consultation files within 30 calendar days.
- Issue a report or resolve a matter on review of an access request within 130 calendar days.
- Issue a report or resolve a matter regarding a breach of privacy within 130 calendar days.
- Complete or close a consultation file within 30 calendar days.
- Respond to an application to disregard within 20 calendar days.

Files and Reports

Increase in Files

The office is experiencing an increase in reviews, investigations and consultations, resulting in more files being opened as is reflected in the bar chart. This resulted in a 22% increase over the previous fiscal year.

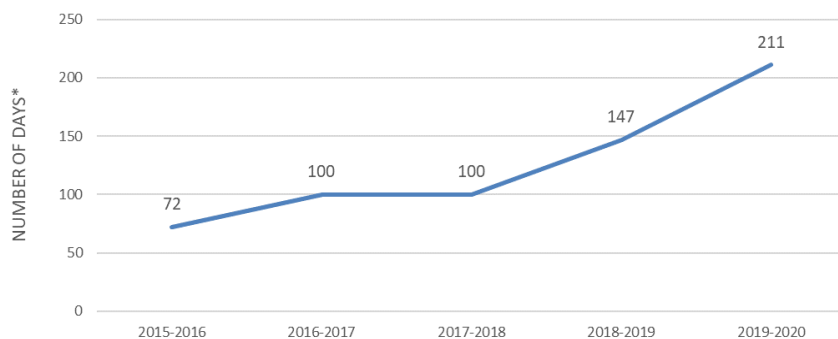


Types of Files Opened

The office opened 396 files in the 2019-2020 fiscal year. This is a chart summarizing the types of files opened.

Response Time

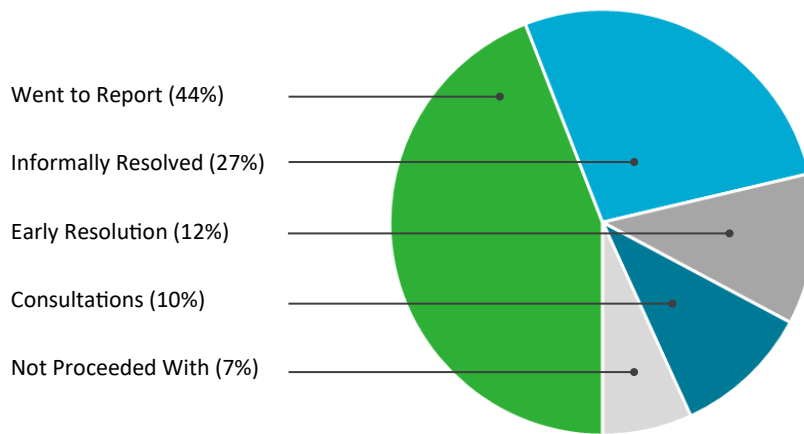
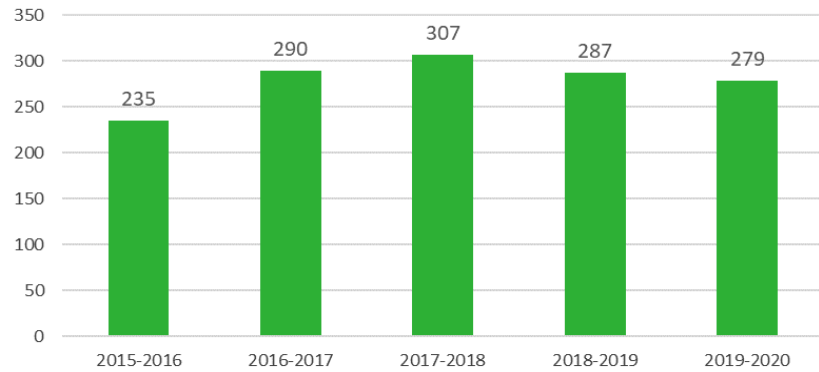
The office has worked hard to improve its response time to citizens and public bodies. In 2019-2020, the response time increased mainly due to the volume of new files. There was a 44% increase in response times in 2019-2020.



*Average number of days that citizens and public bodies received their report, response or a resolution.

Files Closed

Due to workload pressures, the office has gone from closing 307 files in 2017-2018 to 279 files in 2019-2020.

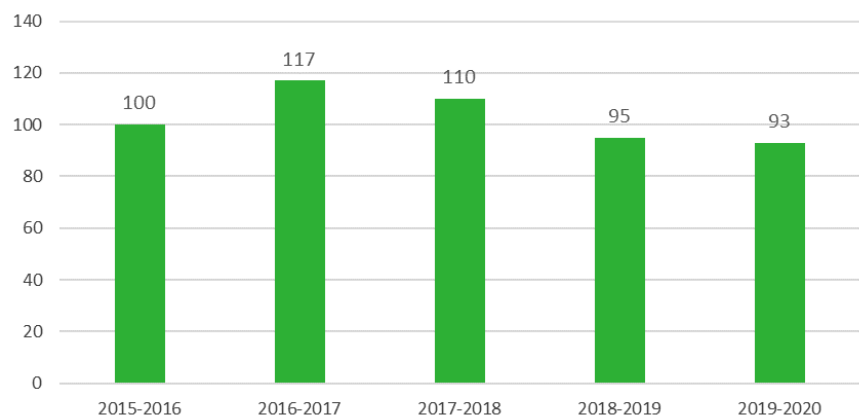


Resolution of Files

The office closed 279 files in the 2019-2020 fiscal year. This is a chart summarizing the percentages of files resolved in different ways, including issuance of a Report.

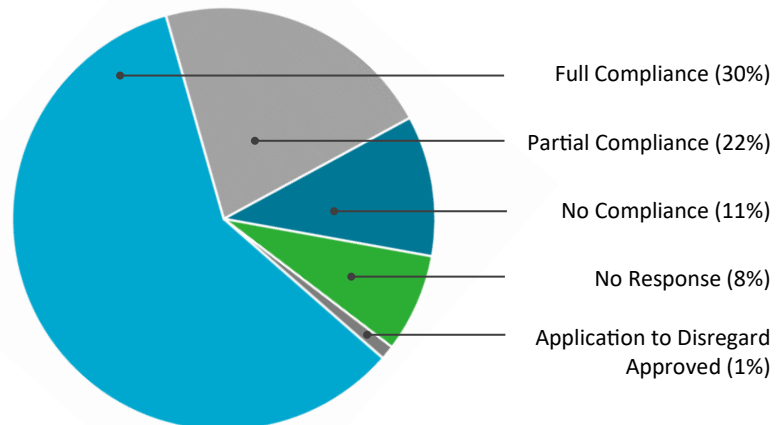
Reports Issued

Due to the increased workload, the number of Reports issued has gone from 117 in 2016-2017 to 93 in 2019-2020.



Compliance with Recommendations

The office issued 93 Reports in the 2019-2020 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 an application to disregard was approved.



My office is obligated to report on the recommendations that were not complied with.

See subsection 62(2) of FOIP, subsection 52(2) of LA FOIP and subsection 60(2) of HIPA. 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 that responded to a Report with partial compliance; the second table lists those public bodies that responded to a Report with no compliance; the third table lists those public bodies that did not respond at all.

Partial Compliance

Government Institution	Report #	Recommendation(s) not or partially complied with*
eHealth Saskatchewan	Review Report 160-2019, 161-2019, 162-2019	[41]
eHealth Saskatchewan	Review Report 171-2018, 189-2018	[142] , [143]
Ministry of Central Services	Review Report 135-2019	[62]
Ministry of Corrections and Policing	Review Report 036-2019, 077-2019	[38]
Ministry of Corrections and Policing	Review Report 130-2019	[39]
Ministry of Corrections and Policing	Investigation Report 322-2017, 120-2018	[63]
Ministry of Education	Review Report 034-2019	[49]
Ministry of Energy and Resources	Review Report 113-2019	[26]
Ministry of Health	Review Report 079-2018	[84]
Ministry of Health	Review Report 081-2018	[117]
Ministry of Social Services	Review Report 150-2018	[47]
Ministry of Social Services	Review Report 254-2017	[58] , [59] , [60]
Saskatchewan Telecommunications	Review Report 119-2018	[164] , [168] , [174] , [175]
Saskatchewan Telecommunications	Review Report 149-2019, 191-2019	[97] , [98] , [99]

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

Partial Compliance

Local Authority	Report #	Recommendation(s) not or partially complied with*
City of Regina	Review Report 108-2019	[163] , [164]
Northern Village of Pinehouse	Review Report 027-2019	[57]
Resort Village of Candle Lake	Review Report 252-2018	[66] , [67]
Rocanville Parks and Recreation Board	Investigation Report 074-2018, 075-2018	[55]
Saskatoon Police Service	Review Report 023-2019, 098-2019	[110]
Town of Rocanville,	Investigation Report 074-2018, 075-2018	[55]
Health Trustee	Report #	Recommendation(s) not or partially complied with*
Dr. Mary Vandergoot	Review Report 027-2018	[60]

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

No Compliance

Government Institution	Report #	Recommendation(s) not complied with*
Ministry of Central Services	Review Report 186-2019	[33]
Ministry of Corrections and Policing	Review Report 131-2019	[28]
Ministry of Health	Review Report 244-2018	[150]
Ministry of Social Services	Review Report 149-2017	[103] , [104]
Saskatchewan Government Insurance	Investigation Report 190-2018	[19]
Saskatchewan Legal Aid Commission	Investigation Report 200-2018	[49] , [50]
Local Authority	Report #	Recommendation(s) not complied with*
Regina Police Service	Review Report 084-2019	[23]
R.M. of Rocanville	Investigation Report 074-2018, 075-2018	[56] , [57] , [58]
Saskatoon Downtown Business Improvement District	Review Report 064-2019	[41]
Saskatoon Police Service	Review Report 157-2019	[19]
Saskatoon Riversdale Business Improvement District	Review Report 020-2019, 087-2019	[39] , [40]

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

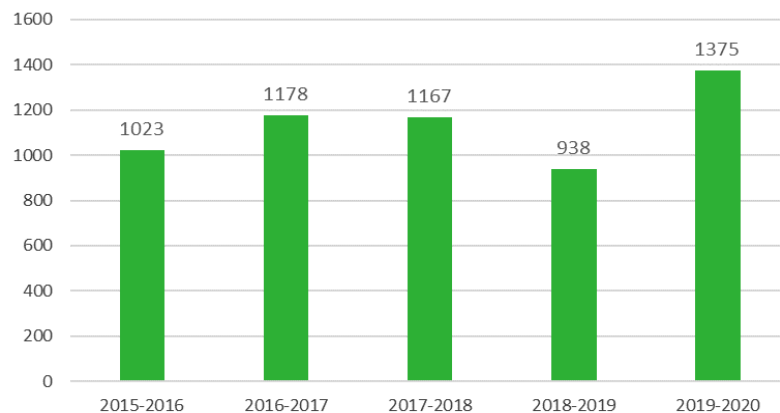
No Response Received

Local Authority	Report #	Recommendation(s) not complied with*
Northern Village Pinehouse	Review Report 040-2019	[54], [55], [56], [57]
Northern Village Pinehouse	Review Report 066-2019	[25], [26], [27], [28]
R.M. of Blaine Lake	Investigation Report 298-2018	[11], [12], [13]
R.M. of Blaine Lake	Review Report 088-2019	[22]
R.M. of Blaine Lake	Review Report 132-2019	[39], [40], [41], [42], [43]
Resort Village of Candle Lake	Investigation Report 136-2018	[12]
Resort Village of Candle Lake	Review Report 049-2019	[54], [55], [56], [57]

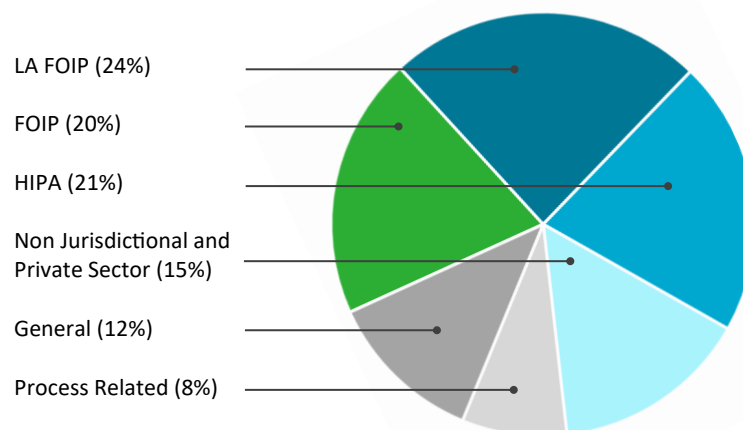
*Refers to paragraph # in the Report. Click on the link to go directly to the Report.

Requests for Advice

The mandate of the office is to provide education and a good portion of that education takes the form of people contacting the office and obtaining advice. In 2019-2020, the office provided summary advice on 1,375 occasions. This is a 47% increase over advice provided in the last fiscal year.



From the chart below, it is clear that the office gives advice related to the three main statutes where the office has jurisdiction; 65% of summary advice was given related to these pieces of legislation.



Issues in a Pandemic

In this pandemic, issues have arisen which have created considerable discussion and debate. Freedom of information and privacy legislation is not suspended during a pandemic and public bodies are still required to follow these statutes. At the same time, some public bodies are operating in extremely difficult and stressful times. The temptation can be to ignore access rules and privacy rules because we are fighting COVID-19. Ignoring the rules is not an option. In fact, I believe public bodies can fight the virus, provide information to the public and protect individual privacy. All they have to do is think carefully before acting and in the process, balance competing interests.

Access to Information

The question has been raised: *What about access requests during a pandemic?*

In Saskatchewan, FOIP, LA FOIP, and HIPA are still in force. Citizens of Saskatchewan still have the right to request records. Public bodies are still required to accept and process access requests. If access officers are assigned to pandemic or other essential issues, this might delay the process, but should not stop it. In other instances, public bodies have designated access officers who may be working from home, and the processing of access requests should continue. It might not be quite as efficient, but it can and should continue. Public bodies, when faced with a heavier than normal workload on access requests, can consider an extension but no public body should just refuse to process requests. If someone is working from home, they may need access to records which are at the office. Before stopping work on the request, the public body should explore other ways of getting the record. It might be slower, but the process can still move forward. Of course, with electronic records, working from home may still allow access to the necessary records.

When access requests focus on COVID-19, I would ask public bodies to accelerate those requests and give them priority because of the public interest. Citizens are naturally concerned and worried about the situation. Being transparent can reduce the anxiety that is in society right now. Getting an answer 30 or 60 days from now will not be of much assistance to the citizen.

Transparency

We are in the middle of a pandemic and many are working hard to protect Saskatchewan. Many are working long hours and are assuming risks. All of us need a certain amount of information about the spread of COVID-19 in our province.

I discuss privacy below and clearly there is a balancing act between public interest and privacy. There is a big gap between giving little to no information and giving all information. In the middle is an opportunity for decision-makers to determine how much information to provide to the public. Officials are always free to provide aggregate or statistical data or de-identified personal information or personal health information. They can provide information such as how many are sick or pass away in a city, town, municipality, area or region. I would encourage as much transparency as is possible while respecting privacy to the extent possible. More is better under the circumstances we are now in.

Of course, giving someone's name and address as being affected would be going too far as this is their personal health information. Yes and maybe in small communities, indicating one person is affected, would potentially identify that person. In those instances, there are work-a-rounds such as saying, "one person in the Ituna vicinity" or "one person north of White City". The idea is that officials can be transparent and provide as much information as is possible, but still avoid identifying an individual.

As the number of cases rise in our province, officials will have more latitude in providing statistical information to citizens as they won't be dealing with one person, but dealing with two, three or more persons in a community or area.

Decision-makers are also free to identify specific events or locations where outbreaks occur. This might involve identifying a specific hospital or nursing care home. Similarly, decision-makers would be free to identify the number of COVID-19 cases in the province, where diabetes, heart conditions, asthma or respiratory issues were complicating factors.

Individuals who are infected with COVID-19 may choose to divulge their personal health information in a public forum such as Facebook, Twitter, Instagram or the media. They may choose to give interviews regarding their illness and recovery. That is their choice and we need to respect that they have voluntarily chosen to do so. If an individual does so, that does not give permission to the public body to release their name. A public body could, however, ask the individual to sign a consent agreeing to the release of their name and details.

The Federal Information Commissioner, Caroline Maynard, in a [News Release](#) dated April 2, 2020 stated:

As Information Commissioner, I call upon heads of federal institutions to set the example in this regard, by providing clear direction and updating guidance on how information is to be managed in this new operating environment. Furthermore, I am of the firm view that institutions ought to display leadership by proactively disclosing information that is of fundamental interest to Canadians, particularly during this time of crisis when Canadians are looking for trust and reassurance from their government without undue delays.

The right of access is a means by which we not only hold our government to account, but determine how and why decisions were made and actions taken, in order to learn and find ways to do better in the future. It is only by being fully transparent, and respecting good information management practices and the right of access, that the government can build an open and complete public record of decisions and actions taken during this extraordinary period in our history—one that will inform future public policy decisions.

In conclusion, I ask public officials, elected and appointed, to continue to provide as much information as possible regarding our province and the pandemic.

Privacy

Privacy laws are not a barrier to appropriate information sharing in a pandemic.

It is important that public bodies, health trustees and private sector organizations know how personal information or personal health information may be shared during a pandemic.

How Information may be shared under Saskatchewan's Privacy Laws

Saskatchewan has three privacy laws:

- FOIP applies to government institutions;
- LA FOIP applies to local authorities such as municipalities, universities and school boards; and
- HIPA applies to health trustees.

These Acts and accompanying Regulations govern the collection, use and disclosure of personal information or personal health information.

Each Act contains provisions to allow for the sharing of personal information or personal health information in the event of an emergency by public bodies and trustees.

All three Acts require that any collection, use or disclosure of personal information or personal health information be limited to that which is needed to achieve the purpose of the collection, use or disclosure. This is referred to as the "data minimization principle."

FOIP

FOIP applies to government institutions, which include provincial government ministries, Crown corporations, boards, agencies and commissions.

FOIP permits public bodies to collect personal information if the collection is expressly authorized by another statute or if the collection relates directly to and is necessary for an operating program or activity of the government institution.

FOIP generally requires government institutions to collect personal information directly from the individual. Government Institutions may collect personal information about an individual from other sources with the individual's consent, or without consent in specific circumstances, such as when the collection is authorized by law or the individual is not able to provide the information directly in a health or safety emergency.

Government Institutions may disclose personal information in emergency situations with the consent of the individual, or without consent if certain circumstances exist, including:

- where necessary to protect the mental or physical health or safety of any individual;
- the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure;
- disclosure would clearly benefit the individual to whom the information relates; or
- if the disclosure is authorized by a statute of Saskatchewan or Canada.

LA FOIP

LA FOIP applies to local authorities, including municipalities, universities and school boards. Basically, the same rules apply as outlined above for FOIP.

HIPA

HIPA applies to personal health information in the custody or control of health trustees. Trustees include the Saskatchewan Health Authority, nursing homes, ambulance operators, physicians, pharmacists and certain other health professionals with custody or control of personal health information. HIPA authorizes trustees to collect and use personal health information for the purposes of providing health services.

HIPA allows trustees to disclose personal health information with the consent of the individual, or without consent in specific circumstances, including:

- where the trustee believes, on reasonable grounds, that the disclosure will avoid or minimize a danger to the health or safety of any person;
- to family members or other individuals in a close relationship with the individual so they may be notified that the individual is ill, injured or deceased, providing the disclosure is not contrary to the expressed wishes of the individual;
- to another health trustee for the provision of health services;
- to a person responsible for continuing treatment and care for the individual; or
- if the disclosure is authorized or required by a statute of Saskatchewan.

The Private Sector

Except for trustees under HIPA, Saskatchewan does not have legislation that applies to the private sector. Private sector organizations might be covered by federal legislation and should check the [federal privacy commissioner's website](#). If the private sector however is contracting with a public body or trustee (e.g. information management service provider), contractual agreements should be checked for language that might actually put personal information or personal health information that the private sector has in its physical possession instead of in the control of the public body or trustee.

General Principles

The Canadian Privacy Commissioner, Daniel Therrien, has issued [A Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19](#). In that framework, he establishes key principles which can be applied by public bodies when making decisions on collection in Saskatchewan. He summarizes those principles in his April 17, 2020 [News Release](#). These principles should be applied in Saskatchewan. With some editing, these principles are:

- legal authority: the proposed measures must have a clear legal basis;
- the measures must be necessary and proportionate, and, therefore, be science-based and necessary to achieve a specific identified purpose;
- purpose limitation: personal information and personal health information must be used to protect public health and for no other purpose;
- use de-identified or aggregate data whenever possible;
- exceptional measures should be time-limited and data collected during this period should be destroyed when the crisis ends; and
- transparency and accountability: public bodies should be clear about the basis and the terms applicable to exceptional measures, and be accountable for them.

The Public Health Act, 1994

The Minister of Health or the chief medical health officer have powers under [The Public Health Act, 1994](#). In particular, section 45 sets out the powers of the minister and the chief medical health officer and provides:

Orders

45(1) The minister may make an order described in subsection (2) if the minister believes, on reasonable grounds, that:

- (a) a serious public health threat exists in Saskatchewan; and
- (b) the requirements set out in the order are necessary to decrease or eliminate the serious public health threat.

(2) An order pursuant to this section may:

- (a) direct the closing of a public place;
- (b) restrict travel to or from a specified area of Saskatchewan;
- (c) prohibit public gatherings in a specified area of Saskatchewan;
- (d) in the case of a serious public health threat that is a communicable disease, require any person who is not known to be protected against the communicable disease:
 - (i) to be immunized or given prophylaxis where the disease is one for which immunization or prophylaxis is available; or (ii) to be excluded from school until the danger of infection is past where the person is a pupil;
- (e) establish temporary hospitals;
- (f) require a local authority, a medical health officer or a public health officer to investigate matters relating to the serious public health threat and report to the minister the results of the investigation;
- (g) require any person who, in the opinion of the minister or medical health officer, is likely to have information that is necessary to decrease or eliminate the serious public health threat to disclose that information to the minister or a medical health officer;
- (h) authorize public health officers, peace officers or prescribed persons to confiscate substances or other materials found in any place, premises or vehicle, if those substances or materials are suspected by the public health officer, peace officer or prescribed person of causing or contributing to a serious public health threat or packages, containers or devices containing or suspected of containing any of those substances or materials;
- (i) in the case of a serious public health threat that is a communicable disease, require any person to be isolated from other persons until a medical health officer is satisfied that isolation is no longer necessary to decrease or eliminate the transmission of a communicable disease.

Further, this Act contains mandatory reporting provisions of certain health care professionals in certain circumstances (e.g. sections 32, 34 and 36).

Balancing Public Interest and Privacy

During a pandemic the expectation of citizens and, in fact, their need for public information, grows. The public needs information in order to make decisions on how to best protect themselves and their families. In addition,

as the pandemic continues there are more patients and their right to privacy is a concern to them and their families. Individual privacy – the right to have a degree of control of how one’s information is collected, used, and/or disclosed – is important. Some patients will self-declare and head to Facebook, Twitter, Instagram or do radio and TV interviews. Others will choose to self-isolate and not tell others, possibly even some of their family members. There can be consequences that an individual can face if their personal information or personal health information is accidentally disclosed.

Therefore, protecting an individuals’ right to privacy is important. Decision-makers are faced with how much information they can give to the public. It is truly a balancing act. Sometimes it must be dealt with on a case-by-case basis. The issue is “when does releasing information get to the point that a patient can be identified.”

For those that do get tested, the public health system will investigate and contact those that may have come into contact with that individual as they are identified. When it is unknown, we have seen cases where the public health officials turn to the media, for example in the case that an individual tested positive on an airplane flight. We’ve seen cases where the flight information and seat numbers are released publicly, so those that were on that flight can contact health authorities. This all is done on a need-to-know basis and different methods are utilized depending on the circumstances.

There are other examples in the province. Information was given out regarding a snowmobile rally for the purpose of those who were at the rally contacting health authorities. Information was given out regarding the Lloydminster Hospital and the Prince Albert Victoria Hospital. Information like this allows health authorities to begin the process of contact tracing.

Through this pandemic, my hope is that we can appropriately balance the need for public information and the protection of patient privacy.

Documenting Decisions

During this pandemic, public officials, elected and appointed, have made and will make many decisions in an attempt to flatten the curve to help prevent our health care system from being overwhelmed and to save lives.

In this pandemic, with decisions being required quickly, there continues to be a need to document those decisions. FOIP and LA FOIP, section 5 gives citizens the right to obtain records (with appropriate exceptions). Implicit in all of this is the duty to document the important decisions as they are being made. To be able to respond to that right, public bodies need to create the records. If there are no records, then citizens will never view records of decisions made during this pandemic. Public officials, elected and appointed, should ensure the decisions made and actions taken are documented.

During this time, more decisions may be made electronically. Emails and texts are sent and received. This is particularly true when people are working from home. Officials need to ensure that records, such as documents, emails, and texts are safeguarded and filed according to their records retention and disposal schedules. Further, there may be a need to document decisions made over the telephone. Public officials, elected and appointed, should ensure that all records created during the pandemic, including those electronic communications, are captured as official records unless transitory in nature.

Under [The Archives and Public Records Management Act](#), there is no need to retain transitory records. Guided by the Provincial Archives’ [Guidelines for the Management of Transitory Records](#) the initiator of the communication or the receiver should determine whether something is transitory. Because of the historical significance of the

decisions being made during this pandemic, public officials, elected and appointed, should take a broader approach and treat more of the communications as official records rather than transitory. In other words, narrow what is considered a transitory record and broaden what is considered an official record.

When this pandemic is over, policy analysts, historians and researchers will and should reflect back on decisions and actions taken by officials in Saskatchewan. They will study what worked and what might not have worked. This analysis will better equip us for the next crisis that may come our way.

The Federal Information Commissioner, Caroline Maynard, in a [News Release](#) on April 2, 2020 stated:

Last week the Prime Minister told Canadians that transparency is crucial to being accountable to Parliament and in maintaining the public's confidence.

When the time comes, and it will, for a full accounting of the measures taken and the vast financial resources committed by the government during this emergency, Canadians will expect a comprehensive picture of the data, deliberations and policy decisions that determined the Government's overall response to COVID-19.

Canadians have a fundamental right to this information. They expect that it will be available to them, and that the government will provide it.

...ministers and deputy ministers must ensure that they and their officials generate, capture and keep track of records that document decisions and actions, and that information is being properly managed at all times.

Doing this is a matter of asking the right questions and then providing the information, tools and support employees need to meet their access to information and information management responsibilities.

For example, are minutes of meetings—even those taking place by teleconference or video conference—continuing to be taken and kept? Are all relevant records—such as decisions documented in a string of texts between co-workers—ultimately finding their way into government repositories? Do employees have a clear understanding of what constitutes “a record of business value” and that this record must be preserved for future access?

In conclusion, the best practice in order to fulfill what is outlined in section 5 of FOIP, LA FOIP and *The Archives and Public Records Management Act*, is for public officials, elected and appointed, to ensure their organizations are creating and maintaining the documents, emails and texts that relate to the decisions and actions being taken during this pandemic.

Health Care Consultation Apps

Since the government has said stay home and self-isolate or quarantine, the question of how might I consult a health professional has arisen. The need for health professionals to be in contact with their patients continues during the pandemic and when the government created a temporary fee for telehealth consultations, the desire and need to create ways of consulting over the telephone, computer or device accelerated.

Media coverage has been given to apps that will facilitate health professional's consultations with their patients. As health professionals and patients are approached to use such apps, they should be asking questions before agreeing to do so.

Health professionals and patients should ask:

- Does the organization offering the app (service provider) reside in Saskatchewan?
- What personal health information is collected and stored by the app (service provider) and for how long?
- Where geographically is the information stored?
- Who is in custody and control of the stored information?
- Can I get a copy of the stored information any time I ask?
- Is there a fee for getting a copy?
- Is the personal health information shared with any other company or individual?
- What safeguards are in place to protect that information?
- Can I see the contract I would have to sign to use the service?
- Have you done a privacy impact assessment and could I have a copy?
- Have you had a security assessment done by an independent third party and if so, can I see a copy?
- What health professional association has reviewed or endorsed this app?

The pandemic will continue to create privacy issues. I expect there will be many apps vying for loyalty of health professionals and patients. As always, it will be “buyer beware”. In other words, health professionals and patients, be careful for what you sign up for.

In the long run, if telehealth is here to stay, health professionals and their governing bodies should establish rules governing the engagement of apps that provide a telehealth service.

Health professionals should insist on a contract with the app service provider, read it carefully and not sign on the dotted line unless satisfied all aspects of HIPA are addressed.

Patients should read the privacy policy on apps (service provider’s) website.

This may turn out to be a very convenient service for health professionals and patients. Let us make sure the service has appropriate privacy and data protection.

Virtual Meetings

The pandemic has required many to work from home. Working at home requires workers to talk to one another and there is a need for meetings to occur. Zoom, over night, has become a way of holding a virtual meeting. There is other software such as Microsoft Teams, Skype and Google’s Hangout to facilitate virtual meetings.

To get work done, we need to meet. We also will gravitate to the most convenient way of meeting, but decision-makers and public bodies need to consider privacy and security issues.

We have seen some headlines about hackers hacking into a Zoom meeting. Therefore, the first thing we need to consider, is our meeting restricted to just those authorized to be there? Organizers need to set things up to ensure the correct settings are in place to prevent intrusion by the unauthorized.

Zoom asks whether you want the session saved. Another decision, will the organizers have the meeting saved? If so, it is a record and at that point, FOIP, LA FOIP, HIPA and *The Archives and Public Records Management Act* come into play. If minutes of a similar meeting are normally kept, then I would suggest the minutes of the virtual meeting need to be kept. If meetings were previously recorded, then organizers need to decide whether the virtual meeting will be recorded. If an ordinary meeting or virtual meeting is recorded, that recording becomes a record. Organizers from public bodies need to decide whether the recording is an official record or a transitory record under *The Archives and Public Records Management Act*. If it is an official record, organizers need to arrange for storage and preservation in its electronic filing system. If it is a transitory record, decisions have to be made as to when it is destroyed. If any access request under FOIP, LA FOIP or HIPA is received and the recording of the virtual meeting exists at that time, the record may have to be disclosed under FOIP, LA FOIP or HIPA (subject to appropriate exemptions).

If you are recording the virtual meeting, the question is who is recording it? If it is the service provider, then is it being stored on the service provider's server? Is that where you want it stored? How do you get that recorded meeting downloaded to your organization's file records system? Does the provider routinely save/store copies of meeting recordings? Can you ensure that it is deleted off the service provider's system?

If your meeting has discussion of issues, which involve personal information or personal health information, what additional precautions can you take to ensure that information is not being accessed by unauthorized persons?

As a practice, a public body might indicate you do not want the meeting recorded. Can an organization be sure the service provider is not saving a copy anyway? This is why it is also important to understand the risks of working with any particular service provider in advance of using that system. If you do not have the appropriate agreements in place or at least an intimate understanding of the risks and benefits, your meeting sessions could be hijacked, information kept and used for purposes that you did not anticipate, and privacy breaches could occur for which the public body would be responsible.

Organizers need to think carefully about the platform they select for virtual meetings. They will want the one that best protects their confidential information and the one that allows them to comply with FOIP, LA FOIP and HIPA. To assist organizers, here are some questions they should ask before selecting a platform:

- Does the service provider offering the platform reside in Canada or the United States?
- Where geographically is the virtual meeting stored? Where is the server located (Canada or the United States)?
- Are virtual meetings going to be recorded and saved and if so, by whom?
- Will your meeting involve possible confidential information? If so, do you want it recorded?
- Who has possession/custody or control of the information?
- If saved, can the public body download the recording into its file management system?
- How long will the service provider retain the recording?
- Can the public body request deletion of the recording at any time?
- Does the service provider share the recording or other information with anyone else? If so, who and under what authority?
- Does the service provider have end to end encryption?
- Does the service provider have a privacy policy and a security policy?

- What settings can the public body set to maximize privacy and security?
- Does the public body consider the recording an official record or a transitory record?
- Has a service provider had a privacy or security assessment done by an independent third party and, if so, request a copy?

The pandemic has forced many public bodies to embrace the virtual meeting. Once restrictions are lifted, I expect virtual meetings will continue to be a way of doing business. Public bodies should approach virtual meetings and platforms as both a short term matter and a long term change. Thus, establishing public body policies regarding virtual meetings is an important step that we should take now.

Working from home

As we try to ‘flatten the curve’ of the COVID-19 outbreak, many are working from home. Below are some security tips for those who are working from home:

1. Follow the policies and guidelines set by your IT department.
2. If a Virtual Private Network (VPN) has been set up by your organization, use it.
3. For your home network, do the following:
 - a. Make sure the password to your router/network is a strong, complex password
 - Use letters, numbers, and symbols for your password. If you are unsure about how strong your password is, use this tool to measure the strength of your password: <https://www.my1login.com/resources/password-strength-test/>
 - b. Ensure your administrator password isn’t the default router password. If it is, change it.
 - c. The router setting should be set to WPA2-AES. This enables network encryption. Do not use WEP.
 - d. Only allow those within your household to connect to your router/network.
 - If you have ever given guests the password to your network, change the password.
 - e. Know which computers/devices are connected to your network.
 - If any of the computers or devices become infected with a virus, disconnect that computer/device from the network. Use anti-virus protection and check all other devices to see if they were infected by the virus. Remove computers and devices as needed and report the matter to your supervisor and/or IT department.
 - f. Tell others in your household the following:
 - Only access websites and download material from trusted sources. If they are not sure, then don’t.
 - If they suspect that they may have downloaded a virus, they are to report this to you immediately so you can contain the virus to try to ensure other computers/devices are not infected and report to your supervisor and/or IT department.
4. Establish administrative, physical, and technical safeguards. Below is a non-exhaustive list. Examples of safeguards are:

Administrative safeguards:

- Follow the policies, procedures, and guidelines established by your organization for working from home.
- Communicate to others within your household they are not to access your computer, devices, documents, etc.

Physical safeguards:

- Do not leave laptops, desktop computers on and unattended. Also do not leave documents or anything else containing sensitive information unattended.
- Securely store away laptops, documents, portable devices not in use.
- Take precautions so that no one else can see the contents of your screen, especially if it contains sensitive information such as personal information and personal health information.
- Do not allow others to use your work computer/laptop/device.

Technical safeguards:

- Use strong passwords.
- Lock computer screen when leaving the computer unattended.
- Log off or shut down computers when not in use.

Transporting PI and PHI Outside of the Office

With a pandemic impacting the world and governments asking people to social distance ourselves, many people are having to work from home and having to bring home personal information (PI) and personal health information (PHI) to do their jobs. You also hear stories of people losing their briefcases, laptops, devices, or even their vehicle being stolen with PI and PHI in them. Yes, these things do happen, but there are ways that you can mitigate the risk from this happening. Wherever you take PI and PHI, all public bodies have a duty to protect it.

Our resource, [Best Practices for Transporting Personal Information \(PI\) and Personal Health Information \(PHI\) Outside of the Office](#), provides you with some best practices to use when transporting information from your office to your home, or to any other place.

Phishing Attacks

A combination of workers getting used to working-from-home and the anxiety and fears arising from the outbreak of COVID-19 may be leaving workers and organizations vulnerable to cyber attacks. For example, malicious actors may set up email accounts to impersonate supervisors and coworkers and trick workers into providing information about themselves or the organization.

Such emails are called “phishing attacks” and the purpose of such attacks is to obtain information that malicious attackers may use to gain access to systems. Organizations who have permitted employees to use personal email accounts are especially vulnerable to such an attack since workers will have a tougher time discerning legitimate email accounts from those of attackers’ email accounts.

The [Canadian Centre for Cyber Security](#) has provided the following guidelines to protect yourself:

Against Malicious Emails:

- Make sure the address or attachment is relevant to the content of the email.

- Make sure you know the sender of an email.
- Look for typos.
- Use anti-virus or anti-malware software on computers.

Against Malicious Attachments:

- Make sure that the sender's email address has a valid username and domain name.
- Be extra cautious if the email tone is urgent.
- If you were not expecting an attachment, verify with the sender.

Against Malicious Websites:

- Make sure URLs are spelled correctly.
- Directly type the URL in the search bar instead of clicking a provided link.
- If you must click on a hyperlink, hover your mouse over the link to check if it directs to the right website.

For more information, check out the website for the Canadian Centre for Cyber Security.

Research: Post Pandemic

Post pandemic there will be many opportunities and much interest in researching many and varied aspects of this world pandemic. I expect there will also be interest on the part of Saskatchewan researchers. Maybe some have started, but I expect as soon as things return to normal, researchers will ramp up research projects and be wanting personal information and personal health information.

The law is VERY CLEAR that researchers can ask public bodies for de-identified or aggregated information. Each public body has to decide how much information it will provide; that is a policy decision. Those public bodies under privacy legislation are allowed to provide de-identified or aggregated information.

What is de-identified information? It is the information without your or my name, address, or any unique identifier such as the individual's Social Insurance Number (SIN) or Health Services Number (HSN). For example, subsection 3(2)(a) of HIPA states that it does not apply to statistical information or de-identified personal health information that cannot reasonably be expected, either by itself or when combined with other information available to the person who receives it, to enable the subject individuals to be identified. A public body can provide all the information that does not identify you or me.

If the health trustee or the researcher has the consent of the individuals to use their personal health information, then that is the best way to go. In many cases, that won't be possible. Either the health trustee did not obtain consent to research or there are thousands and thousands of records and getting consent would not be possible.

If research is being done in such a way that it requires information from two sources and the name, SIN or HSN are sought to connect the information of an individual, that presents a challenge. [The Data Matching Agreements Act](#) is not yet proclaimed. Nonetheless, FOIP, LA FOIP and HIPA have always authorized use and disclosure of personal information or personal health information for legitimate research purposes in the public interest. The best case scenario, and for research at the population level, de-identified data should be used and should suffice for those purposes. However, those same laws provide for the use of identifiable data when appropriate, but I

must emphasize the need for written agreements to ensure that data is protected. This rigour is necessary to ensure that if data is used from one or multiple sources that what is provided is used as intended and protected throughout the process.

I note section 29 of HIPA requires all research projects where personal health information is used or disclosed by a trustee, must be approved by a research ethics committee that has been approved by the Saskatchewan Minister of Health. If a research ethics committee is small and nimble it should never be a barrier to good research.

I have heard that some say “privacy” is a barrier to research. I do not believe or accept that point of view. That is why I write this item to show that good research can continue and the barriers to obtaining the data should be minimal. If public bodies are citing “privacy” as the problem, they are giving the wrong reason and it just might be they don’t want to provide the information or to cooperate. Privacy is not the barrier.

Travel Restrictions and Checkpoints

On April 24, 2020, the Chief Medical Health Officer issued an [Order](#) restricting travel into and out of the Northern Saskatchewan Administration District (NSAD) to essential travel. On April 30, 2020, the Order was amended to restrict travel between communities in NSAD. The Order provides:

1. I hereby ORDER and DIRECT effective immediately:

- a. Subject to subsection (c), no person shall travel to or out of the Northwest Region, whether from within the Province of Saskatchewan or otherwise.
- b. Subject to subsection (c), no person within the Northwest Region shall travel outside the community in which their primary residence is located.
- c. Travel is permitted as follows:
 - i. Persons may return to their primary residence;
 - ii. Employees of, and persons delivering, critical public services and allowable business services, a listing of which is found on the Government of Saskatchewan website: Saskatchewan.ca;
 - iii. Aboriginal persons engaging in activities such as exercising their constitutionally protected right to hunt, fish and trap for food or engaged in other traditional uses of lands such as gathering plants for food and medicinal purposes or carrying out ceremonial and spiritual observances and practices;
 - iv. Persons who are travelling for medical treatment;
 - v. Persons travelling for the purposes of attending court where legally required to do so; and
 - vi. Persons whose primary residence is within the Northwest Region may travel to the community closest to their community of primary residence within the Northwest Region taking the most direct route to obtain essential goods and services, when those goods or services are not available in their community of primary residence, a maximum of twice per week. Each household shall only utilize one vehicle and each vehicle must only contain household members.
 - vii. When persons are traveling outside the Northwest Region for medical treatment they may also stop to obtain essential goods and services outside of the Northwest Region. Only one person in the vehicle may enter a retail establishment outside of the Northwest Region to purchase such essential goods and services.

On June 7, 2020, the Chief Medical Health Officer issued a new Order which did not contain the travel restrictions as quoted above. To my knowledge, this is the first time such travel restrictions were imposed in Saskatchewan. With the travel restrictions removed, the issues discussed below only become relevant if travel restrictions are imposed in the future (e.g. a second wave).

The Public Health Act, 1994, gives the Chief Medical Health Officer broad powers in emergencies and we all agree these are exceptional times.

Section 53 of *The Public Health Act, 1994* provides:

Inspection, investigation, inquiry, search

53(1) For the purposes of enforcing and administering this Act, the regulations or bylaws made pursuant to this Act, a public health officer may:

(a) subject to subsection (2), at any reasonable time and without prior notification, enter any premises or detain any vehicle;

(b) make any inspection, investigation or inquiry that the public health officer considers necessary;

...

(e) take one or more persons to any premises or vehicle to assist the public health officer and may make arrangements with the person in charge of the premises or vehicle for those persons to re-enter the premises or vehicle to perform specified functions;

...

(i) require any person whom the public health officer finds in or at any premises or vehicle to provide the public health officer with any information the person can respecting:

(i) the identity of the owner of the premises or vehicle; or

(ii) the source or cause of a health hazard, disease or injury

The Saskatchewan Public Safety Agency is a government institution and subject to FOIP. That also makes the agency a trustee under HIPA. Highway patrol officers and conservation officers would be employees of ministries, which are government institutions and trustees.

If checkpoints are merely providing information to travelers into or out of a community, then no privacy issues arise. Checkpoints can provide information about COVID-19 regarding how many in the community have been diagnosed, related risks and best practices to help prevent the spread of the virus. If checkpoints are collecting personal information or personal health information from travellers, privacy legislation is applicable.

FOIP, LA FOIP and HIPA allow for the collection of personal health information for specified purposes. The purpose here is restricting travel according to Order 1(c).

Government institutions are bound by FOIP, local authorities are bound by LA FOIP and trustees are bound by HIPA. Municipalities, villages and towns are local authorities.

The challenge will be to ensure the questions asked at checkpoints are limited to addressing the specific purpose set out by the Order. Questions such as:

- Are you coming from or returning to your primary residence? If so, what community are you coming from or returning to? Order 1(c)(i)

- Are you an employee of an organization providing critical public services or allowable business services? If so, what community are you coming from or returning to? Order 1(c)(ii)
- Are you an employee of an organization delivering, critical public services or allowable business services to this community? If so, what community are you coming from or returning to? Order 1(c)(ii)
- Are you an Aboriginal person exercising your constitutional protected rights? Order 1(c)(iii)
- Are you going to a medical appointment or coming from a medical appointment? If so, which community are you going to or coming from? Order 1(c)(iv)
- Are you a person traveling to this community from your community of primary residence to obtain essential goods and services not available in your community of primary residence (a maximum of two times per week)? If so what community are you coming from or returning to? Order 1(c)(iv)
- Are you traveling to attend court? If so what community are you coming from or returning to? Order 1(c)(v)

Other questions beyond these need to be analyzed as to whether they are necessary to restrict travel according to Order 1(c).

A further issue is that after the questions are asked, are the responses recorded? If so, by whom and for what purpose? If recorded, the record may be accessible under HIPA, FOIP or LA FOIP (subject to appropriate exceptions).

Once the questions are asked and answered, possibly recorded, does the information need to be shared with anyone? If so, who and for what purpose? Is there authority to share that information beyond the checkpoint?

There is a principle known as “need-to-know”. Who needs to know or must know for the specified purpose? If you don’t need to know, then the information should not be given to you.

Finally, if personal information or personal health information is recorded, the trustee, government institution or local authority should make a decision as to how long the information is kept. The purpose here is to restrict travel according to Order 1(c). Now that travel restrictions are removed, the purpose for checkpoints are gone. I would recommend government institutions, local authorities and trustees make a decision now as to how long the information will be kept and then destroyed.

The pandemic has created unusual circumstances in our province and actions must be taken quickly, but in that process privacy legislation still exists and needs to be respected and followed to protect privacy to the extent possible. I believe we can do both, but it takes decision-makers carefully thinking through the actions they take.

Contact Notification and Tracing Apps

Information and Privacy Commissioners from across Canada have developed and issued a [joint statement](#) regarding COVID-19 and contact tracing. The statement contains a series of principles that decision-makers should consider when deciding whether to launch a contact notification or tracing app. The principles are as follows:

Consent and trust: The use of apps must be voluntary. This will be indispensable to building public trust. Trust will also require that governments demonstrate a high level of transparency and accountability.

Legal authority: The proposed measures must have a clear legal basis and consent must be meaningful. Separate

consent must be provided for all specific public health purposes intended. Personal information should not be accessible or compellable by service providers or other organizations.

Necessity and Proportionality: Measures must be necessary and proportionate and, therefore, be science-based, necessary for a specific purpose, tailored to that purpose and likely to be effective. To assist in determining whether the measure in question is justifiable in the circumstances, governments should consider the following:

- **Necessity:** the public health purpose or purposes underlying a measure must be evidence-based and defined with some specificity. Is the purpose to notify users and advise them to take certain actions? Is it to assist public health authorities to better understand local conditions for resource allocation purposes? Is it for another purpose?
- **Proportionality:** the measure should be carefully tailored in a way that is rationally connected to the specific purpose(s) to be achieved,
- **Effectiveness:** the measure must be likely to be effective at achieving the defined purpose(s), and,
- **Minimal intrusiveness:** while the least intrusive option for the intended purpose should be chosen, and data minimization should be applied, where that cannot be achieved or demonstrated, governments should clearly communicate the rationale for the level of personal information that they need to collect.

Purpose Limitation: Personal information must be used for its intended public health purpose, and for no other purpose.

De-identification: De-identified or aggregate data should be used whenever possible, unless it will not achieve the defined purpose. Consideration should be given to the risk of re-identification, which can be heightened in the case of location data.

Time-Limitation: Exceptional measures should be time-limited: any personal information collected during this period should be destroyed when the crisis ends, and the application decommissioned.

Transparency: Government should be clear about the basis and the terms applicable to exceptional measures. Canadians should be fully informed about the information to be collected, how it will be used, who will have access to it, where it will be stored, how it will be securely retained and when it will be destroyed. Privacy Impact Assessments (PIAs) or meaningful privacy analysis should be completed, reviewed by Privacy Commissioners, and a plain-language summary published proactively.

Accountability: Governments should develop and make public an ongoing monitoring and evaluation plan concerning the effectiveness of these initiatives and commit to publicly posting the evaluation report within a specific timeline. Oversight by an independent third party – such as review and implementation monitoring by a privacy commissioner’s office – will help ensure accountability and reinforce public trust. While some privacy commissioners have the legal authority to conduct independent audits, it is encouraged that others be given this mandate by government through appropriate means. If effectiveness of the application cannot be demonstrated, it should be decommissioned and any personal information collected should be destroyed.

Safeguards: Appropriate legal and technical security safeguards, including strong contractual measures with developers, must be put in place to ensure that any non authorized parties do not access data and not to be used for any purpose other than its intended public health purpose. Authorities must ensure the public are aware of associated risks and threats (e.g. online fraud or malware).

I hope this statement of principles will help decision-makers work through the complex issues of deciding to use contact notification or application apps or not and balancing protection of public health and privacy.

Questions, Screening or Testing by Employers Regarding COVID-19

Our province is gradually phasing in our economy. Businesses, organizations and government offices are gradually opening up. Employers are contemplating the return of their employees to the workplace. Employers and employees will have questions. This section attempts to answer a number of those questions.

Can an employer test for COVID-19?

Some employers may be considering whether they will require all employees to answer questions, be screened or be tested for COVID-19. Employers have an obligation to make a workplace safe to work in within reasonable limits. *The Saskatchewan Employment Act* provides:

General duties of employer

3-8 Every employer shall:

(a) ensure, insofar as is reasonably practicable, the health, safety and welfare at work of all of the employer's workers;

...

(h) ensure, insofar as is reasonably practicable, that the activities of the employer's workers at a place of employment do not negatively affect the health, safety or welfare at work of the employer, other workers or any self-employed person at the place of employment; and

Each employer will have to make a fundamental decision as to whether requiring all employees to answer questions, be screened or be tested would make the workplace safer.

Prior to considering what privacy legislation might apply, employers need to seriously consider whether they want to require employees to answer questions, be screened or be tested for COVID-19. This is a fundamental issue and can be controversial. It gets us into the issue of whether employers can or should require medical tests in the workplace. There has been considerable debate and court challenges over testing for drugs in the workplace. Employers need to know that requiring employees to answer questions, be screened or be tested for COVID-19 might result in a court challenge.

The Privacy Commissioner of Canada in *A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century* stated:

Following the enactment of the *Canadian Charter of Rights and Freedoms* in 1982, the Supreme Court of Canada formulated a methodological test to determine whether the violation of a *Charter* right is nonetheless justifiable in a free and democratic society. Stemming from the case *R. v. Oakes*, this became known widely as the Oakes test. It requires:

- **Necessity:** there must be a clearly defined necessity for the use of the measure, in relation to a pressing societal concern (in other words, some substantial, imminent problem that the security measure seeks to treat),
- **Proportionality:** that the measure (or specific execution of an invasive power) be carefully targeted and suitably tailored, so as to be viewed as reasonably proportionate to the privacy (or any other rights) of the individual being curtailed,
- **Effectiveness:** that the measure be shown to be empirically effective at treating the issue, and so clearly connected to solving the problem, and finally,

- **Minimal intrusiveness:** that the measure be the least invasive alternative available (in other words, ensure that all other less intrusive avenues of investigation have been exhausted).

The balance of this section presumes an employer has made the decision and understands the legal risks of a challenge, but intends to proceed.

What privacy legislation might apply?

If an employer decides to ask questions, screen or test its employees for COVID-19, that employer needs to know what privacy legislation applies to that employer. FOIP applies to government institutions which include Crown corporations, boards, agencies and other prescribed organizations. Part IV of FOIP deals with the collection, use, disclosure, storage and protection of personal information.

LA FOIP applies to local authorities which include cities, towns, villages, municipalities, universities and the Saskatchewan Health Authority. Part IV of LA FOIP deals with the collection, use, disclosure, storage and protection of personal information.

HIPA applies to health trustees which includes government institutions, the Saskatchewan Health Authority, a licenced personal care home, a health professional licenced under an Act, a pharmacy, and licenced medical laboratories. Parts III and IV of HIPA deal with collection, use, disclosure, storage and protection of personal health information.

If an employer falls into one of the above categories, then that particular statute will apply to the collection, use, disclosure, storage and protection of information. To be sure, an employer should check each of the Acts to see if it has any application. Regulations under each of the Acts can also prescribe government institutions, local authorities or health trustees.

A further issue is that after the questions are asked, are the responses recorded? If so, by whom and for what purpose? If recorded, the record may be accessible under HIPA, FOIP or LA FOIP.

If an employer continues to be in doubt, you may want to obtain legal advice. If an employer does not fall under any of the three Acts, it is possible you, as an organization, may be bound by the *Personal Information Protection and Electronics Documents Act (PIPEDA)*. For information on this, an employer can check the website of the [Federal Privacy Commissioner](#). In some cases, PIPEDA provides rules and protection for employee personal information and in others, it does not. Whether an employer in Saskatchewan fits any of the above definitions, the advice below can be considered best practice and an employer can choose to follow it.

What is the purpose of doing the tests for COVID-19?

Before embarking on questioning or a testing program, an employer needs to define the purpose for collecting the Q&A and test information. Is it to keep the workplace safe? More specifically is it to prevent workers who test positive or have had COVID-19 from being in the workplace? Is it to prevent the spread of COVID-19 to other workers in the workplace? It is important that the employer define the purpose at this early stage and not expand after the fact as would be function creep and may not be authorized.

How should employers notify its employees of the purpose of collection?

Employers should be open and transparent. They should advise staff that they will be asking questions, screening or testing employees as they arrive for work and inform them of the purpose. Later at the time of collection, tell

employees the purpose of collection, what will be collected, who it will be shared with and how long the information will be stored. Employees will particularly want to know if the employer is sharing the information with other third parties and why. As discussed below, the employer should advise employees that positive tests for COVID-19 will be shared with the medical health officer.

If staff test positive or have COVID-19, the employer can provide other staff with statistical information, such as how many have been tested and how many tested positive. The employer should not give out names or identify the ones who tested positive as this may be considered a privacy breach. If very few employees test positive or have COVID-19, the employer needs to determine whether by giving the statistical information, the employee can be identified. If this might be the case, the employer can ask the consent of the employee affected, to release, postpone the release or provide less information that prevents identification.

What information will the employer collect?

Asking an employee a series of questions and obtaining the answers is collection of information. Screening by visual examination or temperature checks is collection of information. Requesting an employee to take a test and recording the results, is a collection of information. An employer needs to define the questions asked, the screening and the test required and ensure those questions, screening and test results are consistent with the purpose. Employers should collect the least amount of information necessary to achieve the purpose. This is referred to as the data minimization principle, that is, only collect what is needed to achieve the purpose.

For example, if an employee tests positive for COVID-19, what is an employer going to do? The assumption is an employer will require the employee to stay home and self-isolate. Thus, once an employer knows the person tested positive, there is no need to know anything more other than if the medical health officer's follow up efforts will impact the employer. You are the employer, not the doctor. If the staff member indicates they already have COVID-19, an employer will need to consult the organization's doctor to determine whether the staff member should be allowed to come to work or is required to stay home. Again, an employer should not collect more information, only tell the employee that they can or cannot work and they should go home. If the test comes back "negative" an employer still is obliged to comply with any requirements of the Chief Medical Health Officer in terms of taking protective procedures in the workplace.

The Information Commissioner (ICO) of Great Britain has stated:

In order to not collect too much data, you must ensure that it is:

adequate – enough to properly fulfil your stated purpose;

relevant – has a rational link to that purpose; and

limited to what is necessary – you do not hold more than you need for that purpose.

Can the employer use the information for any other purpose?

The employer has defined a purpose, authority to collect and has collected information for that purpose. The employee has provided the information for that purpose. The employer cannot use that information for any other purpose without getting the consent of the employee.

If an employee tests positive, who can the employer share the information with?

Since the employer has collected the information that the employee tested positive or has had COVID-19, the employer needs to determine who in the organization needs to know. If the employee is going home, very few

people need to know. Just like other sensitive health information, it is confidential, the employer should prohibit the employee from sharing the information with other staff.

Where does an employer store this information?

The choices are storing on the employees HR personnel file or storing in a separate folder for all employees, containing all information regarding questions, screening and testing. There is probably no need to store it anywhere else.

The information the employer has collected, must be stored in a secure place. Once the employer collects personal information about an employee, it is the employer's obligation to ensure it is protected.

Is an employer obliged to secure the information?

Under privacy legislation, there is an obligation for an employer to protect and secure the information collected and stored. If an employer is not subject to the privacy legislation, best practice would suggest the information be protected anyway. Other resources have made suggestions on securing information and a few tips are given by the [British Columbia Information and Privacy Commissioner](#):

Your organization must make reasonable security arrangements to protect personal information in its custody or under its control. For example, if the collected information is in paper form, it should not be left in a publicly accessible area. Rather, it should be stored in a locked file cabinet. If you are storing the list on a computer, make sure the computer is password protected, encrypted, and on a secure network. Position computer monitors so that personal information displayed on them cannot be seen by visitors.

When should the employer destroy the information?

How long is an employer going to keep this information? Will it get destroyed in accordance with the destruction of documents policy? Should it have a special destruction period, shorter than the normal? Could it or should it be destroyed within 30 days? Employers need to decide whether they will develop a policy including destruction guidelines. There has been media coverage about people's fear of having COVID-19 and the stigma that comes along with that. Maybe a year from now, there will be an approved treatment and vaccination, which might reduce the stigma and the fear. Maybe the information collected can be destroyed earlier than an employer's standard procedure.

Should employers share information with the medical health officer?

The Public Health Act, 1994 provides:

Responsibility to report

32(1) The following persons shall report to a medical health officer any cases of category I communicable diseases in the circumstances set out in this section:

- (a) a physician or nurse who, while providing professional services to a person, forms the opinion that the person is infected with or is a carrier of a category I communicable disease;
- (b) the manager of a medical laboratory if the existence of a category I communicable disease is found or confirmed by examination of specimens submitted to the medical laboratory;
- (c) a teacher or principal of a school who becomes aware that a pupil is infected with or is a carrier of a category I communicable disease;

(d) a person who operates or manages an establishment in which food is prepared or packaged for the purposes of sale, or is sold or offered for sale, for human consumption and who determines or suspects that a person in the establishment is infected with, or is a carrier of, a category I communicable disease.

...

(3) A report submitted pursuant to subsection (1) must include:

- (a) the name, sex, age, address and telephone number of the person who has or is suspected to have, or who is or is suspected to be a carrier of, a category I communicable disease; and
- (b) any prescribed information.

(4) In addition to the report required by subsection (1), the manager of a medical laboratory shall submit to the medical health officer or the co-ordinator of communicable disease control a copy of the laboratory report that identifies the disease.

The Disease Control Regulations lists COVID-19 as a category 1 communicable disease.

If an employer intends to ask a series of questions or do screening by a non-health professional section 32 above would not apply. In that case, if the questions result in their being indications of COVID-19, I would expect the employer would request that the employee be tested for COVID-19 at a nearby testing centre and the employee be advised to go home until testing is done and results are received.

If an employer has an examination done for a test taken by a doctor or nurse, it is clear that, pursuant to section 32, the doctor, nurse or manager of a medical lab must report a communicable disease such as COVID-19 to the medical health officer.

Thus, best practice would be for an employer to advise employees being examined or tested that if the test is positive for COVID-19, it will be reported to the medical health officer. The employer should indicate in their statement of purpose that they will comply with the requirements of *The Public Health Act, 1994*. Being transparent with staff and telling them at the beginning that their information will be shared with public health authorities is important.

Do employers need to document their questions and testing plan?

Once an employer has made a decision, the employer should consider some documentation of the plan. In normal times, my office would recommend a privacy impact assessment (PIA). In these unique times, an employer might move very quickly and my office would still recommend either a shortened version of a PIA or a policy statement regarding question asking, screening and testing plan. Whatever the form of the document, it should contain:

- a statement of the purpose;
- a listing of the questions to be asked;
- a statement of the screening and the tests to be performed;
- a statement on possible actions taken based on the test results;
- a statement where information will be stored;
- a statement as to who it will be shared with (with public authorities or not); and
- a statement when the information will be destroyed.

Conclusion

The principles are simple, establish the purpose, authority, and collect the least amount of information to meet the purpose, share it only with those who need-to-know, store it, keep it secure and destroy it when no longer needed. This is good advice whether an employer is subject to access and privacy legislation or not.

Health Screening of Staff and Visitors in Care Homes

We have all heard the news telling us about the number of deaths of seniors in care homes related to COVID-19. Ontario and Quebec have particularly been impacted, but so has Saskatchewan. The Chief Medical Health Officer has ordered health screening to occur in care homes. The [Public Health Order](#), dated June 13, 2020, provides as follows:

1. I hereby ORDER and DIRECT that in the Province of Saskatchewan effective June 13th, 2020:

...

- (c) Visitors to long-term care homes, hospitals, personal care homes, and group homes shall be restricted to family or designates visiting for compassionate reasons. All visitors shall undergo additional health screening prior to entry. Any visitors who display or disclose signs or symptoms of COVID-19 shall be denied entry to the facility.

2. I hereby ORDER and DIRECT that in the Province of Saskatchewan:

- (a) For the purposes of section 2 of this Order, "Licensee" refers to:
 - (i) operator of a special-care home designated pursuant to The Provincial Health Authority Act;
 - (ii) the licensee of a personal care home licensed pursuant to The Personal Care Homes Act;
 - (iii) an individual who, or corporation that, under a contract or subcontract with an operator of a special care-home or a licensee of a personal care home, provides or arranges for the provision of health care services or support services within the facility.
- (b) For the purposes of section 2 of this Order, "Facility" refers to:
 - (i) A special-care home designated pursuant to The Provincial Health Authority Act;
 - (ii) A personal care home licensed pursuant to The Personal Care Homes Act.

3. I hereby ORDER and DIRECT that in the Province of Saskatchewan:

- (a) For the purposes of section 3 of this Order, "Facility" means the same as defined in section 2 above but is amended to include:
 - (i) All facilities designated pursuant to The Provincial Health Authority Act operated by the Provincial Health Authority as defined in The Provincial Health Authority Act;
 - (ii) Hospital as designated pursuant to The Provincial Health Authority Act operated by an affiliate prescribed in The Provincial Health Authority Administration Regulations;
 - (iii) The following facilities operated by the Saskatchewan Cancer Agency continued pursuant to The Cancer Agency Act:
 - i. Saskatoon Cancer Centre;
 - ii. Allan Blair Cancer Centre; and
 - iii. The Hematology Clinic.
- (b) For the purposes of section 3 of this Order, "Licensee" means the same as defined in section 2 above but is amended to include:

- (i) The Provincial Health Authority as defined in The Provincial Health Authority Act;
 - (ii) The Saskatchewan Cancer Agency continued pursuant to The Cancer Agency Act.
- (c) For the purposes of Section 3 of this Order, “Staff Member” refers to:
- (i) any individual who is employed by, or provides services under a contract with, the Licensee of a Facility; and
 - (ii) any volunteer or student that assists in the provision of services within the Facility.
- (d) For the purposes of Section 3 of this Order, “Individual” means the same as Staff Member but also includes all individuals entering the Facility, except individuals entering for the purposes of receiving care.
- (e) Health screening shall occur as follows:
- (i) Staff Members shall undergo health screening prior to or upon entry to the Facility, which must include a temperature check. Any Staff Members who display or disclose signs or symptoms of COVID-19 shall be denied entry to the Facility. All Staff Members shall undergo a temperature check prior to leaving the Facility. All exceedance temperatures shall be logged by the Licensee.
 - (ii) Individuals who are not Staff Members shall undergo health screening, which must include a temperature check prior to or upon entry to the Facility. Any of these Individuals who display or disclose signs or symptoms of COVID-19 shall be denied entry to the Facility. All exceedance temperatures shall be logged by the Licensee.

...

The Minister of Health or the Chief Medical Health Officer have powers under [The Public Health Act, 1994 \(P.37.1\)](#). In particular, section 45 sets out the broad powers of the Minister and the Chief Medical Health Officer. Further, the Act contains mandatory reporting provisions of certain health care professionals in certain circumstances (e.g. section 32).

This advisory attempts to answer a number of questions related to collection, use, storage, safeguarding and destruction of personal health information involved in carrying out this order.

What privacy legislation might apply?

The Health Information Protection Act (HIPA) applies to health trustees which includes government institutions, the Saskatchewan Health Authority, health care organizations, a licensed personal care home, a health professional licensed under an Act, a pharmacy, and licensed medical laboratories. PARTS III and IV of HIPA deal with collection, use, disclosure, storage, and protection of personal health information.

To be sure, a care home should check HIPA to see if it has any application to it and if necessary, seek legal advice.

What information can be collected of personal health information?

The public health order requires health screening including temperature checks of staff and visitors be taken and exceedance temperatures be logged. For staff and visitors, recording of a name, an exceedance temperature and answers to questions regarding COVID-19 symptoms is a collection. For visitors, due to the potential need to follow up, it would appear reasonable to ask which resident they were there to visit. It would not be reasonable to ask for the visitor’s Health Services Number (HSN) or other unrelated health information. To ask other unrelated questions and record answers, is going beyond the provisions of the public health order.

In collecting personal health information, the principle is to collect and record the least amount of personal health information necessary to carry out the purpose. The purpose here would be to comply with the public health order, which in turn is intended to keep care home staff and residents safe.

How should care homes notify staff and visitors of the collection?

Care homes should be as open and transparent as possible. They should advise staff that they will be doing temperature checks as they arrive for work and leave work. Care homes should advise visitors that health screening, including temperature checks, will be conducted at their care home through posters at the front door, pamphlets and postings on their website. Care homes should protect the information they collect and let staff and visitors know that the personal health information they have provided will not be shared with other staff and residents at the care home. The care home should not give out names or identify the ones who have exceedance temperatures, as this may be considered a privacy breach.

Care homes should develop a policy on health screening, including temperature checks, share that policy with staff, residents and visitors and post on the care home's website.

To support the advice and principles above, the Information Commissioner (ICO) of Great Britain has stated:

In order to not collect too much data, you must ensure that it is:

adequate – enough to properly fulfil your stated purpose;

relevant – has a rational link to that purpose; and

limited to what is necessary – you do not hold more than you need for that purpose.

Can the care home use the information for any other purpose?

The care home is subject to the public health order, and has authority to collect personal health information for that purpose. The care home cannot use that information for any other purpose without getting the consent of the staff member or visitor whose information was collected.

If the staff member or visitor has an exceedance temperature, who can the care home share the information with?

Since the care home has collected the information that the staff member or visitor has an exceedance temperature, the care home needs to determine who in the organization needs to know. Once the staff member or visitor is refused entry, very few people need to know. If a staff member has an exceedance temperature, only the staff member's supervisor or director of the care home needs to know. The rest of the staff do not need to know. If a visitor has an exceedance temperature, that visitor should be asked whether the information can be shared with the resident that the visitor came to visit and the information should not be shared with other staff.

Where does a care home store this personal health information?

The public health order requires exceedance temperatures to be logged. The log could be a separate sheet of paper for each person with an exceedance temperature, a log book where all the persons with an exceedance temperature are recorded or an electronic spreadsheet (such as excel) where all persons with an exceedance temperature are recorded. For visitors, there is no need to store the information anywhere else. For staff, a decision needs to be made whether a notation is made in the staff member's HR file. Best practice would suggest that the care home only record on the HR file that the staff member is away on sick leave or another type of leave. There is no need to store it anywhere else.

Is a care home obliged to secure the information?

Under HIPA, section 16, there is an obligation for a care home to protect the personal health information collected and stored.

Once the care home collects personal health information about a staff member, it is the care home's obligation to ensure it is protected. For example, leaving the log book at the front entrance would not be securing or protecting the personal health information and should not be accessible to all staff. Similarly, having a computer monitor at the front entrance, making the log accessible to all that pass by would be unacceptable.

Other resources detail suggestions on securing information and a few tips are given by the British Columbia Information and Privacy Commissioner:

Your organization must make reasonable security arrangements to protect personal information in its custody or under its control. For example, if the collected information is in paper form, it should not be left in a publicly accessible area. Rather, it should be stored in a locked file cabinet. If you are storing the list on a computer, make sure the computer is password protected, encrypted, and on a secure network. Position computer monitors so that personal information displayed on them cannot be seen by visitors.

When should the care home destroy the personal health information?

How long is a care home going to keep this information? Will it get destroyed in accordance with the destruction of documents policy of the care home? Should it have a special destruction period, shorter than the normal? Could it or should it be destroyed after 30 days after the public health order is rescinded or should it just be destroyed after 30 days? The care home should develop a policy including destruction guidelines.

Should care homes share the exceedance temperature information with the Medical Health Officer?

The Public Health Act, 1994 provides:

Responsibility to report

32(1) The following persons shall report to a medical health officer any cases of category I communicable diseases in the circumstances set out in this section:

(a) a physician or nurse who, while providing professional services to a person, forms the opinion that the person is infected with or is a carrier of a category I communicable disease;

...

(3) A report submitted pursuant to subsection (1) must include:

(a) the name, sex, age, address and telephone number of the person who has or is suspected to have, or who is or is suspected to be a carrier of, a category I communicable disease; and

(b) any prescribed information.

...

The Disease Control Regulations lists COVID-19 as a category 1 communicable disease.

If a doctor or nurse performing the health screening concludes that an individual may have COVID-19, the doctor or nurse will have to determine whether section 32 of [The Public Health Act, 1994](#) applies. If the health screening is done by someone other than a doctor or nurse, section 32 would not apply. Since the exceedance temperature and answers to questions on COVID-19 symptoms may be an indication of COVID-19, best practice would suggest the care home request that the staff member or visitor call the healthline 811 or go to a testing centre.

Do care homes need to document their questions and testing plan?

Best practice would suggest that a care home develop a policy regarding its practices and procedures on temperature checking and make that policy available to staff, residents, and visitors. The policy should contain:

- a statement of the purpose;
- a statement that health screening will include, a temperature check and specific questions related to other symptoms of COVID-19;
- a statement on possible actions taken based on the results of health screening;
- a statement on how and where information will be stored;
- a statement as to who will have access;
- a statement that the information will be shared with only those that need-to-know and will not be shared with all staff and residents;
- a statement on how the personal health information will be protected;
- a statement as to who it will be shared with (public authorities or not); and
- a statement as to when the information will be destroyed.

A policy should be made available to staff, residents and visitors including postings on the care home's website.

Conclusion

The principles are simple; establish the purpose, authority, and collect the least amount of personal health information to meet the purpose. Share it only with those who need-to-know, store it, keep it secure and destroy it when no longer needed.

The Information Commissioner's Office in Great Britain has issued a document regarding "[Work Testing – Guidance for Employers](#)". Although British legislation is different from the legislation in Saskatchewan, the principles set out are good ones and may have some application to public bodies and health trustees in Saskatchewan.

Final Thought

In conclusion, maintaining a sense of balance during these difficult times can be done. It just takes a bit of thinking through the principles.

Resources

To assist organizations with decisions during a pandemic, please refer to the [office's website](#), and more particularly, the office's [Pandemic Binder](#).



Office of the
Saskatchewan Information
And Privacy Commissioner

503 – 1801 Hamilton Street
Regina SK S4P 4B4
306-787-8350

www.oipc.sk.ca