PANDEMIC BINDER:

Statements and Blogs by the Saskatchewan IPC
during the COVID-19 Pandemic

Office of the
Saskatchewan Information
and Privacy Commissioner

Table of Contents

Statements by the IPC

April 3, 2020 – Statement from the Office of the Information and Privacy Commissioner of Saskatchewan on Access to Information During a Pandemic

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

In Saskatchewan, *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) are still in force. Citizens of Saskatchewan still have the right to request information or records. The public bodies still are required to accept and process access requests. If staff are assigned to pandemic or other essential issues, I understand. On the other hand, public bodies have designated FOI staff who may be now working from home, and the processing of access requests can 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 to 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. 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.

When we thought this situation would take two weeks, suspension of service might have been reasonable. When isolation might occur for three months or longer, we need to have our information process systems operating, although maybe not quite as efficiently as before.

Finally, FOIP, LA FOIP and HIPA are still operative and requirements and timelines in legislation cannot be waived by me. My office can be flexible on timelines imposed by my office during review sand investigations. For example, providing a submission, providing the record or answering questions. If you need an extension, please make those requests directly to the individual in my office working on that file with you.

I ask all public bodies to work with my office to keep the access to information system working.

Ronald J. Kruzeniski
Information and Privacy Commissioner

April 20, 2020 – Updated Statement from the Office of the Information and Privacy Commissioner of Saskatchewan on COVID-19

Privacy in the Context of COVID-19

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

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

How Information May be Shared under Saskatchewan's Privacy Laws

Saskatchewan has three privacy laws:

- *The Freedom of Information and Protection of Privacy Act* (FOIP) applies to government institutions;
- *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) applies to local authorities such as municipalities, universities and school boards; and
- *The Health Information Protection Act* (HIPA) applies to health trustees.

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

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 or public bodies, 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 public body.

FOIP generally requires public bodies to collect personal information directly from the individual the information is about. Public bodies may collect 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.

Public bodies may disclose personal information in emergency situations with the consent of the individual, or without consent in certain circumstances, including:

- where necessary to protect the mental or physical health or safety of any individual; or
- the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure; or
- 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 also 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; or
- 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; or
- to another health trustee for the provision of health services; or
- 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: https://www.priv.gc.ca/en/. 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 News Release April17, 2020. 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* (P.37.1) which can be viewed here: https://publications.saskatchewan.ca/#/products/786. In particular, section 45 sets out the powers of the Minister and the Chief Medical Officer. Further, this Act contains mandatory reporting provisions of certain health care professionals in certain circumstances (e.g. sections 32, 34 and 36).

The Information and Privacy Commissioner

The Office will continue to work on matters during this time, but will be closed to the public. People seeking information can call 306-787-8350 or the toll free number 1- 877-748-2298 or email us at intake@oipc.sk.ca. There may be delays getting back to those who contact us, but we will get back to you.

My office usually requests that public bodies respond with information within certain timelines. We know other offices may be experiencing difficulties in getting back to us. Thus, we will be flexible regarding tight timelines. We do ask that you call us so that we can set a different timeline if one is required.

Ronald J. Kruzeniski, K.C.
Saskatchewan Information and Privacy Commissioner

April 21, 2020 – Statement from the Office of the Information and Privacy Commissioner of Documenting Decisions in a Pandemic

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. As we all can see, things are moving very quickly so decisions have to be made very quickly. Citizens and the media look forward and appreciate the daily briefings.

In this pandemic with decisions being required quickly, there continues to be a need to document those decisions. *The Freedom of Information and Protection of Privacy Act* (FOIP) and *The Local Authority Freedom of Information and Protection of Privacy Act* (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. I would ask public officials, elected and appointed, to ensure the decisions made and actions taken are documented.

During this time, more decisions may be made electronically. Emails and texts have been sent and 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. I ask public officials, elected and appointed, to 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' *Transitory Records Guidelines*, 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, I would ask public officials, elected and appointed, to 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.

Ronald J. Kruzeniski, K.C.
Saskatchewan Information and Privacy Commissioner

April 21, 2020 - Advisory from the Office of the Information and Privacy Commissioner of Saskatchewan on Apps that Offer Health Care Consultations

Since the government has said stay home and self-isolate or quarantine and the temporary closure of offices, including those of some health professionals, has been mandated 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 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 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 recommendations have your professional association made?

The prospective patient before signing up should ask:

- Does the organization offering the app (service provider) reside in Saskatchewan?
- What personal health information about me is collected and stored by the app and for how long?
- Where geographically is my information stored?
- Can I get a copy of my stored information any time I ask?
- Is there a fee for getting a copy of my personal health information?
- Is my personal health information shared with any other company or individual?

- What safeguards are in place to protect my personal health information?

The questions for the health professional and the patient are similar. Both need to know where personal health information is stored, who has access to it, how long is it stored and what steps are taken to protect personal health information.

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. However, in terms of health care providers, the ‘beware’ includes an expectation that you will do your homework and know whether or not by participating in the service you are or are not meeting your obligations under *The Health Information Protection Act*.

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.

Ronald J. Kruzeniski
Information and Privacy Commissioner

April 22, 2020 – Updated Statement from the Office of the Information and Privacy Commissioner on Transparency in a Pandemic

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

I have written earlier about a pandemic and privacy and 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 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 where diabetes or heart conditions 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 or the media. They may choose to conduct 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 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.

Ronald J. Kruzeniski
Information and Privacy Commissioner

April 24, 2020 – Advisory from the Office of the Information and Privacy Commissioner of Saskatchewan on Pandemic and Virtual Meetings

I read an article today saying over 7,000 Crown Corporation workers are working from home. In addition, thousands of executive government workers are doing the same. Many in businesses are also working from home. It is amazing how quickly this province was able to switch to an at home work environment.

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 video 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, *The Freedom of Information and Protection of Privacy Act* (FOIP), *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP), *The Health Information Protection Act* (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 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? If so, 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.

Ronald J. Kruzeniski
Information and Privacy Commissioner

May 4, 2020 - Statement from the Office of the Information and Privacy Commissioner of Saskatchewan on Contact Tracing and Privacy

I read an interesting article in *The Atlantic* by Derek Thompson. I was aware that South Korea and Singapore and other Asian countries were applying technology to the issue of contact tracing. What is contact tracing? As I understand it, when someone is diagnosed with having COVID-19, they are asked who they had been in contact with in the last while. Then those individuals are contacted. The old way was to do that by interviews. The existence of smartphones and apps allows contact tracing to take place by using Global Position System (GPS) and Bluetooth technology. For example, in South Korea, GPS is enabling authorities to know where patients have been using information from CCTV footage, credit card records and GPS data from the patient's smartphone. Singapore has taken a different approach by using a government developed app called "TraceTogether" that uses signals between mobile phones to record who you may have had close contact with.

Also, Asian countries are using technology to enforce quarantine. For example, Taiwan uses GPS to create an "electronic fence" for those who should be in quarantine. In Hong Kong, those who must quarantine themselves are given a wristband. They are to activate the wristband using a smartphone app.

Finally, technology is being used to enable movement in China as restrictions are being lifted.

European countries, including Germany and Italy, are also following Asia's lead and are developing and using apps to assist with combating the spread of COVID-19.

It would appear that Asia has been successful in reducing infections and deaths because of their approach to contact tracing along with other measures taken. We in North America are interested in when self-isolation could end and when our economy might get going again but are worried about a second wave. I can see that authorities here in North America will look to the digital methods used in Asia for ways to start the economy and reduce the risk of a second wave. As they consider these issues, alternatives will be presented and no doubt, smartphones will be raised as an option. In fact, Google recently announced on its blog that it is partnering with Apple to use Bluetooth technology to assist governments and health agencies conduct contact-tracing to help reduce the spread of COVID-19.

Technology can help us combat the spread of COVID-19 but it also increases the surveillance citizens are put under. The Electronic Frontier Foundation (EFF) asserts that surveillance invades privacy, deters free speech, and unfairly burdens vulnerable groups.

As North America adjusts its strategies to combat this pandemic, we must consider the impact such initiatives have on our privacy and our democracy. Can these technologies be used in a way that maximizes its potential in combatting the spread of the virus while minimizing the impact it has on our privacy? I am sure they can. I recommend that authorities be transparent in the technology they use. They should consider technology that doesn't collect and retain information unnecessarily. For example, it is being reported that Singapore's "TraceTogether" app uses Bluetooth technology so that information is stored only on the users' mobile phone for 21 days (the incubation period for COVID-19). If a person

tests positive, it is only then that authorities will access the information on the patient's phone so that authorities know who the patient has been in close contact with.

Another way for authorities to be transparent is letting the public know what information they are collecting, the purpose for the collection, and how the information will be used and/or disclosed. Individuals should have access to the information that is collected about them by authorities.

Furthermore, I recommend that authorities also consider how they can collect, use, and/or disclose the information that is necessary for the purpose of combating the spread of COVID-19 and to have processes in place to ensure such information is not used for other purposes, now or in the future. This includes setting a limit on how long information should be retained.

In Alberta, the provincial government has rolled out a contact-tracing app called "ABTraceTogether". It has completed a privacy impact assessment (PIA) and submitted the PIA to Alberta's Information and Privacy Commissioner. Once Alberta's Information and Privacy Commissioner reviews and accepts the PIA, the provincial government will make a summary of the PIA available. I recommend that if any similar initiative is undertaken in Saskatchewan, that a PIA be completed and submitted to my office.

The information and privacy commissioner has issued a news release. In that news release the information and privacy commissioner stated:

> *Ensuring this app is voluntary, collects minimal information, uses decentralized storage of de-identified Bluetooth contact logs, and allows individuals to control their use of the app are positive components.*

Alberta Health has issued a privacy statement that pertains to ABTraceTogether.

Whatever solutions are posed, my office is here to consult on the privacy implications in advance of any roll-out in Saskatchewan.

Ronald J. Kruzeniski
Information and Privacy Commissioner

May 7, 2020 News Release – Information and Privacy Commissioners from across Canada establish principles to be applied in consideration of contact notification and tracing apps

Information and Privacy Commissioners from across Canada have developed and issued a joint statement today 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 outlined under the following headings:

- Consent and trust
- Legal authority
- Necessity and Proportionality
- Purpose limitation
- De-identification
- Time-Limitation
- Transparency
- Accountability
- Safeguards

The Commissioner recognized that COVID-19 has created unique circumstances and there are serious public health risks but privacy legislation continues to be in force and must be factored in when making decisions regarding the utilization of new tools in controlling the spread. With a careful consideration of contact notification and tracing apps, it is possible to protect public health and personal privacy at the same time.

“I hope this statement of principle will help decision-makers work through the complex issues of balancing protection of public health and privacy”, Kruzeniski said.

The Commissioner also encourages any public body that is considering the adoption of such tools in Saskatchewan to consult with his office as soon as possible to help ensure that balance is met.

The full joint statement can be viewed here: https://oipc.sk.ca/assets/FPT-joint-statement-on-contact-tracing.pdf

May 27, 2020 – Advisory from the Office of the Information and Privacy Commissioner of Saskatchewan on 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 advisory 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 advisory 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. *The Freedom of Information and Protection of Privacy Act* (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.

The Local Authority Freedom of Information and Protection of Privacy Act (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.

The Health Information Protection Act (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.

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 whom 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.

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.

Ronald J. Kruzeniski
Information and Privacy Commissioner

June 9, 2020 – UPDATED Advisory from the Office of the Information and Privacy Commissioner of Saskatchewan on Pandemic, 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 on May 6, 2020, the Order was further amended and on May 20, 2020 the Order was amended to only apply to the northwest region. The May 20, 2020 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 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.

The Saskatchewan Public Safety Agency is a government institution and subject to *The Freedom of Information and Protection of Privacy Act* (FOIP). That also makes the agency a trustee under *The Health Information Protection Act* (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. If checkpoints are collecting personal information or personal health information from travelers, privacy legislation is applicable.

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

The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP) also allows for the collection of personal information by local authorities. Municipalities, villages and towns are local authorities. Local authorities can collect personal information for a specified purpose. The purpose here would be the restriction of travel into and out of a community according to Order 1(c).

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.

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.

Ronald J. Kruzeniski
Information and Privacy Commissioner

June 16, 2020 – Advisory from the Office of the Information and Privacy Commissioner of Saskatchewan on 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 exceedances 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 exceedances 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 heath 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 will 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.

Ronald J. Kruzeniski, Information and Privacy Commissioner

September 8, 2020 – UPDATED – Advisory from the Office of the Information and Privacy Commissioner of Saskatchewan to Teachers, School Boards, Parents and Students

The pandemic initially resulted in classes being suspended and students staying at home. Now that September is here, schools are reopening, but schools are also offering students the option to learn remotely from home. School Divisions and teachers have been planning during August, selecting the online learning platforms and preparing to use those platforms for those students and parents who select online learning. There are many platforms from which a school division can choose and I expect each school division may select a different platform. Each platform comes with its privacy settings and each school division will have to make decisions as to which settings are selected. In analyzing each platform a school division needs to, among other things, apply a privacy lens and ensure they are protecting the privacy of a student.

Zoom, and other video conference platforms, have received a lot of publicity. I expect every platform has over the last six months examined its privacy settings. School divisions and teachers need to think through the privacy risks for students in using video conferencing or virtual meeting platforms.

There are many educational offerings through the web that teachers will be tempted to use to help instruct and fill the day. Again, school divisions and individual teachers need to know the privacy protections afforded their students by *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP), which should cause school divisions to monitor closely what products are being used. This issue existed before the pandemic, but because of the current situation, the pressure to have online tools has increased. Teachers should only use the educational tools approved by their school divisions and should carefully review the privacy settings they can control, so as to reduce the risk of privacy breaches.

Before the pandemic, school divisions may have had a list of authorized or approved apps and educational products that the school division considered safe to use. I encourage school divisions to revisit the tools they have approved in the past to double check on privacy protections. Teachers should ensure that they are checking with the division with regard to any guidelines or restrictions on products they might want to use. Teachers need to consider which products are safe for use.

If school divisions have authorized virtual meeting/classroom platforms, they need to consider what information is collected and disclosed by use of the platform. For example, is the teacher seeing an image of the student and are all the students seeing images of the other students. As an individual's image is personal information, displaying the images of students to other students is a disclosure of personal information. School divisions need to determine whether that disclosure is authorized.

To determine whether a disclosure is authorized, a school division needs to review LA FOIP. If the authority is not clear in LA FOIP, the best thing to do is obtain a consent from each student or parent. School divisions may have already obtained a written consent at the beginning of the school year and school divisions should review that consent to determine whether it is a consent that covers the streaming or broadcasting of a student's image. Consent forms should be specific enough that parents or students know what they are consenting to.

I need to distinguish between the teachers seeing an image of each student in the class versus all students seeing the images of one another. The teacher seeing an image of a student is close to what the teacher would see if in a normal classroom. All students seeing the image of one another is a somewhat different issue because when this occurs, the images may be viewed by not only other students, but parents of the students, family members of the students, or caregivers of the students who are in the home. The streaming or broadcasting is potentially much broader than the teacher and other students in the class. Again, consent of a student or a parent can deal with this.

There are many questions for school divisions to consider in an online learning environment. What if a parent or student does not consent to the streaming or broadcasting of the student's image to other students? Has the school division made provisions for students/parents to not consent to the streaming or broadcasting of the student's image? Does the selected platform allow for students/parents opting out of streaming or broadcasting images? What if the student or parent turns off the camera on the home device? What if the student or parent puts masking tape over the lens of the camera? Should or does the school division encourage staff to advise students to turn off the camera and only turn on the microphone when a student is speaking?

The pandemic has given rise to many new privacy issues but, when one reflects, the principles that existed before the pandemic still apply. Does a school division have the authority to collect personal information? How will the school division/teacher use the personal information (student image)? Does the school division/teacher have authority to disclose (stream or broadcast) student personal information? Has the school division/teacher taken steps to safeguard the student's personal information? These were all relevant questions before the pandemic and the questions remain relevant today.

For parents that have chosen distant education or online learning for the time being, the pressure is there to search for and use educational apps. My office has no jurisdiction over what parents do, but I would encourage parents to do some research on educational tools and the impact on their child's privacy and ask questions if needed. One would not want your child's profile, pictures, art work, and essays to show up in unexpected places.

Finally, students, you have some responsibility in this area too. As you work with various educational tools, you can check in to see how well your privacy is protected. Where you have concerns, you should let your parent, your teacher, or your school division know.

I would recommend that school divisions, teachers and students check the privacy policies, terms of use, and privacy settings of every educational app that they are considering using.

If any staff member has questions, I would suggest the staff member call the designated access and privacy officer for the school division.

For an advisory that looks at similar issues from a different point of view, you can check out my advisory on virtual meetings.

If a school division is evaluating a particular platform, it should consider a privacy impact assessment (PIA). If there is no time to do this, the questions they would be asked during such an assessment should be asked by the director, superintendents, or the access and privacy officer. For details regarding a PIA, see Privacy Impact Assessment: A Guidance Document.

For information on back to school plans see Saskatchewan School Board Association and for detailed information of access and privacy check out Privacy and Access in Saskatchewan Schools.

Ronald J. Kruzeniski
Information and Privacy Commissioner

December 11, 2020 – Advisory from the Office of the Information and Privacy Commissioner of Saskatchewan on questions regarding vaccines for organizations, employers and health trustees

Announcements regarding the development of vaccines for COVID-19 has been greeted with excitement. There are still steps to go before the roll out of a vaccine, such as approval, delivery and administering the vaccine. As citizens receive the vaccine, questions arise as to how organizations, health trustees and employers will handle this new reality. In my *Advisory from the Office of the Information and Privacy Commissioner of Saskatchewan on questions, screening or testing by employers regarding COVID-19*, I attempted to answer many of the questions surrounding the issue of employers asking questions about screening or testing for COVID-19. This Advisory attempts to answer similar questions in regard to getting the vaccination for COVID-19.

1. Can organizations ask whether a customer or employee has received a vaccination for COVID-19?

Private sector businesses and other organizations engaged in commercial activities in Saskatchewan are not covered by *The Freedom of Information and Protection of Privacy Act* (FOIP) and *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP), but are subject to orders made under *The Public Health Act, 1994*. Many organizations are covered by the *Personal Information Protection and Electronic Documents Act* (PIPEDA). I note that PIPEDA only protects personal information of employees of federally regulated businesses, works and undertakings (FWUBs). Those organizations, if they have questions, may have to contact the Federal Privacy Commissioner . It should be noted that the federal government has introduced Bill C-11, which introduces significant changes to PIPEDA. 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 following definitions, the advice below can be considered best practice and an employer can choose to follow it.

2. What organizations are covered by PIPEDA?

PIPEDA defines an "organization" in Part 1, section 2(1) as follows:

> 2. "organization" includes an association, a partnership, a person and a trade union.**"**

PIPEDA indicates that the "protection of personal information" applies as:

> 4. (1) This Part applies to every organization in respect of personal information that
> (a) the organization collects, uses or discloses in the course of commercial activities; or

PIPEDA defines "commercial activity" as follows:

> 2. "commercial activity" means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

As one can see, an "organization" is broad and includes a business, community based organization and charity, if that organization carries on commercial activity. In the rest of this Advisory I will refer to them as "organizations".

3. Can an employer ask an employee whether they have received the vaccination for COVID-19?

Some employers may be considering whether they will require their employees to receive the vaccine or provide a vaccination certificate 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 they need all employees to receive the vaccine or provide a vaccination certificate to make the workplace safer.

Prior to considering what privacy legislation might apply, employers need to seriously consider whether they want to require employees to receive the vaccine or provide a vaccination certificate. Because these vaccines are new, there will be many questions about their use and effectiveness. There may be workplaces where social distancing, wearing masks and washing hands may be determined to be sufficient protection. These are considerations for the employer. Requiring employees to receive the vaccine is a fundamental issue and can be controversial. Requiring proof an employee has received the vaccine is less controversial, but does have privacy implications. 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. This particularly is a challenging issue for hospitals, medical clinics, long-term care and group homes. Employers need to know that requiring employees to receive the vaccine or provide a vaccination certificate, might result in a court challenge.

The OPC 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 Advisory presumes an employer has made the decision to require vaccinations and understands the legal risks of a challenge, but intends to proceed.

4. What questions might an employer ask?

If an employer decides to require vaccinations, what questions might the employer be asking? Possible questions include:

- Are you planning to get vaccinated?
- When will you receive your first injection?
- Have your received your first injection?
- When will you receive your second injection?
- Have you received your second injection?
- Will you provide me a vaccination certificate?

5. What privacy legislation might apply?

If an employer decides to require its employees to get vaccinated or provide a vaccination certificate, the employer needs to know what privacy legislation applies. 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.

The Health Information Protection Act (HIPA) applies to health trustees which include government institutions, the Saskatchewan Health Authority, a licenced personal care home, a health professional licenced under an Act, a pharmacy, and licenced medical laboratories with custody or control of personal health information. 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 personal information/personal health information. To be sure, an employer should check each of the Acts to see if it has any application. If in doubt, the employer should obtain legal advice.

Regulations under each of the Acts can also prescribe the organizations that are government institutions, local authorities or health trustees.

The Privacy Act may allow a lawsuit where a business, community based organization, employer or health trustee has breached someone's privacy.

A further issue is that after the employee has received the vaccine, is the employee required to show a proof of vaccination? Will the employer accept the employee's word that the vaccination was taken? If the employee is required to provide proof, will the employer visually examine it or make a copy of it? If so, by whom and for what purpose? If a copy is made, the record may be accessible under HIPA, FOIP or LA FOIP.

If an employer is in doubt regarding requiring employees to get vaccinated or requiring a copy of the vaccination certificate, the employer should obtain legal advice.

6. What is the purpose of the employer asking whether an employee has gotten a vaccine or requiring a vaccination certificate?

Before embarking upon requiring vaccinations, the employer must determine the purpose for which it is requiring vaccinations and the purpose for requiring a copy of the vaccination certificate. Is it to keep the workplace safe? More specifically, is it to prevent transmission of COVID-19 being spread from employee to employee, customer or patient? It is important that the employer not expand the purpose after the fact.

7. How should employers notify its employees of the purpose?

Employers should be open and transparent. They should advise staff that they will be asking whether the employee has received the vaccine, has a vaccination certificate and inform them of the purpose. Later, at the time of collection of the vaccination certificate, tell employees the purpose of the 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, why and under what legal authority.

The employer can provide other staff with statistical information, such as how many have been vaccinated. The employer should not give out names or identify the ones who were or were not vaccinated as this may be considered a privacy breach.

8. What information will the employer collect?

Asking an employee whether they have had the vaccination and requesting a vaccination certificate is a collection of personal information/personal health information. Employers should collect the least amount of information necessary to achieve the purpose. If the employer is comfortable, they could choose to accept the employee's verbal statement that they have had the vaccination. Alternatively, the employer could ask the employee to show a vaccination certificate, but choose not to make a copy of the vaccination certificate. This is referred to as the data minimization principle, that is, only collect what is needed to achieve the purpose.

9. What if an employee refuses to be vaccinated?

If an employee refuses to get the vaccination, refuses to confirm that they had the vaccination or refuses to provide a vaccination certificate, employers will need to decide if it will require the employee to wear a mask at work, stay home and self-isolate, send the employee home without pay or end the employment relationship.

10. Can the employer use the information for any other purpose?

The employer must determine its authority to collect for a defined purpose, and only collect personal information/personal health information for that purpose. This may include the employee providing the information for that purpose (indicating they had a vaccination and provided a vaccination certificate). The employer should check the relevant legislation before using that information for any other purpose without getting the consent of the employee.

11. Who can the employer share the information with?

Since the employer has collected the information that the employee has received the vaccination or refused to get it, the employer needs to determine who in the organization needs to know. If the employee gets the vaccination, very few people need to know, but the employer can provide statistical information as to how many employees have received the vaccination. If the employee refuses to get the vaccination and is sent home, very few people need to know. Just like other sensitive health information, it is confidential, the employer should prohibit supervisors and HR employees from sharing the information with other staff. This does not prevent an individual employee from alerting others around them that they have been vaccinated (sticker, badge, lanyard, headband). An employer could promote this, but should not make it mandatory.

12. 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 vaccination of employees or refusal to vaccinate. 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/personal health information about an employee, it is the employer's obligation to ensure it is protected and only those with a need-to-know should be able to access it.

13. 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 privacy legislation, best practice would suggest the information be protected. 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.

14. 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 six months? Employers need to decide whether they will develop a policy including destruction guidelines. Maybe the information collected can be destroyed earlier than an employer's standard procedure.

15. Do employers need to develop a policy on COVID-19 vaccinations?

Once an employer has made a decision, the employer should consider developing a policy. 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 COVID-19 vaccinations. Whatever the form of the document, it should contain:

- authority for the collection;
- a statement of the purpose;
- a statement as to whether employees will be asked to show a vaccination certificate;
- a statement on possible actions taken based on whether the employee has the vaccination or not;
- a statement on where information will be stored;
- a statement as to who it will be shared with (with public authorities or not); and
- a statement on when the information will be destroyed.

16. Can a public body ask visitors whether they have had a vaccination for COVID-19?

Public bodies (government institutions and local authorities) have carried on their activities during the pandemic. As much as possible, communications have shifted to emails and telephone calls, but it is still possible that citizens or patients will attend at a public bodies' front door or reception area. The question arises, can those public bodies ask questions about receipt of a vaccination for COVID-19? Secondly can public bodies insist on seeing the vaccination certificate? If a public body decides to ask the citizen or patient whether they had a vaccination, then many of the questions raised above would apply. Of course public bodies considering this issue should think about obtaining legal advice.

17. Can a health trustee ask whether patients or employees received a vaccination for COVID-19?

Health trustees are subject to HIPA. That Act contains principles similar to FOIP and LA FOIP when it comes to collection, use, protection or disclosure of information (in this case personal health information). Many of the questions posed and answered above will apply to health trustees.

Conclusion

The principles are simple: establish the purpose and authority, 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 a business, non profit, employer or health trustee is subject to privacy legislation or not.

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.

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

Media contact:
Julie Ursu
jursu@oipc.sk.ca

Additional Resources

UK Information Commissioner Office:
Data protection and coronavirus – advice for organizations
Data protection and coronavirus – six data protection steps for organizations
Health, social care organisations and coronavirus – what you need to know

Alberta Office of the Information and Privacy Commissioner:
Pandemic FAQ: Customer Lists

British Columbia Office of the information and Privacy Commissioner:
Collecting Personal Information at Food and Drink establishments, gatherings, and events during COVID-19

Ontario Office of the Information and Privacy Commissioner:
COVID Alert and Your Privacy

March 3, 2021 – UPDATED – Advisory from the Office of the Information and Privacy Commissioner of Saskatchewan on questions regarding vaccines for organizations, employers and health trustees

Announcements regarding the approval of vaccines for COVID-19 has been greeted with excitement. The roll out of vaccines is occurring in our province and in other provinces in Canada. As citizens receive the vaccine, questions arise as to how organizations, health trustees and employers will handle this new reality. In my *Advisory from the Office of the Information and Privacy Commissioner of Saskatchewan on questions, screening or testing by employers regarding COVID-19*, I attempted to answer many of the questions surrounding the issue of employers asking questions about screening or testing for COVID-19. This Advisory attempts to answer similar questions in regard to getting the vaccination for COVID-19.

1. Can organizations ask whether a customer or employee has received a vaccination for COVID-19?

Private sector businesses and other organizations engaged in commercial activities in Saskatchewan are not covered by *The Freedom of Information and Protection of Privacy Act* (FOIP) and *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP), but are subject to orders made under *The Public Health Act, 1994*. Many organizations are covered by the *Personal Information Protection and Electronic Documents Act* (PIPEDA). I note that PIPEDA only protects personal information of employees of federally regulated businesses, works and undertakings (FWUBs). Those organizations, if they have questions, may have to contact the Federal Privacy Commissioner . It should be noted that the federal government has introduced Bill C-11, which introduces significant changes to PIPEDA. 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 following definitions, the advice below can be considered best practice and an employer can choose to follow it.

2. What organizations are covered by PIPEDA?

PIPEDA defines an "organization" in Part 1, section 2(1) as follows:

> 2. "organization" includes an association, a partnership, a person and a trade union.**"**

PIPEDA indicates that the "protection of personal information" applies as:

> 4. (1) This Part applies to every organization in respect of personal information that
>
> (a) the organization collects, uses or discloses in the course of commercial activities; or

PIPEDA defines "commercial activity" as follows:

> 2. "commercial activity" means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

As one can see, an "organization" is broad and includes a business, community based organization and charity, if that organization carries on commercial activity. In the rest of this Advisory I will refer to them

as “organizations” and they are covered by PIPEDA and not by FOIP or LA FOIP.

Let us now turn to discuss employers who are covered by FOIP, LA FOIP or The Health Information Protection Act (HIPA).

3. Can an employer ask an employee whether they have received the vaccination for COVID-19?

Some employers may be considering whether they will require their employees to receive the vaccine or provide a vaccination certificate 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 they need all employees to receive the vaccine or provide a vaccination certificate to make the workplace safer.

Prior to considering what privacy legislation might apply, employers need to seriously consider whether they want to require employees to receive the vaccine or provide a vaccination certificate. Because these vaccines are new, there will be questions about their use and effectiveness. There may be workplaces where social distancing, wearing masks and washing hands may be determined to be sufficient protection. These are considerations for the employer. Requiring employees to receive the vaccine is a fundamental issue and can be controversial. Requiring proof an employee has received the vaccine is less controversial, but does have privacy implications. 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. This particularly is a challenging issue for hospitals, medical clinics, long-term care and group homes. Employers need to know that requiring employees to receive the vaccine or provide a vaccination certificate, might result in a court challenge.

The OPC 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 Advisory presumes an employer has made the decision to require vaccinations and understands the legal risks of a challenge, but intends to proceed.

4. What questions might an employer ask?

If an employer decides to require vaccinations, what questions might the employer be asking? Possible questions include:

- Are you planning to get vaccinated?
- When will you receive your first injection?
- Have you received your first injection?
- When will you receive your second injection?
- Have you received your second injection?
- Do you have a vaccination certificate?
- Will you show me a vaccination certificate?
- Will you provide me with a vaccination certificate?

The least intrusive approach would be that an employer requests, “Please show me your vaccination certificate”. The employer looks at the certificate and does nothing else. Slightly more intrusive would be where the employer checks off on an employee list that this employee has a vaccination certificate.

5. What questions might be asked in a pre-employment interview?

The above questions could be asked of existing employees. Another question is what employers might want to ask of people applying for a job. Employers will need to decide whether they ask any questions or no questions at all.

6. What privacy legislation might apply?

If an employer decides to require the employee to show or provide a vaccination certificate, the employer needs to know what privacy legislation applies. 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 include government institutions, the Saskatchewan Health Authority, a licenced personal care home, a health professional licenced under an Act, a pharmacy, and licenced medical laboratories with custody or control of personal health information. 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 personal information/personal health information. To be sure, an employer should check each of the Acts to see if it has any application to it. If in doubt, the employer should obtain legal advice.

Regulations under each of the Acts can also prescribe the organizations that are government institutions, local authorities or health trustees.

The Privacy Act may allow a lawsuit where a business, community based organization, employer or health trustee has breached someone's privacy.

A further issue is that after the employee has received the vaccine, is the employee required to show or provide a proof of vaccination? Will the employer accept the employee's word that the vaccination was taken? If the employee is required to provide proof, will the employer visually examine it or make a copy of it? If so, by whom and for what purpose? If a copy is made, the record may be accessible under HIPA, FOIP or LA FOIP.

If an employer is in doubt regarding requiring employees to get vaccinated or requiring a copy of the vaccination certificate, the employer should obtain legal advice.

7. What is the purpose of the employer asking whether an employee has gotten a vaccine or requiring a vaccination certificate?

Before embarking upon requiring vaccinations, the employer must determine the purpose for which it is requiring vaccinations and the purpose for an employee showing or providing a vaccination certificate. Is it to keep the workplace safe? More specifically, is it to prevent transmission of COVID-19 being spread from employee to employee, customer or patient? It is important that the employer define the purpose before starting and not change the purpose after starting.

8. How should employers notify its employees of the purpose?

Employers should be open and transparent. They should advise staff that they will be asking the employee to show or provide the vaccination certificate and inform them of the purpose and the purpose for so asking. Later, at the showing or providing of the vaccination certificate, tell employees the purpose of the 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, why and under what legal authority.

The employer can provide other staff with statistical information, such as how many have been vaccinated. The employer should not give out names or identify the ones who were or were not vaccinated as this may be considered a privacy breach.

9. What information will the employer collect?

Asking an employee whether they have had the vaccination and requesting the showing or providing of a vaccination certificate is a collection of personal information/personal health information. Employers should collect the least amount of information necessary to achieve the purpose. If the employer is comfortable, they could choose to accept the employee's verbal statement that they have had the vaccination. Alternatively, the employer could ask the employee to show a vaccination certificate, but choose not to make a copy of the vaccination certificate. This is referred to as the data minimization principle, that is, only collect what is needed to achieve the purpose.

10. What if an employee refuses to be vaccinated?

If an employee refuses to get the vaccination, refuses to confirm that they had the vaccination or refuses to show or provide a vaccination certificate, employers will need to decide if it will require the employee to wear a mask at work, stay home and self-isolate, send the employee home without pay or end the employment relationship.

11. Can the employer use the information for any other purpose?

The employer must determine its authority to collect for a defined purpose, and only collect personal information/personal health information for that purpose. This may include the employee providing the information for that purpose (indicating they had a vaccination and showing or providing a vaccination certificate). The employer should check the relevant legislation before using that information for any other purpose without getting the consent of the employee.

12. Who can the employer share the information with?

Since the employer has collected the information that the employee has received the vaccination or refused to get it, the employer needs to determine who in the organization needs to know. If the employee gets the vaccination, very few people need-to-know, but the employer can provide statistical information as to how many employees have received the vaccination. If the employee refuses to get the vaccination and is sent home, very few people need-to-know. Just like other sensitive health information, it is confidential, the employer should prohibit supervisors and HR employees from sharing the information with other staff. This does not prevent an individual employee from alerting others around them that they have been vaccinated (sticker, badge, lanyard, headband). An employer could promote this, but should not make it mandatory.

13. Where does an employer store this information?

The choices are storing on the employees HR personnel file, storing on the employee's separate health information file or storing in a separate folder for all employees, containing all information regarding vaccination of employees or refusal to vaccinate. 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/personal health information about an employee, it is the employer's obligation to ensure it is protected and only those with a need-to-know should be able to access it. Possibly the best practice is to set up a separate employee file to contain any personal health information collected. That would include COVID-19 vaccination and testing information.

14. 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 privacy legislation, best practice would suggest the information be protected. 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.

15. 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 employer's destruction of documents policy? Should it have a special destruction period, shorter than the normal? Could it or should it be destroyed within six months? Employers need to decide whether they will develop a policy including destruction guidelines. Maybe the information collected can be destroyed earlier than an employer's standard procedure.

16. Do employers need to develop a policy on COVID-19 vaccinations?

Once an employer has made a decision, the employer should consider developing a policy. 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 COVID-19 vaccinations. Whatever the form of the document, it should contain:

- authority for the collection;
- a statement of the purpose;
- a statement as to whether employees will be asked to show a vaccination certificate;
- a statement on possible actions taken based on whether the employee has the vaccination or not;
- a statement on where information will be stored;
- a statement as to who it will be shared with (with public authorities or not); and
- a statement on when the information will be destroyed.

17. Can a public body ask visitors whether they have had a vaccination for COVID-19?

Public bodies (government institutions and local authorities) have carried on their activities during the pandemic. As much as possible, communications have shifted to emails and telephone calls, but it is still possible that citizens or patients will attend at a public bodies' front door or reception area. The question arises, can those public bodies ask questions about receipt of a vaccination for COVID-19? Secondly can public bodies insist on seeing a vaccination certificate? If a public body decides to ask the

citizen or patient whether they had a vaccination, then many of the questions raised above would apply. Of course public bodies considering this issue should think about obtaining legal advice.

18. Can a health trustee ask whether patients or employees received a vaccination for COVID-19?

Health trustees are subject to HIPA. That Act contains principles similar to FOIP and LA FOIP when it comes to collection, use, protection or disclosure of information (in this case personal health information). Many of the questions posed and answered above will apply to health trustees.

Conclusion

The principles are simple: establish the purpose and authority, 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 a business, non profit, employer or health trustee is subject to privacy legislation or not.

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.

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

Media contact:
Julie Ursu
jursu@oipc.sk.ca

Additional Resources

UK Information Commissioner Office:
Data protection and coronavirus – advice for organizations
Data protection and coronavirus – six data protection steps for organizations
Health, social care organisations and coronavirus – what you need to know

Alberta Office of the Information and Privacy Commissioner:
Pandemic FAQ: Customer Lists

British Columbia Office of the information and Privacy Commissioner:
Collecting Personal Information at Food and Drink establishments, gatherings, and events during COVID-19

Ontario Office of the Information and Privacy Commissioner:
COVID Alert and Your Privacy

May 19, 2021 – Vaccine passports must meet highest level of privacy protection

Privacy should be front and centre as governments and businesses consider COVID-19 vaccine passports as a tool to help Canadians return to normal life, say Canada's privacy guardians.

Vaccine passports would allow people to travel and gather again and could support economic recovery while protecting public health. They would, however, require individuals to disclose personal health information about their vaccine or immunity status in exchange, potentially, for access to goods and services, for example, restaurants, sporting events and airline travel.

"While this may offer substantial public benefit, it is an encroachment on civil liberties that should be taken only after careful consideration," federal, provincial and territorial privacy commissioners and the ombuds of Manitoba and New Brunswick say in a joint statement issued today.

"Vaccine passports must be developed and implemented in compliance with applicable privacy laws. They should also incorporate privacy best practices in order to achieve the highest level of privacy protection commensurate with the sensitivity of the personal health information that will be collected, used or disclosed," the statement says.

The statement was endorsed during the annual meeting of federal, provincial and territorial access to information and privacy guardians. The Manitoba Ombudsman hosted the meeting, which took place virtually given the pandemic.

This statement outlines fundamental privacy principles that should be adhered to in the development of vaccine passports.

In particular, it notes that, in light of the significant privacy risks involved, the necessity, effectiveness and proportionality of vaccine passports must be established for each specific context in which they will be used.

In other words, vaccine passports need to be shown to be necessary to achieve the intended public health purpose; they need to be effective in meeting that purpose; and the privacy risks must be proportionate to the purpose, i.e. the minimum necessary to achieve it.

Further, vaccine passports, whether introduced by governments or public bodies for public services, or by private organizations, need to have clear legal authority. In addition, organizations considering vaccine passports should consult with the privacy commissioners in their jurisdiction as part of the development process.

The statement also notes that any personal health information collected through vaccine passports should be destroyed and vaccine passports decommissioned when the pandemic is declared over by public health officials or when vaccine passports are determined not to be a necessary, effective or proportionate response to address their public health purposes. Vaccine passports should not be used for any purpose other than COVID-19.

Related Documents
Joint statement – Privacy and COVID-19 Vaccine Passports

For more information:
Office of the Privacy Commissioner of Canada
Manitoba Ombudsman
Provincial and territorial privacy Ombudspersons and Commissioners

Media Contact
Julie Ursu
jursu@oipc.sk.ca

June 2, 2021 – Federal, Provincial and Territorial Information and Privacy Commissioners and Ombudsman issue joint resolution about privacy and access to information rights during and after a pandemic

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

The global pandemic has brought to the forefront the pressing need for strong access to information and privacy laws. The regulators noted that the pandemic has accelerated trends that were ongoing prior to March 2020, namely concerns among the public about increasing surveillance by public bodies and private corporations and the slowing down of processing access requests. The pandemic has also highlighted the need to modernize the access to information system by leveraging technology and innovation to advance transparency.

Saskatchewan's Information and Privacy Commissioner, Ron Kruzeniski, Q.C., stated:

> "There is no doubt that technology and digitization have been instrumental in the response to the pandemic. As we work towards recovery, I encourage authorities to consider the impact such initiatives have on our access and privacy rights. The lessons we have learned during this global crisis should be used to modernize our access and privacy legislation. Digitization is here to stay. It is time our legislation reflected that."

The joint resolution adopted 11 access to information and privacy principles and called on Canada's governments to show leadership by implementing them and making the modernization of legislative and governance regimes around freedom of information and protection of privacy a priority.

Related Document:
Joint Resolution: Reinforcing Privacy and Access to Information Rights During and After a Pandemic

Media Contact:
Julie Ursu, Manager of Communication
Office of the Saskatchewan Information and Privacy Commissioner
Phone: 306-798-2260
Email: jursu@oipc.sk.ca

Joint Statements by the Federal, Provincial and Territorial Commissioners

FPT Joint Statement – Privacy and COVID-19 Vaccine Passports

May 19, 2021

Background

Vaccine passports[1] are being considered by some governments and businesses as a means of allowing a return to something more closely resembling normal life. Canada's Privacy Commissioners have decided to make a statement at this time in an effort to ensure that privacy is considered at the earliest opportunity as part of any discussions about vaccine passport development.

A vaccine passport can take a number of different forms, such as a digital certificate presented on a smart phone app or a paper certificate, but it essentially functions to provide an individual with a verified means of proving they are vaccinated in order to travel or to gain access to services or locations. Proponents justify this measure based on the idea that vaccinated individuals have a significantly decreased risk of becoming infected and a decreased risk of infecting others.[2] If supported by evidence of their effectiveness, vaccine passports could bring about broad and impactful benefits, including allowing increased personal liberties, fewer restrictions on social gatherings, and accelerated economic recovery resulting from greater participation in society.

At its essence, a vaccine passport presumes that individuals will be required or requested to disclose personal health information – their vaccine/immunity status – in exchange for goods, services and/or access to certain premises or locations. While this may offer substantial public benefit, it is an encroachment on civil liberties that should be taken only after careful consideration. This statement focuses on the privacy considerations.

Vaccine passports must be developed and implemented in compliance with applicable privacy laws. They should also incorporate privacy best practices in order to achieve the highest level of privacy protection commensurate with the sensitivity of the personal health information that will be collected, used or disclosed.

Above all, and in light of the significant privacy risks involved, the necessity, effectiveness and proportionality of vaccine passports must be established for each specific context in which they will be used.

- **Necessity:** vaccine passports must be necessary to achieve each intended public health purpose. Their necessity must be evidence-based and there must be no other less privacy-intrusive measures available and equally effective in achieving the specified purposes.

[1] Vaccine passport is the most common term, which refers to a means of confirming a person's COVID-19 vaccination or immunity status. There are others, such as immunity passport, vaccine or vaccination certificate or card, and digital proof of vaccination, and all of these terms may have slightly different meanings in different jurisdictions.

[2] According to the recent Report of the Chief Science Advisor of Canada on this issue (March 31, 2021).

- **Effectiveness:** vaccine passports must be likely to be effective at achieving each of their defined purposes at the outset and must continue to be effective throughout their lifecycle.
- **Proportionality:** the privacy risks associated with vaccine passports must be proportionate to each of the public health purposes they are intended to address. Data minimization should be applied so that the least amount of personal health information is collected, used or disclosed.

The necessity, effectiveness and proportionality of vaccine passports must be continually monitored to ensure that they continue to be justified. Vaccine passports must be decommissioned if, at any time, it is determined that they are not a necessary, effective or proportionate response to address their public health purposes.

We recognize that scientific knowledge about COVID-19 and the vaccines is advancing quickly and discussions about vaccine passports are underway in some jurisdictions. When contemplating the introduction of vaccine passports, we recommend that governments and businesses adhere to the following privacy principles:

- **Legal authority:** There must be clear legal authority for introducing use of vaccine passports for each intended purpose. Public and private sector entities that require or request individuals to present a vaccine passport in order to receive services or enter premises must ensure that they have the legal authority to make such a demand or request. Clear legal authority for vaccine passports may come from a new statute, an existing statute, an amendment to a statute, or a public health order that clearly specifies the legal authority to request or require a vaccine passport, to whom that authority is being given, and the specific circumstances in which that can occur.
- **Consent and trust:** For vaccine passports introduced by and for the use of public bodies, consent alone is not a sufficient basis upon which to proceed under existing public sector privacy laws. Furthermore, consent alone may not be meaningful for people dealing with governments and public bodies that often have a monopoly over the services they provide. The legal authority for such passports should therefore not rely on consent alone.

For businesses and other entities that are subject to private sector privacy laws and are considering some form of vaccine passport, the clearest authority under which to proceed would be a newly enacted public health order or law requiring the presentation of a vaccine passport to enter a premises or receive a service. Absent such order or law, i.e. relying on existing privacy legislation, consent may provide sufficient authority if it meets all of the following conditions, which must be applied contextually given the specifics of the vaccine passport and its implementation:

- Consent must be voluntary and meaningful, based on clear and plain language describing the specific purpose to be achieved;
- The information must be necessary to achieve the purpose;
- The purpose must be one that a reasonable person would consider appropriate in the circumstances;
- Individuals must have a true choice: consent must not be required as a condition of service.

In Quebec, consent cannot form the legal basis for vaccine passports. In that jurisdiction, requesting their presentation would require that the information is necessary to achieve a specific purpose, one that is serious and legitimate.

- **Limiting Collection, Use, Disclosure and Retention / Purpose Limitation:** The collection, use, disclosure and retention of personal health information should be limited to that which is necessary for the purposes of developing and implementing vaccine passports. Active tracking or logging of an individual's activities through a vaccine passport, whether by app developers, government, or any third party, should not be permitted. Also, the creation of new central databases of vaccine information nationally or across jurisdictions should not be permitted, other than the local databases necessary for the administration and verification of the vaccine. Secondary uses of personal health information collected, used or disclosed through vaccine passports must be limited to only those required or authorized by law.
- **Transparency:** Canadians should be informed about the purposes and scope of vaccine passports and about the collection, use, disclosure, retention and disposal of their personal health information for the purposes of vaccine passports.
- **Accountability:** Policies, agreements and laws must minimize any impact on privacy. Individuals should be informed about who to contact to request access to, and correction of, any information available through vaccine passports or to make an inquiry or complaint about vaccine passports.
- **Safeguards:** Technical, physical and administrative safeguards must be put in place that are commensurate with the sensitivity of the information to be collected, used or disclosed through vaccine passports. Processes must be put in place to regularly test, assess and evaluate the effectiveness of the privacy and security measures adopted.
- **Independent Oversight:** To ensure accountability and reinforce public trust, Privacy Commissioners should be consulted throughout the development and implementation of vaccine passports. Privacy Impact Assessments or other meaningful privacy analyses should be completed, reviewed by Privacy Commissioners, and a plain-language summary published proactively.
- **Time and Scope Limitation:** Any personal health information collected through vaccine passports should be destroyed and vaccine passports decommissioned when the pandemic is declared over by public health officials or when vaccine passports are determined not to be a necessary, effective or proportionate response to address their public health purposes. Vaccine passports should not be used for any purpose other than COVID-19.

FPT Joint Resolution – Reinforcing Privacy and Access to Information Rights During and After a Pandemic

June 2, 2021

CONTEXT

- The public health emergency arising from the COVID-19 pandemic has seriously impacted access to information and respect for individual's privacy rights.
- The pandemic has accelerated trends that were ongoing prior to March 2020. It has heightened concerns among the public about increasing surveillance by public bodies and private corporations and has significantly slowed the processing of many access requests and highlighted a need to modernize this system.
- Privacy and access rights are quasi-constitutional rights. Governments have an obligation to protect them. Particularly during an emergency, respect for the privacy and access to information rights of Canadians remains crucial. This also helps demonstrate accountability in times of crisis.
- Access to government information and respect for privacy are essential for governments to be held accountable for their actions and decisions, and to maintain the public's trust in times of widespread crisis. By ensuring confidence in decision-making, design and implementation of emergency measures and the systems that support them, access to information and privacy laws actually promote and assist the health and well-being of individuals and their families.
- The lessons learned during this global crisis should be used to improve access to information and protection of personal data as we recover from the current crisis, not only to become better prepared for emergency situations in the future, but also to help Canadians adapt to the new normal of a digital era that is here to stay.
- Recovery and resumption of activities - supported by innovation, technology and digitization - will only be successful and sustainable when they also protect the interests and rights of all citizens.

THEREFORE

Canada's Information and Privacy Commissioners call on their respective governments to show leadership and apply the following principles in the implementation and the necessary modernization of governance regimes around freedom of information and protection of privacy:

In terms of Access:

- Federal, provincial and territorial institutions must recognize the importance of transparency, and uphold the right of access to information during an emergency by ensuring business continuity plans include measures for processing requests for access.
- Institutional leaders must provide clear guidance and direction on the ongoing importance of information management in this new operating environment, which may include working remotely. Properly documenting institutional decisions and any resulting actions, and organizing and storing such documentation in a manner that enables timely access to such documentation are central to principles of open, transparent and responsible government.
- Governments should emphasize both the proactive and voluntary disclosure of government information – particularly, information of significant public interest related to policy-making, public health, public safety, economy, procurements and benefits.

- Respecting the privacy of individuals is critically important. Public bodies must be open and transparent with non-personal or aggregate-level information that the public needs to know to make informed choices and decisions about how to protect themselves and to ensure fair distribution of risks and benefits among all members of society, including the most vulnerable and marginalized groups.
- Federal and provincial institutions should leverage technology and innovation now and in the future to advance the principle of transparency in a manner that meets the public interest and accords with the modern needs of a digital society. The modernization of access-to-information systems must focus on innovative approaches and new information technologies, supported by adequate human resources.

In terms of Privacy:

- To appropriately address digital transformation, privacy laws must be interpreted so as to recognize the fundamental nature of the right to privacy and apply it in a modern, sustainable way, by allowing for responsible innovation that is in the public interest and prohibiting uses of technology that are incompatible with our rights and values.
- Exceptions exist in privacy laws to enable the collection, use and disclosure of personal information for public health purposes during a pandemic and other emergencies. Privacy laws should not be characterized by those subject to them as a barrier to appropriate collection, use and sharing of information. Instead, privacy laws, norms and best practices should be viewed as a way to ensure responsible data use and sharing that supports public health and promotes trust in our healthcare system and governments.
- Emergency measures, including those related to economic and social recovery, should incorporate principles of "privacy by design" to ensure the collection, use and disclosure of personal information is done fairly, lawfully, and securely, in a transparent manner that promotes demonstrable accountability.
- Emergency response and recovery measures involving the exceptional collection, use and disclosure of personal information without consent must be necessary and proportionate in scope, meaning they must be evidence-based, necessary for the specific purpose identified, not overbroad and time-limited.
- Personal information collected in support of emergency measures should be destroyed when the crisis ends, except where the purpose for which the information was collected extends beyond the end of the crisis, or for narrow purposes such as research, ongoing healthcare, or ensuring accountability for decisions made during the emergency, particularly decisions about individuals and marginalized groups.
- Public and private entities must respect principles of data minimization and use limitation, and be required to use de-identified or aggregate-level data, whenever possible, when informing others of information they need to know to keep safe, including the general public.

Source: https://oipc.sk.ca/assets/2021-06-02_-joint-resolution_privacy-and-access-rights-in-pandemic-1.pdf

Statements by the International Conference of Information Commissioners

Access to Information in the context of a global pandemic Statement

14 April 2020

The impact of coronavirus (COVID-19) brings unprecedented challenges for our society, both nationally and globally.

Public authorities must make significant decisions that affect public health, civil liberties and people's prosperity.

The public's right to access information about such decisions is vital.

As a global community, we recognize that resources may be diverted away from usual information rights work. Public organisations will rightly focus their resources on protecting public health, and we recognise our role in taking a pragmatic approach, for example around how quickly public bodies respond to requests.

But the importance of the right to access information remains.

Public bodies must also recognize the value of clear and transparent communication, and of good record-keeping, in what will be a much analysed period of history.

As an international network, the International Conference of Information Commissioners (ICIC) supports a flexible approach that takes into account the compelling public interest in the current health emergency, while safeguarding the values of the right to access information. We ask governments to support this vision.

We add our support and gratitude to those who are dedicated to tackling the current pandemic.

The signatories:

ICIC Members

- Alberta(Canada)- Office of the Information and Privacy Commissioner
- Argentina- Agencia de Acceso a la Información Pública
- Australia- Office of the Australian Information Commissioner
- Bermuda– Information Commissioner's Office
- Brazil - Controladoria-Geral da União (CGU)
- Cayman Islands-Ombudsman
- Chile– Consejo para la Transparencia
- Coahuila (Mexico) – Instituto Coahuilense de Acceso a la Informacion Publica
- Guatemala- Procuraduría de los Derechos Humanos de Guatemala

- Hungary- Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)
- Isle of Man - Information Commissioner
- Israel – Freedom of Information Unit
- Kenya - Commission on AdministrativeJ ustice (Office of the Ombudsman)
- Mexico - Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)
- Nepal- National Information Commission
- Nova Scotia (Canada) – Information and Privacy Commissioner for Nova Scotia
- Punjab(Pakistan)-Punjab Information Commission
- The Philippines- Freedom of Information - Project Management Office
- Scotland- Scottish Information Commissioner
- Serbia – Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti
- Sierra Leone – Right to Access Information Commission
- South Africa – Information Regulator (South Africa)
- Spain – Consejo de Transparencia y Buen Gobierno
- Switzerland- Préposé federal à la protection des données et à la transparence(PFPDT)
- Tunisia– Instance Nationale d'Acces a l'Information
- United Kingdom- Information Commissioner's Office
- United States - Office of GovernmentI nformation Services- National Archives and Records Administration

Non-ICIC members

- Andalusia(Spain) - Consejo de Transparencia y Protection de Datos de Andalucia
- Ireland– Office of the Ombudsman
- Rhineland-Palatinate(Germany)-Landesbeauftragte für den Datenschutz und die Informationsfreiheit-Rheinland-Pfalz
- South Australian Ombudsman
- Yukon (Canada)-Information and PrivacyCommissioner

Source: https://www.informationcommissioners.org/covid-19

International Conference of Information Commissioners Joint Resolution on the proactive publication of information relating to the COVID-19 pandemic

June 24, 2021

Title of the resolution	*Proactive publication of information relating to the COVID-19 pandemic*
Author	*The Office of the Australian Information Commissioner* *- Angelene Falk - Australian Information Commissioner and Privacy Commissioner*
Co-sponsors	• *Office of the Information Commissioner, Western Australia, Australia* • *Office of the Victorian Information Commissioner, Victoria, Australia* • *Information and Privacy Commission, New South Wales, Australia* • *Office of the Information Commissioner, Queensland, Australia* • *Office of the Ombudsman, New Zealand* • Information Commissioner of Canada • *Information Commissioner's Office, United Kingdom*
Anchor with the Charter	*The resolution links to the following themes of the 2021 conference:* *- Transparency and trust in pandemic times* *- Privacy and transparency in health issues* *- Transparency by design and document management as means of good governance* *- Access to Information and public services delivery* *The resolution is in the spirit of the ICIC Johannesburg Charter, supporting the vision, mission and goals of the ICIC.* *The resolution supports the ICIC's **Vision** to promote access to information laws and improve transparency and accountability.* *The resolution is consistent with the ICIC's **Mission** to 'share knowledge and best practices, to build capacity, to help identify what is needed for global progress and to act as a collective voice in international fora with a view to improving people's right to public information and their ability to hold to account bodies that provide public functions'.* *The resolution also links to the **Goals** of the ICIC which are to:* *1. Protect and promote access to public information;*

	8. Act as a collective voice in the international community to raise awareness of issues that impact upon access to public information; *9. Promote the development and adoption of international standards in access to public information in all regions across the world, including the establishment of independent oversight bodies.* *(https://www.informationcommissioners.org/goals-and-objectives)*
Body of the Resolution (including rationale)	**PREAMBLE:** RECALLING that: • the Vision of the International Conference of Information Commissioners is to improve transparency and accountability to the benefit of everyone • the Mission of the International Conference of Information Commissioners is to act as a collective voice in international fora with a view to improving people's right to public information and their ability to hold to account bodies that provide public functions • a key Goal of the International Conference of Information Commissioners is to protect and promote access to public information, and raise awareness in the international community of issues that impact upon access to public information. RECOGNISING that the proactive publication or release of information provides public access to information held by government or public institutions without the need for formal access requests; ACKNOWLEDGING that the public's right to access to information relating to the COVID-19 pandemic is of critical importance for providing confidence in, and transparency around, decision making at all levels of public authorities during the crisis; APPRECIATING that the proactive release of information increases participation, scrutiny, discussion, learning, comment and review of government decisions; CONFIRMING the benefits of public engagement in government decision making at all times, but in particular, in times where the participation of all citizens is critical to the success of public health initiatives; **The 12th Annual Closed Session of the International Conference of Information Commissioners** EMPHASIZES the importance of access to information in the context of the ongoing global pandemic; RECOGNISES that public authorities make significant decisions that affect public health, civil liberties and economic participation; PROMOTES the proactive disclosure of information held by government or public institutions, wherever this is appropriate; and

	ENCOURAGES the proactive release of information through existing state-based mechanisms such as information publication schemes and promotes the implementation of such schemes. **The 12th Annual Closed Session of the International Conference of Information Commissioners calls on all members to:** • promote, or continue to promote, proactive publication of information held by government or public institutions relating to the COVID-19 pandemic, wherever appropriate; • continue to share knowledge and best practice in relation to the proactive publication of information as affirmed in the 'ICIC -Access to information in the context of global pandemic COVID-19' statement issued on 14 April 2020; **The 12th Annual Closed Session of the International Conference of Information Commissioners therefore resolves to issue the joint statement (Appendix A to this Resolution) highlighting the importance of proactive disclosure of health and pandemic management information held by government or public institutions during a global pandemic, wherever this is appropriate.**

Appendix A – Joint Statement

PROACTIVE PUBLICATION OF INFORMATION RELATING TO THE COVID-19 PANDEMIC STATEMENT

24 June 2021

The impact of coronavirus (COVID-19) continues to bring unprecedented challenges for our society, both nationally and globally. Governments around the world continue to face significant challenges in responding to the pandemic to protect public health, civil liberties and individual prosperity.

As the global pandemic continues, the importance of transparency and the right to access information remains.

Recognising the role that access to information has in building trust in our global community during times of crisis and beyond, Information Commissioners around the world highlight the importance of the proactive disclosure of information held by government or public institutions.

The 12th Annual International Conference of Information Commissioners therefore urge governments responding to the ongoing global pandemic to pay due regard to the following principles, which reflect common information access principles and practice around the proactive publication of information held by government or public institutions:

- *Proactive disclosure of information held by government or public institutions increases citizen participation in government processes and promotes better informed decision making through increased scrutiny, discussion, comment and review of government decisions.*
- *Public engagement in government decision making is important at all times, but in particular, during a global pandemic.*

- *The public's right of access to information relating to the COVID-19 pandemic is of critical importance to the effectiveness of the public health response, in circumstances where authorities make significant decisions that affect public health, civil liberties and economic participation.*
- *Information held by government or public institutions is to be managed for a public purpose and is a national resource.*
- *To the greatest extent possible, information held by government or public institutions should be published promptly and proactively, without the need for formal access requests.*

Mechanisms, such as information publication schemes and administrative release, encourage the proactive release of information. Members will continue to promote, support, develop and implement such mechanisms to the greatest extent possible.

Source: https://cdn.website-editor.net/61ed7ac1402f428695fcc2386ad0577f/files/uploaded/ADOPTED_ICIC-Resolution-Proactive-publication-of%2520information-relating-to-the-COVID-19-pandemic.pdf

Blog Postings

How About Some Privacy Education for All Our Stuck at Home Kids?

March 24, 2020 – Sherri Fowler, Analyst

Like many of you, I am a mom of a kid who is off school. This is uncharted territory for all of us – I never even had a snow day growing up. Many of us are trying to be creative with what other types of learning we can provide our kids at this time. So, before they become even more obsessed with Fortnite, TikTok and Snapchat (sorry parents, Facebook is not cool anymore), there couldn't be a better time to introduce them to some privacy learning.

The Privacy Commissioner of Canada has produced some excellent resources available at www.youthprivacy.ca. On this website you will find many activities, games and presentations for kids from kindergarten to grade 12 – you might even learn something new about privacy yourself. This site includes resources for teachers and parents to help support your child's privacy learning.

One of my favorites is the *Data Defender* game aimed at kids in grades 4 to 6 that was created by Media Smarts through funding from the Privacy Commissioner of Canada. In it, Algo Rhythm – or Al for short – gives the game player extra moves in exchange for the player agreeing to provide certain details about themselves such as birthdays and friends' email addresses. Throughout the game, you learn about the tricks used online to get you to give up your personal data.

You will also find a great graphic novel: *Social Smarts: Privacy, the Internet and You.* The site describes Social Smarts as*, "…the story of a brother and sister who learn (sometimes the hard way) about the privacy risks related to social networking, mobile devices and texting, and online gaming."* Social Smarts is geared towards teenage readers.

On the site you will also find fun activity sheets and games for younger kids to introduce them to privacy at an age appropriate level.

If you need help to begin a dialogue with your kids about privacy and their online presence check out Topics to Talk About. This includes discussion ideas and guidance on conversations ranging from the importance of password protection to sexting.

I encourage you to check out www.youthprivacy.ca as it has so much great stuff to create a privacy savvy generation.

Balancing Public Interest and Privacy in a Pandemic

March 27, 2020 – Ron Kruzeniski, Information and Privacy Commissioner

As the COVID-19 pandemic becomes more real in our province, 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 grows 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 or do radio and TV interviews. Others will choose not to do that and 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 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."

The Regina Leader Post has developed an article on this issue. It can be found here: Privacy during a pandemic: Sask. gov't being cautious with listing locations of COVID-19 cases

I believe the article takes a balanced approach to this issue.

Many people may have the virus and not even know it so personal distancing and washing hands becomes even more important. 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 officials. This all is done on a need-to-know basis and different methods are utilized depending on the circumstances.

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

Working from home

April 2, 2020 – Sharon Young, Analyst

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.

Phishing Attacks: In Ordinary times and during a Pandemic

April 8, 2020 – Sharon Young, Analyst

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 gain 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.

Contact tracing and privacy

April 14, 2020 – Ron Kruzeniski, Information and Privacy Commissioner and Sharon Young, Analyst

I read an interesting article in *The Atlantic* by Derek Thompson. I was aware that South Korea and Singapore and other Asian countries were applying technology to the issue of contact tracing. What is contact tracing? As I understand it, when someone is diagnosed with having COVID-19, they are asked who they had been in contact with in the last while. Then those individuals are contacted. The old way was to do that by interviews. The existence of smartphones and apps allows contact tracing to take place by using Global Position System (GPS) and Bluetooth technology. For example, in South Korea, GPS is enabling authorities to know where patients have been using information from CCTV footage, credit card records and GPS data from the patient's smartphone. Singapore has taken a different approach by using a government developed app called "Trace Together" that uses signals between mobile phones to record who you may have had close contact with.

Also, Asian countries are using technology to enforce quarantine. For example, Taiwan uses GPS to create an "electronic fence" for those who should be in quarantine. In Hong Kong, those who must quarantine themselves are given a wristband. They are to activate the wristband using a smartphone app.

Finally, technology is being used to enable movement in China as restrictions are being lifted.

I also note that European countries, including Germany and Italy, are also following Asia's lead and are developing and using apps to assist with combating the spread of COVID-19.

It would appear that Asia has been successful in reducing infections and deaths because of their approach to contact tracing along with other measures taken. We in North America are interested in when self-isolation could end and when our economy might get going again but are worried about a second wave. I can see that authorities here in North America will look to the digital methods used in Asia for ways to start the economy and reduce the risk of a second wave. As they consider these issues, alternatives will be presented and no doubt, smartphones will be raised as an option. In fact, Google recently announced on its blog that it is partnering with Apple to use Bluetooth technology to assist governments and health agencies conduct contact-tracing to help reduce the spread of COVID-19.

Technology can help us combat the spread of COVID-19 but it also increases the surveillance citizens are put under. The Electronic Frontier Foundation (EFF) asserts that surveillance invades privacy, deters free speech, and unfairly burdens vulnerable groups.

As North America adjusts its strategies to combat this pandemic, we must consider the impact such initiatives have on our privacy and our democracy. Can these technologies be used in a way that maximizes its potential in combatting the spread of the virus while minimizing the impact it has on our privacy? I am sure they can. I recommend that authorities be transparent in the technology they use. They should consider technology that doesn't collect and retain information unnecessarily. For example, it is being reported that Singapore's "TraceTogether" app uses Bluetooth technology so that information is stored only on the users' mobile phone for 21 days (the incubation period for COVID- 19). If a person tests positive, it is only then that authorities will access the information on the patient's phone so that authorities know who the patient has been in close contact with.

Another way for authorities to be transparent is letting the public know what information they are collecting, the purpose for the collection, and how the information will be used and/or disclosed. Individuals should have access to the information that is collected about them by authorities.

Furthermore, I recommend that authorities also consider how they can collect, use, and/or disclose the information that is necessary for the purpose of combating the spread of COVID-19 and to have processes in place to ensure such information is not used for other purposes, now or in the future. This includes setting a limit on how long information should be retained.

Whatever solutions are posed, my office is here to consult on the privacy implications in advance of any roll-out in Saskatchewan.

Research: post pandemic

April 16, 2020 – Ron Kruzeniski, Information and Privacy Commissioner

As I listen to the news, my head keeps telling me 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 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 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 *The Health Information Protection Act* (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, *The Freedom of Information and Protection of Privacy Act* (FOIP), *The Local Authority Freedom of Information and Protection of Privacy Act* (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 wrote this blog 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.

With a little help from our friends…

April 17, 2020 – Sharon Young, Analyst

Our friends from oversight offices from other provinces and territories have developed some helpful guidance documents to work through issues that are arising from this outbreak of COVID-19. Below is a list of some of these resources.

These resources are a great starting point when working through some of the access and privacy issues we may be coming up against as we go through this pandemic. However, please keep in mind that while Saskatchewan's access and privacy legislation is similar to the legislation in other provinces and territories, there are differences as well. Therefore, double-check with your organization's Privacy Officer for Saskatchewan-specific requirements when working through these access and privacy issues!

Yukon Information and Privacy Commissioner

- Applications to Help You Work from Home: Knows the risks, avoid the risks

Alberta's Office of the Information and Privacy Commissioner

- Managing Records When Transitioning from Work to Home

British Columbia's Office of the Information and Privacy Commissioner

- FIPPA and online learning during the COVID-10 Pandemic

Newfoundland's Office of the Information and Privacy Commissioner

- Don't Blame Privacy – What to Do and How to Communicate in an Emergency

We are working on a Pandemic Binder which will have a collection of statements and blogs that have been issued by our office. We think it is important to have in one spot a collection of issues that are arising during this pandemic.

New Resource: Best Practices for Transporting PI and PHI Outside of the Office

April 28, 2020 – Monique Meister, HIMS Practicum Student

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. It does not matter where 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, when you are travelling to meet with clients, or going offsite to attend meetings.

I hope that these guidelines will also help public bodies create policies, procedures, and guidelines to assist and support employees, if they do not already have that in place.

For more tips on working from home, please also see our blog Working from home.

Other Commissioners

Office of the Information Commissioner of Canada - Access to information in extraordinary times

Gatineau, Quebec, April 2, 2020 — In these extraordinary times, it is understandable that our collective focus as a society is on existential matters of public health and security. We all acknowledge the need for our leaders and decision-makers to be able to react quickly to events and make timely decisions in the best interests of Canadians.

In such circumstances, access to information and information management may not currently be top-of-mind within government institutions, where day-to-day work is focused on rapid decision-making and delivering on issues of prime importance, such as public health and essential financial support to Canadians, among other things.

Nevertheless, if the government is to inspire the confidence in Canadians that will be required to successfully navigate this challenging period as a nation, timely decision-making and the proper documentation of both the decisions and any resulting actions must go hand-in hand.

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.

Of course, because it is impossible to implement measures to ensure transparency retroactively, **now** is the time for government institutions to ensure that appropriate decision-making documentation safeguards and practices are in place. A commentator recently likened the current situation to trying to re-build a plane in midair. In today's circumstances, we cannot forget to ensure that the in-flight data recorder, which captures information in real time as the plane flies, is functioning correctly.

At this moment, while government offices are closed, I understand that many public servants are working from home, and occasionally, using other private communications channels such as personal telephone or computer to avoid overburdening government infrastructure. Every day, work previously done within the confines of government offices is now taking place outside of traditional work arrangements.

While this flexibility and creativity reflect well on Canada's public service and speaks to its level of commitment, 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?

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.

Caroline Maynard
Information Commissioner of Canada

Source: https://www.oic-ci.gc.ca/en/resources/news-releases/access-information-extraordinary-times

Office of the Privacy Commissioner of Canada - A Framework for the Government of Canada to Assess Privacy- Impactful Initiatives in Response to COVID-19

April 2020

Context

The safety and security of the public is of grave concern in the current COVID-19 health crisis. The urgency of limiting the spread of the virus is understandably a significant challenge for government and public health authorities, who are looking for ways to leverage personal information and "Big Data" to contain and gain insights about the novel virus and the global threat it presents. In this context, we may see more extraordinary and less voluntary measures being contemplated, and some of these measures will have significant implications for privacy and civil liberties.

During a public health crisis, privacy laws and other protections still apply, but they are not a barrier to the appropriate collection, use and sharing of information. When reasonably and contextually interpreted, existing privacy legislation, norms and best practices for data collection, use and disclosure ensure responsible data use and sharing that supports public health. They also promote continued trust in our health system and in government generally.

All organizations must continue to operate under lawful authority and act responsibly, particularly with respect to handling personal health information, and information about individuals' travel, movements and contacts or association–all of which are generally considered sensitive. In scenarios involving public-private partnerships, where the lawful authority relied upon for collection is consent provided by individuals to a private-sector partner, the public-sector organization should approach its own collection of that information by ensuring the private-sector framework is properly applied, including meaningfulness of consent.

Privacy protection isn't just a set of technical rules and regulations, but rather represents a continuing imperative to preserve fundamental human rights and democratic values, even in exceptional circumstances. Government institutions should still apply the principles of necessity and proportionality, whether in applying existing measures or in deciding on new actions to address the current crisis. Purpose limitation, that is, ensuring that personal information collected, used or disclosed for public health reasons is not used for other reasons, is particularly important in current circumstances. How personal information is safeguarded, and how long it is retained after the crisis, is also crucial.

The COVID-19 public health crisis has raised exceptionally difficult challenges to both privacy and public health. The following are key privacy principles that should factor into any assessment of measures proposed to combat COVID-19 that have an impact on the privacy of Canadians. It accompanies our previously issued guidance to help departments and organizations subject to federal privacy laws understand their privacy-related obligations during the COVID-19 outbreak. For guidance on other privacy principles that continue to apply, please read Expectations: OPC's Guide to the Privacy Impact Assessment Process.

Framework

1) Legal Authority:

Identify the legal authority to collect, use, and disclose personal information.

Key Messages:

- All organizations must continue to operate with lawful authority. This means, for federal government institutions, the *Privacy Act* and specific laws that govern their activities; for private-sector organizations, PIPEDA or substantially similar provincial laws; and special provisions that may be adopted under emergency laws. (For more information, see our guidance: Privacy and the COVID-19 outbreak).
- Privacy laws apply to personal information, that is information about an identifiable individual. This is so even when using "open" or public sources such as social media, although the reasonable expectation of privacy may be less for such sources. Some laws also allow for use of publicly available data under specific conditions. (See also principle four: de-identification.)

2) Necessity and Proportionality:

Ensure the measures that the government institution wants to take are necessary and proportionate.

The OPC recognizes that the COVID-19 crisis is a rapidly evolving situation that requires swift and effective responses to address extraordinary public health needs. The right to privacy is not absolute. However, even in these challenging circumstances, government institutions should still ensure that their measures are necessary and proportionate, which means essentially evidence-based, necessary for the specific purpose identified and not overbroad.

Key Messages:

- The public health purpose underlying a potentially privacy infringing measure must be science-based and defined with some specificity. It is not enough to simply state that a measure supports public health without being more precise.
- The measure must be tailored in a way that is rationally connected to the specific purpose to be achieved. If the purpose of a measure is to reduce the occurrence of large gatherings in public places, mass collection of all movements of a population would not be proportionate.
- The measure must be necessary; that is, more than potentially useful. Again, it must be evidence-based and likely to be effective. However, demonstrating effectiveness must be assessed in context. Also, necessity does not mean "absolute necessity" (i.e., that no other conceivable means are available, regardless of costs).

The document Expectations: OPC's Guide to the Privacy Impact Assessment Process contains a number of Questions for high-risk programs: necessity, effectiveness, proportionality and minimal intrusiveness that, read in context, can assist government institutions in assessing the privacy impact of measures to address COVID-19.

3) Purpose Limitation:

Personal information collected, used or disclosed to alleviate the public health effects of COVID- 19 must not be used for other reasons.

Key Messages:

- This is particularly important in the current context, where more personal information may be collected, used and disclosed than in normal circumstances. Individuals' reasonable expectation of privacy may be less in a public health crisis, but they would not reasonably expect that sensitive information (such as health or places or persons visited) would be available for other government or commercial purposes.
- Personal information collected in an emergency situation should also be destroyed when the crisis ends, except for narrow purposes such as research or ensuring accountability for decisions made during the crisis, particularly decisions about individuals. (see also principle nine: Time Limitation)

4) De-Identification and other safeguarding measures:

Use de-identified or aggregate data whenever possible.

Key Messages:

- Consider whether identifiable information is required in the context, or if de identified or aggregate data is sufficient.
- Be aware that there is always a real risk of re-identification, although it is generally less for aggregate data. It is important to be attentive to the risks, which are highly case-specific - dependent on what data is used, in what form, and with what other data it is combined, and with whom it will be shared.
- Be especially mindful about the unique challenges with location data:
  - Location data points themselves can lead to reidentifcation as they can reveal personal details, such as the location of an individual's home, routine behaviours, and associations.
  - Precise location data, particularly in real-time, can be very challenging to fully anonymize or de-identify.
- Take administrative, technical and physical means to protect the personal information collected. Ensure safeguards are enhanced for sensitive information.

5) Vulnerable Populations:

Consider the unique impacts on vulnerable groups.

Key Messages:

- Consider how certain information, such as health and precise location data, may have greater sensitivities or disproportionate impacts on vulnerable populations and certain groups of individuals, for example:
  i. For some individuals, the collection of health-related data concerning gender, gender identity and expression is of even greater sensitivity.
  ii. Data sets on populations, or subsets of populations, may affect different subgroups or communities with disproportionate consequences.
  iii. Algorithmic decision-making or AI may contain inherent biases that could create disproportionate impacts.

6) Openness and Transparency:

Provide clear and detailed information to Canadians about new and emerging measures, on an ongoing basis.

Key Messages:

- Transparency is a cornerstone of democratic governance, as well as our privacy laws. It is all the more vital in the midst of a crisis, when extraordinary measures are being contemplated.
- The public, and wherever possible individuals, must be informed of the purpose of the collection of their personal information.

7) Open Data:

Carefully weigh the benefits and risks of the release of public datasets, giving particular attention to health and location data, and impacts on vulnerable populations.

Key Messages:

- An assessment of how granular public datasets should be is context-specific.
- Even with the release of aggregate data, be attentive to the impacts on vulnerable populations, subsets of populations, and groups. Give particular attention when geolocation data is involved, as it can disproportionately impact marginalized and vulnerable communities.

8) Oversight and Accountability:

New laws and measures specific to the crisis should also provide specific provisions for oversight and accountability.

Key Messages:

- Institutional safeguards become more, not less, important during times of crisis.
- New laws should contain provisions for oversight and accountability.

9) Time Limitation:

Privacy invasive measures should be time-limited, with obligations to end when they are no longer required.

Key Messages:

- There should be strict time and other limits on measures implemented in response to the crisis (e.g. type and range of personal data collection, sharing, and use). Time limits should be conservative, with the option to extend.
- Personal information collected in an emergency situation should also be destroyed when the crisis ends, except for narrow purposes such as research or ensuring accountability for decisions made during the crisis.

Source: https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/fw_covid/

ON IPC - Letter to public health and government officials on release of COVID-19 related data

Apr 16 2020

I want to thank you and your staff for all that you are doing to protect the public's health during this crisis. At a time like this, people depend on public servants more than ever, and it's heartening to see health care workers and other essential staff across the province demonstrate their commitment to the public good, despite the risks to their own health and safety.

In the last few weeks, various media outlets have contacted me seeking to clarify what information can and cannot be disclosed by public health units and government organizations concerning the COVID-19 outbreak in Ontario. Because of these questions, I am reaching out to clarify that during a public health crisis, Ontario's privacy laws are not a barrier to sharing information that can help control disease outbreaks, keep the public safe, and allow people to assess the public health response.

Public health units and government organizations should provide as much information as is necessary to protect public health, without naming individuals. This non-identifying information could include numbers of affected individuals, demographic data such as approximate age and gender, as well as geographic locations of infected or deceased individuals, including long term care facilities, or workplaces, especially if they are in a location where large numbers of people might have gathered.

Your efforts to keep Ontarians safe, while protecting the health privacy of individuals, should be lauded. Please feel free to reach out to me or my staff if you have any questions related to the application of Ontario's privacy laws relative to this emergency. While our office is physically closed, the IPC is working and is available at all times for consultation and advice on access and privacy issues.

Again, please accept my thanks and hope for an end to this public health crisis.

Sincerely,

Brian Beamish
Information and Privacy Commissioner of Ontario

Source: https://www.ipc.on.ca/letter-to-public-health-and-government-officials-on-release- of-covid-19-related-data/

Office of the Information Commissioner of Canada - Letter: A Critical Phase for the Access to Information System

April 28, 2020

The Honourable Jean-Yves Duclos
President of the Treasury Board
Jean-Yves.Duclos@parl.gc.ca

Subject: A critical phase for the access to information system

Dear Minister Duclos:

In my public statement of April 2, 2020, Access to Information in Extraordinary Times, I addressed the importance of properly documenting government decisions during the COVID-19 crisis in order to preserve the quasi-constitutional right of access. It is widely accepted that Canadians' trust in their government is contingent upon openness and transparency. Today I am writing to you to signal that the access to information system, a key pillar in safeguarding this trust, is currently in a critical phase and may soon be beyond repair if certain ongoing and developing issues remain unaddressed. However, with the appropriate leadership and some bold choices, this difficult period could prove to be the catalyst for a true renewal of the access system sought by so many.

Context

Even before the pandemic and the widespread adoption of alternative work arrangements, chronic under-resourcing had created backlogs in both access requests and complaints that had grown year after year. Government employees are now working from home on a large scale, with limited access to physical files, protected information and other resources. I understand that this has curtailed much of the gathering of requested documents, and by extension, the ability of access to information teams to process requests and respond to complaints. My office anticipates that the delays we already see will only become worse the longer that alternative work arrangements are in place. Further, we anticipate that some Access to Information and Privacy (ATIP) units will be completely overwhelmed when they resume their full duties.

Given the scale of the pandemic response, institutions can anticipate a surge of access requests related to the government's handling of the response to COVID-19. Without outstanding leadership and proper planning, we can foresee that the new backlog generated during the current crisis will become another systemic burden, further impeding a system that is already facing major challenges. Simply put, this cannot become the "new normal".

Recommended Measures

I strongly recommend that the government's approach include a greater focus on proactive disclosure of data and decisions related to the pandemic, as a way to mitigate some of the burden on institutions in responding to the inevitable surge of access requests. Enhanced, timely proactive disclosure of reliable and accurate information related to COVID-19 will undoubtedly also counter disinformation and myths – a challenge which is particularly relevant to address in the context of COVID-19.
I note with approval your expression of support of journalistic access to information during a press

conference on April 23, and I also acknowledge the work that Treasury Board Secretariat officials have been doing in recent weeks to support the ATIP community. Collecting information centrally on the impact of workplace measures on the capacity of ATIP Offices is an important initial step. I call upon the government to act on this data and put in place mitigation measures wherever possible to deal with the operational impacts of the current alternative work arrangements on these units. The government must make funds available to the system in order to cope with both the delays attributable to the pandemic itself and the impending surge. It is important to take action now. Delays in appropriate resourcing will almost certainly result in backlogs from which it will take years to recover. Canadians expect and deserve a forward-looking and effective response.

Money alone, however, will not address the entirety of the challenge. We are in a moment in time when strong leadership can guide the testing and pursuit of modernization and innovation. One example of such an innovation could include considering identifying the processing of ATIP requests as a priority service even under exceptional working situations like the one we find ourselves in today. This would include equipping ATIP units with leaner processes, better infrastructure and new tools to support the work of managing the inventory of requests and complaints, both in the current operating environment and into the future. Bringing institutions fully into the digital world could create significant efficiencies, not to mention increase the productivity of employees operating under alternative work arrangements.

Conclusion

To reiterate, transparency in government is crucial to maintaining trust between citizens and their government. In order to safeguard openness and transparency, it is incumbent on the government to show leadership and develop a new vision and strategy for modernizing the access system; one that includes innovation, ensures adequately resourced and equipped ATIP units across all institutions, as well as increased proactive disclosure. Based on the concerns I have raised, I trust you will agree that a failure to take action on all these fronts could have serious consequences.

In closing, I encourage you to consider the opening lines of a recent Policy Options piece by Kathryn May:

> The COVID-19 pandemic has handed the public service a grand-scale opportunity to experiment with new ways of operating (…) What public servants learn in the next few months by working remotely and in crisis could jolt the bureaucracy into a reordering of practices and culture that reformers haven't been able to do in 25 years.

The current crisis has indeed brought new challenges, but I also believe it has created a window of opportunity for bringing about much-needed changes to the operating model of government and the culture that underlies it. I sincerely hope that the government will seize the moment and take on this task. I would be happy to discuss with you what change might look like for the access to information system and how we can bring it about.

Yours sincerely,
Caroline Maynard, Information Commissioner of Canada

Cc: Secretary of the Treasury Board, Treasury Board of Canada Secretariat

Source: https://www.oic-ci.gc.ca/en/resources/news-releases/critical-phase-access-information-system

AB IPC - Commissioner Comments on Alberta's Contact Tracing App

May 1, 2020

Information and Privacy Commissioner Jill Clayton has issued the following statement in response to the launch of Alberta Health's AB TraceTogether contact tracing application:

> I support efforts by Alberta Health to try to enhance contact-tracing processes to respond to the current pandemic.
>
> We have seen several technological ways to supplement contact tracing worldwide, some of which are more invasive than others. In my view, Alberta Health has chosen a less intrusive approach in deploying this app, while continuing to rely on the human expertise required for effective contact tracing. A technological approach alone is not a panacea.
>
> Ensuring this app is voluntary, collects minimal information, uses decentralized storage of de-identified Bluetooth contact logs, and allows individuals to control their use of the app are positive components. People diagnosed with COVID-19 also decide whether to disclose to public health officials the contact log stored on their phone.
>
> My office received a privacy impact assessment on the app earlier this week. An initial review has been undertaken and we have sent questions to Alberta Health to clarify certain aspects of the PIA. For example, I am seeking confirmation that the data collected through this app is to be used for contact tracing, and not for any other purpose.
>
> To complement the good work of public health officials in disclosing information about the pandemic, I appreciate that Alberta Health has committed to publishing a summary of its PIA. We have seen similar steps taken in other jurisdictions to promote accountability and transparency, and to build public trust.
>
> My office will monitor the implementation of this app. Any individual concerned about how their personal or health information is collected, used or disclosed may submit a complaint to my office.

Contact
Scott Sibald
Office of the Information and Privacy Commissioner of Alberta
(780) 422-9048

BC IPC – Collecting Personal Information at Food and Drink Establishments During COVID-19

On May 15, 2020 the Provincial Health Officer (PHO) issued an order that food and drink establishments must, if practicable, retain contact information for one member of every party of patrons for 30 days. The purpose of collection is for the local medical health officer to conduct contact tracing if someone who visited the establishment is diagnosed with COVID-19.

The purpose of this guide is to assist establishments subject to this order with compliance with this requirement in a manner that also protects patrons' privacy under BC's *Personal Information Protection Act* (PIPA). For more information about PIPA, see our guide here.

Collected personal information is valuable, and can be used for many purposes. Because of its value, this information is susceptible to being stolen or misused. Under s. 34 of PIPA, organizations must protect personal information by making reasonable security arrangements to prevent unauthorized access or similar risks. Below are some tips to help you securely collect, store, and dispose of personal information from patrons.

Explain to customers why you are collecting their contact information

At the time of collecting a patron's contact information, clearly explain what information you are collecting and why. Reference the PHO order (it would be helpful to have a copy on hand if a customer would like to see it).

Only collect the minimum amount of personal information necessary

The purpose of collection is to notify individuals if they have come into contact with someone diagnosed with COVID-19. Therefore, name, phone number or email, and date of visit from one member of the party should be sufficient. Do not collect a patron's physical address or other contact information such as where they work.

Do not use or disclose the collected information other than to provide to the PHO upon request

Do not use the collected information for other purposes, such as marketing or analytics. Further, do not provide the collected information to anyone other than the PHO upon request or as authorized in certain circumstances under BC's PIPA. Consult PIPA or contact us if you want help deciding whether PIPA authorizes your organization to make a disclosure.

If you share the collected information with the PHO, keep a record of the transaction

If the information is requested by the PHO, keep a record of what information you share. Under s. 23 of PIPA, individuals have a right to ask organizations who the organization has disclosed their personal information to. Keeping a record of what you have shared will ensure your establishment can meet this requirement.

Only keep collected information for 30 days

Routinely and securely destroy information collected after 30 days. A suggested practice would be to delete 31-day old information at the same time you add daily contact information. Any papers containing

personal information should be securely shredded rather than just placing them in a garbage can or recycling bin.

Properly secure the collected information

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.

Conclusion

If you have any questions about how to collect, use, disclose or protect personal information at your establishment, call us at (250) 387-5629 or email us at info@oipc.bc.ca. Other toll- free numbers are available here.

If collected personal information is stolen or lost (also known as a privacy breach), contact our office for assistance.

These guidelines are for information purposes only and do not constitute a decision or finding by the Office of the Information and Privacy Commissioner for British Columbia. These guidelines do not affect the powers, duties, or functions of the Information and Privacy Commissioner regarding any complaint, investigation, or other matter under FIPPA or PIPA.

Source: https://www.oipc.bc.ca/

ORIGINAL TEXT IN FRENCH

Commission
d'accès à l'information
du Québec

QB IPC - Pandemic, privacy and protection of personal information

Considerations regarding the use of certain technologies (e.g. contact tracing, activity trackers, use of location data)

Document updated on 4 May 2020

BACKGROUND

Québec, like the rest of Canada and other countries throughout the world, is in the midst of an unprecedented health crisis. Difficult choices have been made, and have disrupted our lives. Government authorities, under the powers granted to them by the *Public Health Act* when a health emergency is declared, have introduced a set of measures designed to protect public health.

These measures have had a major impact not only on our daily lives, but also on public health and on Québec's economy. A gradual resumption of certain activities is now being planned, for when the timing is right. Technological initiatives continue to emerge or are under development throughout the world, with the aim of supporting the resumption of economic activity while helping to limit the pandemic. They include location data sharing, contact tracing applications, electronic alerts for breach of isolation orders, infection risk assessment applications and so on. Some countries are already using these types of devices and applications, while others are considering it.

As it has been pointed out, however, these tools are not without consequences for fundamental rights such as the right to privacy, the risk of discrimination, and so on. The issues they raise must therefore be considered carefully before such tools are implemented in Québec, because our values and legal framework are different from those of some of the countries that have introduced these solutions.

Despite the scope of the current crisis and the need for Québec to state its position on this matter quickly, a prior assessment and weighing of the values at stake is necessary to make an informed decision and well thought-out choices. The current "pause" in Québec suitable time for this process of reflection.

As part of its role of promoting the protection of personal information, the Commission d'accès à l'information would like to play a role in this process by proposing certain considerations in connection with the issues of privacy and protection of personal information that are likely to arise if these devices and applications are used. This document will not analyze the tools themselves, nor will decide whether or not they are appropriate or compliant with current legislation. It will, however, summarize the elements that must be considered before deciding whether or not to implement or use them in Québec, and where possible, will suggest additional guidelines to support the process of reflection.

This document may be updated as needed, to reflect the rapidly changing context.

PROTECTION OF PERSONAL INFORMATION AND PRIVACY

First, it may be useful to begin by reviewing the notions of privacy and protection of personal information.

Respect for private life is a fundamental right under Québec's *Charter of Human Rights and Freedoms* (s. 5). It was also protected in 1948, in the United Nations' *Universal Declaration of Human Rights* (art. 12). As a right, it is important not only at the individual level (e.g. autonomy, freedom, privacy, dignity, protection of a private sphere required for psychological well-being, the right to control the use of one's image) but also at the collective level in a democratic society (e.g. avoiding surveillance of individuals, protecting a person's domicile from abusive search and seizure). The right to respect for private life can also be tied to respect for other rights, such as protection from discrimination, the right to autonomy, freedom of circulation or opinion, and a person's right to safeguard his or her honour, dignity and reputation, etc.

However, the right to privacy, like every other fundamental right, is not absolute. Among other things, it must be exercised with proper regard for democratic values, public order and the general well-being of the citizens of Québec. The law therefore provides that it can be infringed in specific circumstances and on certain conditions, to ensure a balance and equilibrium between the needs of society and the rights of individuals. Among other things, infringement of a fundamental right may be justified if it can be shown that the measure in question aims to achieve a legitimate, serious and important objective and that the infringement is proportional to that objective. In such cases, the Charter provides that the law can then set the scope and limits to the exercise the right.

The **protection of personal information** is one dimension of the right to respect for private life: the information dimension. Québec has two Acts that protect personal information, one applicable to the public sector and the other to the private sector. They prevail over all Québec's other legislation, reflecting the importance of these rights within our society.

Their objective is to set out the rules that allow individuals to control their personal information, and to place limits on what public bodies and private enterprises can do in situations where they must collect and use information as part of their activities. Protecting personal information does not mean simply ensuring that it remains confidential. It also involves compliance with a set of rules designed to limit invasions of individual privacy through the collection, use, communication and storage of personal information. Two of the basic principles underlying these laws are to reduce the collection and use of personal information to a strict minimum, and to obtain consent from the person concerned.

Although the legislation certainly needs to be brought up to date, the principles on which it is based can still serve as a landmark for the considerations proposed in this document.

When considering the impacts of technological solutions, a two-step assessment is required. The first step balances the objective of the solution (is it necessary?) and its impact on individual privacy (is the invasion proportional to the objective?). If, and only if, the conclusion from this first step is that the objective justifies the solution and that the ensuing invasion of privacy is proportional to the objective, then the second step, namely to ensure that the terms and conditions of the solution are consistent with the principles and best practices associated with the protection of personal information, can be taken.

1. Is the invasion of privacy justified and proportional?

Valid objective (is it necessary?)

The first consideration addresses the objective of the proposed technological solution. This objective is critical in assessing whether or not it is proportional to the proposed action

The objective should be sufficiently important to justify the limitation of a right protected by the Charter. It must be valid and relevant to a real, urgent social concern.

The objective of the technology itself must therefore be questioned. Obviously, the aim of all these technologies is to eradicate COVID-19 and limit the spread of the virus. However, it is important to clarify this by answering the following questions: How is the application or device likely to do this? What, specifically, does it aim to do with respect to the pandemic? For example, will it help public health authorities to carry out epidemiological surveys, trace contacts or obtain a more general profile of the disease's prevalence within the population? Or is its aim to ensure compliance with self-isolation measures by carriers of the virus? Or to identify people who may have been in contact with infected people, and if so, the reason why (tracing, recommendation of health measures, profiling, etc.)? Or to give advice to people based on their "level of risk", symptoms or potential contact with infected people? And so on.

A further question to ask is how consistent this objective is with the current public health strategy. Since the Government has declared a health emergency, the validity of any measure or solution that would hinder the actions of the public health authorities would be questionable, especially if it also infringed a fundamental right. In addition, there is the question of who proposed and developed the solution and established its objective. Was it a public body? The public health authorities? A private enterprise? Or another group? Are there any other, secondary objectives? If so, are they lawful?

Proportionality of the proposed measure

Furthermore, the designers of these solutions or the government authorities that adopt or promote them must demonstrate that the solutions are reasonable and can be justified, i.e. that the invasion of privacy they require is proportional to the objective or situation being addressed. It is a matter of finding a balance between the means chosen to address the problem and respect for individual rights.

Proportionality is assessed using a three-step process.

1) First, there must be a **rational connection** between the pursued objective (including- secondary objectives if any) and the proposed solution, i.e. the solution must provide an effective way of achieving the objective(s).

In practical terms, this means asking the following questions: Is it reasonable to conclude that the proposed solution will in fact achieve the objective? How, concretely, will the proposed application or technology achieve this objective? How will the collection, use or communication of personal information help to achieve this? How effective is the device (or at least, how effective is it expected to be, based on real, scientific data and a rational, objective assessment)? Has the device been effective in fighting COVID-19 elsewhere? If so, within what parameters? Was it combined with another measure, such as a testing or another policy?

2) Secondly, because privacy is a fundamental right, **any infringement of an individual's right to privacy must be minimal** and must only take place if **there is no other effective solution** that is less intrusive.

This involves questioning the scope of the proposed solution and asking whether other, less intrusive means would provide an effective solution or help achieve the objective. For example: Could the objective be achieved in another way, without invading individual privacy, without collecting or using personal information? What could be done to minimize any invasion of privacy? Should the use of this type of device or application be regulated specifically to the current context, because of the major privacy issues it raises? If so, how?

The nature of the information that would be collected and used will affect the assessment. The use of sensitive information, such as health-related information (e.g. a positive result to a Coronavirus diagnostic test, or symptoms) or information on a person's location, is more intrusive than the use of aggregate or other types of information.

Where the information is stored (centralized or decentralized) is also relevant to the assessment, as well as the circulation and accessibility to the information. For how long will the information be stored?

The secondary objectives or uses associated with the proposed solution must also be considered. Are they essential? Do they represent an additional invasion of privacy? If so, can these additional objectives or uses of personal information be removed?

What measures are provided to put a stop to the invasion of privacy at the end of the pandemic? Will the application be withdrawn from the market? Will the data be destroyed?

3) Last, the concrete **benefits** of the proposed solution **must outweigh the damaging consequences** for individuals.

This is basically a balance between the real benefits and disadvantages of applying the proposed technological solution. What are they? Do the benefits for the collective good outweigh the infringement of individual rights?

All the potential consequences likely to occur should be considered. For example, is the proposed measure likely to infringe other rights, such as the right to dignity or the right to safeguard one's reputation? Is it likely to cause discrimination or to stigmatize certain individuals? Might it have a positive or negative impact on measures adopted by the authorities to fight the pandemic (e.g. by creating a false sense of safety among the general public, or conversely, needlessly worrying people, contradicting public health directives, undermining public trust in the authorities, contradicting certain voluntary measures, etc.)? Is the solution consistent with the current testing strategy? Is it designed to facilitate epidemiological surveys? Will it add tasks or increase the current workload of medical staff, including public health officials, who are already overworked? Do the issues change, depending on whether the information is collected and used by the public authorities or by a private enterprise? If the application is available for use on a voluntary basis, what are the advantages and disadvantages of this approach?

If the conclusion from the first part of the assessment is that the proposed solution is justified and necessary in the current context, and that the ensuing invasion of privacy is proportional and allows for a balance between the needs of society and the rights of individuals, then the next step is to assess the conditions of application, to ensure that they are consistent with the principles and best practices for the protection of personal information in Québec.

2. Compliance with principles and best practices for the protection of personal information

As mentioned earlier, protecting personal information does not simply mean maintaining the confidentiality and security of information concerning individuals. On the contrary, it involves the application of a set of principles and good practices designed to structure and minimize the collection, use, communication and storage of personal information.

It is important to refer to the appropriate legislation, depending on who will be collecting personal information through the proposed technological solution: a public body, a private enterprise or both. Public bodies must comply with the provisions of the *Act respecting Access to documents held by public bodies and the Protection of personal information,* and private companies must comply with the *Act respecting the protection of personal information in the private sector*.

The Commission would like to draw attention to the following non-exhaustive list of principles and good practices:

1. Prevention

Before implementing a technological device or application that involves the collection, use or communication of personal information, it is important to ensure compliance with the legislation and generally accepted principles governing the protection of personal information and privacy. This process, known as a Privacy Impact Assessment or PIA, is mandatory in many countries and in some Canadian provinces. It is used to identify issues from the early stages onwards, and ensures that solutions can be adjusted so that they are compliant and have minimal impacts for privacy.

A PIA examines all the factors that affect the protection of personal information and respect for privacy, either positively or negatively. The assessment involves an analysis that:

- presents the project (objective, internal procedures, etc.);
- identifies the personal information targeted by the project, and how it circulates within the information system (information life cycle);
- describes the project's repercussions for the personal information;
- links the project to the legal principles governing the protection of personal information (purpose of the file, necessity, collection, information, use, consent, communication, destruction, safety, access, etc.);
- identifies risks and consequences for the protection of personal information;
- identifies and implements ways to minimize invasions of privacy and to protect personal information.

A PIA is an iterative process that monitors the development of the application and is revisited each time changes or additions are made.

For additional details: https://www.cai.gouv.qc.ca/documents/CAI_FI_efvp.pdf (in French only). A preliminary guide (in French only) will shortly be available on the Commission's website: https://www.cai.gouv.qc.ca/.

Another good preventive practice is to design intended solutions or applications by integrating the privacy and personal information protection principles from the beginning (privacy by design) or by default (privacy by default). Privacy by design, as its name suggests, consists in designing a solution that maximizes respect for privacy at every stage of development, from needs analysis to design, during implementation, and during audits and maintenance, including decommissioning, whether voluntarily by the user or at the end of the solution's useful life. These measures must be applied to every stage of the information life cycle (from collection to destruction) and be transparent (users must be told about them). As for privacy by default, it involves ensuring that all the application's default settings provide maximum data protection (i.e. without the user having to choose the settings that offer the highest level of protection).

Some technological developments may also be used to improve the protection of personal information. These are known as privacy enhancing technologies or PETs. For example, they can help limit the collection of personal information (e.g. data anonymization), enhance confidentiality or security, limit access to certain people or improve a person's control over his or her own personal information (e.g. pseudonymization, differential privacy, cryptography, homomorphic encryption, cryptographic hashing, selective disclosure techniques, data tagging, etc.). For examples of these different techniques, see: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/.

2. Limit collection to necessary personal information only

One of the most important legislative principles for the protection of personal information is that collection must be limited solely to personal information that is necessary. This rule cannot be circumvented by consent: in other words, a private enterprise or public body cannot collect unnecessary personal information even if the person concerned has given consent.

It must therefore be possible to explain and prove necessity when collecting personal information. This involves considering how each piece of information will help to achieve the proposed solution's objective. Here too, proportionality is important in determining necessity. In other words, the nature of the information to be collected must be established, and every possible measure must be taken to minimize the impact on the person's privacy.

For example, if the information in question is sensitive, the measures taken to minimize the invasion of privacy must be more significant, and all other means of achieving the objective must be used first. However, if the objective can be achieved by collecting anonymized, depersonalized, pseudonymous or aggregate data, then this is the path that must be taken. If less sensitive information is available, it should be collected instead, or reasons should be given to show why it is less effective. For example, some contact- tracing applications use geolocation data, while others use proximity information (Bluetooth) only, which does not involve surveillance or monitoring of movement.

The following clarifications will help you determine the nature of information that is collected.

- **Personal information:** Information is personal if it concerns and can be used to identify a natural person. The assessment of the criterion "Can be used to identify" refers to the ability to distinguish the person from someone else and to maintain a connection between the person and the information concerning him or her.

- **Sensitive personal information**: The "sensitive" nature of information is determined by its intimate nature or by the harmful consequences that would arise from its disclosure. For example, health-related, taxation, financial or genetic information, or information concerning a person's sexuality, would be classified as "sensitive", as would information associated with the risk of discrimination (race, ethnic origin, religion, handicap) or identity theft (contact information, unique identifiers such as a person's health insurance number, driver's licence or social insurance number). Biometric data, which is unique, permanent and intimate, also falls

into this category. See section 6.1 of this document for additional information on the nature of biometric data and the specific rules applicable to it.

- **Anonymous information**: Information is anonymous if it cannot be used to identify an individual and if anonymization is irreversible even with the use of other information or re-identification techniques. The removal of direct identifiers (name, address, health insurance number, driver's licence number, IP address, etc.) is insufficient to anonymize information. Anonymization must be irreversible. Before concluding that information has been anonymized, the risk of re-identification must be carefully analyzed and proved.

  It can be challenging to anonymize certain data because of their nature. For example, it may be fairly easy to deduce a person's home or work address, and hence his or her identity, from geolocation data.

- **Depersonalized information:** This is personal information from which direct identifiers have been removed, or from which it is impossible to identify an individual without using other information, a match key or re-identification techniques. There are a number of depersonalization techniques, including pseudonymization (replacing direct identifiers by digital or other pseudonyms), encryption, and so on. However, it is important to remember that this type of information is still personal information and is therefore subject to all the legislative rules governing the protection of personal information.

- **Inferred personal information:** Some projects may require the use of artificial intelligence systems whose algorithms can infer new information from collected information: for example, your risk level of being infected by the virus or of having been in contact with an infected person. When this inferred information concerns and can be used to identify a natural person, it becomes personal information and is subject to the legislative rules governing personal information. This means that a private enterprise or public body holding inferred information must comply with the requirements for the protection of personal information, including the need to limit its use and communication as required by law, ensure that it remains confidential, and destroy it. The individual concerned is also entitled to access the information and rectify it where necessary.

3. Transparency

The legislation governing the protection of personal information provides that individuals must be informed of certain elements when personal information is collected. The sameapplies when consent must be obtained in order to use or communicate personal information to a third party. Lastly, public bodies and private enterprises must show that they are acting responsibly by being transparent about the steps they have taken to protect personal information.

Before the application is used, transparency can be shown by indicating, in complete, simple, easy-to-understand terms:

- which information is being collected: list all the information, including any that will be inferred by an algorithm. Special attention should be paid to the descriptors used; as noted earlier, depersonalized information is not anonymized.

- the purposes for which the information will be used: describe all the proposed uses and specify which information will be used in each case.

- if the information will be processed automatically, via an algorithm, explain the most important factors and parameters that will be used for decision-making, prediction or profiling. What is the underlying logic of the processing mechanism? Which personal information will be used in this way?

- who will have access to which information: be precise and state why it is necessary for these categories of people or these other bodies or enterprises to have access to the information.

- where the information will be stored.

- what have been the measures taken to ensure that the information remains confidential and secure throughout its life cycle.

- how individuals can exercise their right of access to and rectification of information that concerns them: appoint someone to be responsible for this and provide contact details. The person can also answer questions and address concerns raised by individuals regarding the way your organization protects their personal information.

4. Limit the use and disclosure of personal information

The legislation applicable to the public and private sectors provides that information collected can be used only for the purposes for which it was collected, or for purposes that are consistent with them. Given the sensitive nature of the information required by many of the applications currently in use or described by the media as being under development, combined with the high level of intrusiveness and the likelihood that these applications will infringe other fundamental rights, the use of personal information should be limited to the purposes stated during the collection process.

Similarly, personal information should also be depersonalized or anonymized wherever possible.

The legislation also provides that information cannot be communicated to third parties without the consent of the person concerned or without legal authorization. Additional requirements apply to the communication of personal information outside Québec, including the obligation to ensure that the information will be given a level of protection equivalent to that required by law in Québec.

5. Consent

Some of the principles arising from our democratic values and our fundamental rights and freedoms serve as clear arguments to suggest that technology applications should be used only on a voluntary basis as solutions to the current situation. For other projects, including those that require the communication of personal information, consent is usually required, unless the law states otherwise.

To be valid, consent must be:

- **Free**: expressed without conditions, constraints, threats or promises. A person may therefore withdraw his or her consent at any time.
- **Informed**: given with awareness as to its scope, with full knowledge of the facts, hence the importance of transparency.
- **Specific**: authorizing the use or communication of specific personal information, to specific people, for specific purposes and at a specific time. If there are plans to use or communicate the information for several different purposes, separate consent must be obtained in each case.
- **Limited in time**: valid for the time needed to achieve the objectives for which the consent was requested.
- **Manifest**: expressed clearly and unequivocally. If it relates to sensitive information, it must be express, i.e. given in writing.

For some of the applications described in the media, effectiveness appears to depend on the extent to which the public adopts them, and it has been a suggestion that incentives, or even social pressure, would be desirable. However, this would cast doubt on the free and informed aspects of consent and would impact the measure's proportionality to the ensuing infringement of rights.

The possibility that an application may become a *de facto* condition for entry into a building, store or workplace must also be considered. This includes the risk that a person using an application may be forced to disclose personal information: level of infection risk, declared symptoms, results of virus testing, recommendations by the application, etc. Not only does this cast doubt on consent, but the risk of service denials and infringements of other rights must also be considered when deciding whether or not to use these applications.

6. Assess the impacts of using artificial intelligence systems

If the use of an artificial intelligence system (or automated information system) involving personal information is being considered, the Commission feels that a number of principles should be implemented, even though they are not currently part of Québec's personal information legislation, which is outdated in this respect.

Some of these principles have been covered by preceding sections of this document. Others, however, including those relating to governance and liability, must also be considered. For example, it may be appropriate to assess the algorithmic impacts of an automated system. For an example of this, see: https://www.canada.ca/en/government/system/digital-government/modern-emerging- technologies/responsible-use-ai/algorithmic-impact-assessment.html

For further details regarding the principles and features of the protection of personal information as they apply to the use of artificial intelligence, the Commission's consultation document (in French only) can be found here.

Although these documents have not yet been finalized, they may nevertheless be useful in the current exceptional circumstances.

6.1 Comply with the specific rules applicable to biometric information and geolocation data

Geolocation

Section 43 of the *Act to establish a legal framework for information technology* (CQLR, c. C-1.1; hereinafter the ALFIT) limits the use of a device that allows the person's whereabouts to be known, such as a device that provides geolocation data: [...] "*Unless otherwise expressly provided by law for health protection or public security reasons, a person may not be required to be connected to a device that allows the person's whereabouts to be known.*"

Biometric data

A public body, private enterprise or any other organization considering the use of biometric measures or characteristics to achieve the objective of preventing COVID-19 must take the specific nature of biometric data into account.

The term "biometrics" refers to a technique that uses one or more pre-recorded unique physical or behavioural characteristics to verify the identity of a person who wishes to perform an action.

There are two main categories of biometrics:

- **Morphological biometrics**, which identifies specific physical traits. This category includes fingerprint, hand shape, retina and iris recognition.

- **Behavioural biometrics**, which analyses aspects of a person's behaviour such as handwritten signature, voice print, gait, keyboard strokes and so on.

This information, whether in raw (image or print) or digital (algorithm-derived code) format, constitutes sensitive personal information to which additional rules apply. These rules are set out in sections 43 to 45 of the *ALFIT*.

The Commission has published documents that provide information for biometrics-based initiatives. They include an information sheet entitled *La biométrie au Québec* (available in French only) and a document entitled *Biometrics in Québec: Application Principles – Making an Informed Choice*. Other information tools are currently under preparation.

7. Destroy personal information

Personal information must be destroyed when the purposes for which it was collected have been accomplished. Health-related and geolocation data are highly sensitive, and these are the types of data generally required for the projects described in the media or applied in other countries. It is vital that they be destroyed because of the infringement of fundamental rights and freedoms that they represent.

8. Allow the person concerned to exercise their rights

The law provides that individuals have the right to access and rectify personal information that concerns them. How can individuals exercise this right with respect to the information collected by some of the proposed solutions, and with respect to information inferred by algorithms?

9. Structuring, reporting, independent external controls and reassessment

Any solution that involves collecting, using or communicating personal information should also be subject to governance measures and be supervised by an independent control authority.

The organizations responsible for these devices and applications should issue regular public reports on the effectiveness of:

- the measure itself, in achieving the health-related objective, and the relevance of maintaining it;

- the measures introduced to protect personal information and minimize invasions of privacy.

CONCLUSION

This document does not attempt to list all the issues and elements to be weighed when considering the relevance, legality and effectiveness of technology-based tools and devices; it simply sets out the elements that the Commission wishes to submit for consideration. The Commission reaffirms the importance of engaging in this process of reflection before deciding to proceed with the use of these tools, which should not be considered or implemented without a guarantee that individual privacy of citizens will be upheld and that every possible step has been taken to comply with the current legislation in Québec.

To continue the thinking process…

The following resources, while by no means exhaustive, may contribute to the present considerations provide additional food for thought:

- Commission de l'éthique en science et en technologie :
  - ✓ Framework for reflection on the ethical issues of the COVID-19 pandemic (in French)
  - ✓ Use of mobile artificial intelligence applications for COVID-19 surveillance in Québec:
    - General information (in French)
    - Special committee interim report (in French)
- Traçage des données mobiles dans la lutte contre le Covid-19 : Analyse des potentiels et des limites, by Mounir Mahjoubi (in French). See also this summary (also in French).
- European Commission Recommendation on a common union toolbox for the use of mobile technology and data
- Letter of April 14, 2020 from the European Data Protection Board concerning a draft guide to the use of apps during the COVID-19 pandemic
- CDPDJ website (content available in French only)
- Letter from Dutch scientists and specialists from different fields
- Analysis of the risks of anonymous tracing for non-specialists (version of April 21, 2020) (in French only)

Source: https://www.cai.gouv.qc.ca/documents/CAI_Document_reflexion_ANG.pdf

YK IPC – Yukon Information and Privacy Commissioner issues advisory on COVID-19 related scams

Diane McLeod-McKay offers suggestions for individuals and organizations

WHITEHORSE – The Information and Privacy Commissioner (IPC) for Yukon has developed an advisory to help individuals avoid falling victim to scams that attempt to capitalize on fears and concerns related to the COVID-19 pandemic. The advisory also includes best practices for organizations that work with and store personal information.

As IPC, part of Diane McLeod-McKay's role is to promote compliance with privacy laws and inform the public about their privacy rights. Throughout the COVID-19 pandemic, her office has been working to increase awareness amongst public bodies and custodians and their employees, as well as the general public, about the importance of privacy and access to information, as well as risks and concerns that are emerging as a result of the pandemic.

"The response to COVID-19 has included a number of unique measures being taken by governments and businesses around the world," said McLeod-McKay. "We have also seen the rise of a new kind of cybercrime, which tries to take advantage of evolving concerns and priorities that citizens may have over COVID-19. This creates new and perhaps unexpected vulnerabilities that can put personal information and finances at risk."

The advisory being issued today deals with campaigns run by cybercriminals that are aimed at collecting personal and financial information in order to commit fraud or theft. The campaigns use social media, text messages, emails and robo-calls to impersonate government agencies, businesses or non-government organizations. They may claim that you have been in contact with someone who has COVID-19, that they have information about your government benefit, that they are collecting donations for charities fighting the pandemic, or that they are selling personal protective equipment, such as masks.

"There have been a number of media reports about these scams and so our office has put together an advisory to help Yukon organizations, businesses and citizens understand this threat to privacy, learn how to detect fraudulent activity and avoid becoming its victim," said McLeod-McKay.

The advisory is located on the IPC website here. If they have questions or concerns, citizens may also contact the IPC office at 867-667-8468 or info@ombudsman.yk.ca.

The Ombudsman, Information and Privacy Commissioner, and Public Interest Disclosure Commissioner is an independent officer of the Yukon Legislative Assembly. For more information, please go to www.ombudsman.yk.ca.

Contact:

Elaine Schiman, Communications Manager

elaine.schiman@ombudsman.yk.ca | 867-332-4555 | 867-334-2975

www.ombudsman.yk.ca | Follow us on Twitter

EDPD - Statement on the processing of personal data in the context of the COVID-19 outbreak.

Adopted on 19 March 2020

The European Data Protection Board has adopted the following statement:
Governments, public and private organisations throughout Europe are taking measures to contain and mitigate COVID-19. This can involve the processing of different types of personal data.

Data protection rules (such as the GDPR) do not hinder measures taken in the fight against the coronavirus pandemic. The fight against communicable diseases is a valuable goal shared by all nations and therefore, should be supported in the best possible way. It is in the interest of humanity to curb the spread of diseases and to use modern techniques in the fight against scourges affecting great parts of the world. Even so, the EDPB would like to underline that, even in these exceptional times, the data controller and processor must ensure the protection of the personal data of the data subjects. Therefore, a number of considerations should be taken into account to guarantee the lawful processing of personal data and in all cases it should be recalled that any measure taken in this context must respect the general principles of law and must not be irreversible. Emergency is a legal condition which may legitimise restrictions of freedoms provided these restrictions are proportionate and limited to the emergency period.

1. Lawfulness of processing

The **GDPR is a broad piece of legislation and provides for rules that also apply to the processing of personal data in a context such as the one relating to COVID-19**. **The GDPR allows competent public health authorities and employers to process personal data in the context of an epidemic, in accordance with national law and within the conditions set therein**. For example, when processing is necessary for reasons of substantial public interest in the area of public health. Under those circumstances, there is no need to rely on consent of individuals.

1.1 With regard to the processing of personal data, including special categories of data by competent public authorities (e.g. public health authorities), the EDPB considers that articles 6 and 9 GDPR enable the processing of personal data, in particular when it falls under the legal mandate of the public authority provided by national legislation and the conditions enshrined in the GDPR.

1.2 In the employment context, the processing of personal data may be necessary for compliance with a legal obligation to which the employer is subject such as obligations relating to health and safety at the workplace, or to the public interest, such as the control of diseases and other threats to health.

The GDPR also foresees derogations to the prohibition of processing of certain special categories of personal data, such as health data, where it is necessary for reasons of substantial public interest in the area of public health (Art. 9.2.i), on the basis of Union or national law, or where there is the need to protect the vital interests of the data subject (Art.9.2.c), as recital 46 explicitly refers to the control of an epidemic.

1.3 With regard to the processing of telecom data, **such as location data**, national laws implementing the ePrivacy Directive must also be respected. In principle, location data can only be used by the operator when made anonymous or with the consent of individuals. However, Art. 15 of **the ePrivacy Directive enables Member States to introduce legislative measures to safeguard public security.** Such exceptional legislation is only possible **if it** constitutes a **necessary, appropriate and proportionate measure within a democratic society**. These measures must be in accordance with the Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Moreover, it **is subject to the judicial control of the European Court of Justice and the European Court of Human Rights.** In case of an emergency situation, it should also be strictly limited to the duration of the emergency at hand.

2. Core principles relating to the processing of personal data

Personal data that is necessary to attain the objectives pursued should be processed for specified and explicit purposes.

In addition, data subjects should receive transparent information on the processing activities that are being carried out and their main features, including the retention period for collected data and the purposes of the processing. The information provided should be easily accessible and provided in clear and plain language.

It is important to adopt adequate security measures and confidentiality policies ensuring that personal data are not disclosed to unauthorised parties. Measures implemented to manage the current emergency and the underlying decision-making process should be appropriately documented.

3. Use of mobile location data

- **Can Member State governments use personal data related to individuals' mobile phones in their efforts to monitor, contain or mitigate the spread of COVID-19?**

In some Member States, governments envisage using mobile location data as a possible way to monitor, contain or mitigate the spread of COVID-19. This would imply, for instance, the possibility to geolocate individuals or to send public health messages to individuals in a specific area by phone or text message. **Public authorities should first seek to process location data in an anonymous way (ie. processing data aggregated in a way that individuals cannot be re-identified), which could enable generating reports on the concentration of mobile devices at a certain location ("cartography").**

Personal data protection rules do not apply to data which has been appropriately anonymised.

When it is not possible to only process anonymous data, the ePrivacy Directive **enables Member States to introduce legislative measures to safeguard public security (**Art. 15)**.**

If measures allowing for the processing of non-anonymised location data are introduced, a Member State is obliged to put in place **adequate safeguards**, such as providing individuals of electronic communication services the **right to a judicial remedy**.

The proportionality principle also applies. The least intrusive solutions should always be preferred,

taking into account the specific purpose to be achieved. Invasive measures, such as the "tracking" of individuals (i.e. processing of historical non-anonymised location data) could be considered proportional under exceptional circumstances and depending on the concrete modalities of the processing. However, it should be subject to enhanced scrutiny and safeguards to ensure the respect of data protection principles (proportionality of the measure in terms of duration and scope, limited data retention and purpose limitation).

4. Employment

- **Can an employer require visitors or employees to provide specific health information in the context of COVID-19?**

The application of the principle of proportionality and data minimisation is particularly relevant here. The employer should only require health information to the extent that national law allows it.

- **Is an employer allowed to perform medical check-ups on employees?**

The answer relies on national laws relating to employment or health and safety. Employers should only access and process health data if their own legal obligations requires it.

- **Can an employer disclose that an employee is infected with COVID-19 to his colleagues or to externals?**

Employers should inform staff about COVID-19 cases and take protective measures, but should not communicate more information than necessary. In cases where it is necessary to reveal the name of the employee(s) who contracted the virus (e.g. in a preventive context) and the national law allows it, the concerned employees shall be informed in advance and their dignity and integrity shall be protected.

- **What information processed in the context of COVID-19 can be obtained by the employers?**

Employers may obtain personal information to fulfil their duties and to organise the work in line with national legislation.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Source:
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

UK ICO – Workplace testing – guidance for employers

Note: Although similar, there are variations in approach taken by the UK Government and the three devolved administrations. Employers should ensure that they comply with the relevant local requirements for each of their premises, including any local differences that may be introduced as the UK moves out of lockdown.

When they return to work, I want to carry out tests to check whether my staff have symptoms of COVID-19 or the virus itself. Do I need to consider data protection law?

Yes. You will be processing information that relates to an identified or identifiable individual, so, you need to comply with the GDPR and the Data Protection Act 2018. That means handling it lawfully, fairly and transparently.

Personal data that relates to health is more sensitive and is classed as 'special category data' so it must be even more carefully protected.

Data protection law does not prevent you from taking the necessary steps to keep your staff and the public safe and supported during the present public health emergency. But it does require you to be responsible with people's personal data and ensure it is handled with care.

The ICO has published a document setting out our regulatory approach during the coronavirus pandemic.

Which lawful basis can I use for testing employees?

As long as there is a good reason for doing so, you should be able to process health data about COVID-19. For public authorities carrying out their function, public task is likely to be applicable. For other public or private employers, legitimate interests is likely to be appropriate, but you should make your own assessment for your organisation.

Due to its sensitivity, health data has the protected status of 'special category data' under data protection law. As such, employers must also identify an Article 9 condition for their processing.

The relevant condition will be the employment condition in Article 9(2)(b), along with Schedule 1 condition 1 of the DPA 2018. This applies due to their employer health and safety obligations. This condition will cover most of what employers need to do, as long as they are not collecting or sharing irrelevant or unnecessary data.

How can I show that our approach to testing is compliant with data protection law?

To show that your processing of test data is compliant, you will need to use the accountability principle. It makes you responsible for complying with the GDPR and says that you must be able to demonstrate your compliance such as additional recording keeping requirements when processing sensitive data. One way of demonstrating accountability is through a data protection impact assessment (DPIA).

If your organisation is going to undertake testing and process health information, then you should conduct a DPIA focussing on the new areas of risk.
This DPIA should set out:

- the activity being proposed;
- the data protection risks;
- whether the proposed activity is necessary and proportionate;
- the mitigating actions that can be put in place to counter the risks; and
- a plan or confirmation that mitigation has been effective.

DPIAs are designed to be flexible, as appropriate to the context. We have a template organisations can use to help them focus on the minimum requirements. One important point is that the initial DPIA should be regularly reviewed and updated. This is especially important in a fast-moving crisis situation, as new risks and benefits emerge.

How do I ensure that I don't collect too much data?

For special category data, such as health data, it is particularly important to only collect and retain the minimum amount of information you need to fulfil your purpose.

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.

In the context of test results, you need to ensure you do not collect unnecessary or excessive information from people. For example, you will probably only require information about the result of a test, rather than additional details about underlying conditions. Consider which testing options are available, to ensure that you are only collecting results that are necessary and proportionate. As an employer, you should be able to demonstrate the reason for testing individuals or obtaining the results from tests.

Data protection law also requires that any personal data you hold is accurate. As such, you should record the date of any test results, because the health status of individuals may change over time and the test result may no longer be valid.

Can I keep lists of employees who either have symptoms or have been tested as positive?

Yes. If you need to collect specific health data about employees, you need to ensure the use of the data is actually necessary and relevant for your stated purpose. You should also ensure that the data processing is secure, and consider any duty of confidentiality owed to employees.

As an employer, you must also ensure that such lists do not result in any unfair or harmful treatment of employees. For example, this could be due to inaccurate information being recorded, or a failure to acknowledge an individual's health status changing over time. It would also not be fair to use, or retain, information you have collected about the number of staff who have reported symptoms of COVID-19 for purposes they would not reasonably expect.

What do I need to tell my staff?

Transparency is very important. As an employer, you should be clear, open and honest with employees from the start about how and why you wish to use their personal data. This is crucial when processing health information. If you are testing employees for COVID-19 or checking for symptoms, you should be clear about what decisions you will make with that information. Where possible, you should have clear and accessible privacy information in place for employees, before any health data processing begins. We recognise, however, that in this exceptional time it may not be possible to provide detailed information.

Before carrying out any tests, you should at least let your staff know what personal data is required, what it will be used for, and who you will share it with. You should also let them know how long you intend to keep the data for. It would also be helpful for you to provide employees with the opportunity to discuss the collection of such data if they have any concerns.

Can I share the fact that someone has tested positive with other employees? What do I need to consider if I am planning to disclose this information to third parties?

You should keep staff informed about potential or confirmed COVID-19 cases amongst their colleagues. However, you should avoid naming individuals if possible, and you should not provide more information than is necessary.

As an employer, it's your duty to ensure the health and safety of all your employees. Data protection doesn't prevent you doing this, and should not be viewed as a barrier to sharing data with authorities for public health purposes, or the police where necessary and proportionate. There are many routes available to share data, using some of the conditions and exemptions in the DPA 2018. You also need to take into account the risks to the wider public which may be caused by failing to share information, and take a proportionate and sensible approach.

How do I ensure that staff are able to exercise their information rights as part of this process?

In order for individuals to exercise their rights, they need to understand what personal data you hold, and what you are using it for. As such, transparency is crucial and you should let your staff know how you will use their data in a way that is accessible and easy to understand.

You should also ensure that staff are able to exercise their information rights. To make this easier you may wish to put processes or systems in place that will help your staff exercise their rights during the COVID-19 crisis.

For example, in relation to the right of access (also known as Subject Access), you might consider setting up secure portals or self-service systems that allow staff to manage and update their personal data where appropriate. This may also allow individuals to exercise other rights such as the right to rectification or erasure of their data. Where this is not possible, you should make sure that basic policies and procedures are in place to allow employee data to be readily available when needed.

Some staff already have the results of tests that they have arranged for themselves. If they disclose these results to me, what are the data protection considerations?

For any test results that are voluntarily disclosed to you, as an employer you should have due regard to the security of that data, and consider any duty of confidentiality owed to those individuals who have provided test results.

Your focus should be on making sure your use of the data is necessary and relevant, and you do not collect or share irrelevant or excessive data to authorities if this is not required.

Would it be appropriate to use temperature checks or thermal cameras on site, as part of testing or ongoing monitoring of staff?

When considering the use of more intrusive technologies, especially for capturing health information, you need to give specific thought to the purpose and context of its use and be able to make the case for using it. Any monitoring of employees needs to be necessary and proportionate, and in keeping with their reasonable expectations. Again, transparency is key.

You should also think about whether you can achieve the same results through other, less privacy intrusive, means. If so, then the monitoring may not be considered proportionate.

The Surveillance Camera Commissioner (SCC) and the Information Commissioner's Office (ICO) have worked together to update the SCC DPIA template, which is specific to surveillance systems. This will assist your thinking before considering the use of thermal cameras or other surveillance.

Source: https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/data-protection-and-coronavirus/workplace-testing-guidance-for-employers/

AB IPC – Pandemic FAQ: Customer Lists

June 2020

The Office of the Information and Privacy Commissioner (OICP) has received several questions from organizations and individuals about keeping a customer list or contact log during the COVID-19 pandemic, particularly in retail locations and at restaurants.

The following are some considerations to ensure that organizations comply with Alberta's *Personal Information Protection Act* (PIPA) when making and keeping lists of customers and their contact information.

Consent and Notice

Organizations must generally obtain an individual's consent to collect that individual's personal information (sections 7 and 8). An organization must also notify an individual about why the personal information is being collected – before or at the time of the collection (section 13). Both consent and notification can be done in writing or orally.

In addition to notifying customers about the purpose for collecting personal information, an organization must also be prepared to provide a customer with the name or position of a person who is able to answer questions on behalf of the organization about the collection of personal information.

Businesses can make customers aware of their personal information collection practices and the purpose for the collection through websites, social media pages, or posters at entrances or other highly visible locations. Another option may be to provide a staff member with a script to describe the personal information collection practice and the reason for the collection at the time of the collection. Other options may be available to a business.

If an organization decides to collect customer information during the COVID-19 pandemic, they are advised to understand their authority to collect personal information and be able to cite their authority under PIPA.

Further, section 7(2) of PIPA says that an organization shall not, as a condition of supplying a product or service, require an individual to consent to the collection of personal information beyond what is necessary to provide the product or service. Organizations should determine whether it is necessary for a customer to provide contact details in order to shop in a store or eat at a restaurant. If it is not necessary, then the organization cannot require the individual to provide the information.

There are circumstances in which consent may not be required, such as if a public health order requires the collection of personal information. Organizations are advised to keep up to date on public health orders, which may require that personal information of customers be collected by some businesses or in certain circumstances. In such a scenario, organizations should also be prepared to notify customers why they are required to collect personal information.

Reasonable Purpose and Extent

PIPA requires that organizations collect personal information only for purposes that are reasonable and only to the extent reasonable for meeting those purposes (section 11).

For example, an organization may decide as a health and safety measure for employees and customers to collect personal information in order to assist contact-tracing efforts during the COVID-19 pandemic. The organization can only collect personal information that would be reasonably required to meet the purpose. For example, it might be reasonable to collect an individual's name,

cellphone number or email address, and the date and time the customer attended the store or restaurant. It is unlikely that it would be reasonable to collect other types of personal information that are not required for the purposes of contact tracing.

Secondary Use Restrictions

Organizations cannot use information collected for one purpose for another, different purpose, unless the individual consents to the new use, or the new use is otherwise authorized by PIPA (section 17). This means, for example, that an organization cannot use personal information collected to contact a customer in the event of exposure to COVID-19 to add them to a mailing or subscription list. The organization would have to obtain consent for this additional purpose.

Another example may be a restaurant that uses an online platform for booking reservations. If the restaurant intends to use the information collected for booking reservations to assist with contact tracing in certain circumstances, they may have to get consent and notify customers before or at the time of the collection that the information may also be used to assist contact tracing efforts during the COVID-19 pandemic. The business may also need to get consent for this new use of information prior to disclosing the customer's contact information.

Retention

If an organization collects a list of customers and associated personal information, it will need to consider how long to retain the information. The organization might want to consider factors such as the period of time public health authorities say it takes for COVID-19 virus to present itself in individuals and how long it might take for someone to be tested and diagnosed with COVID-19 (e.g. Alberta Health's contact-tracing app retains contact logs for 21 days). PIPA prohibits an organization from retaining the information longer than is necessary for legal or business purposes.

When the information is no longer required for those legal or business purposes, the organization is required to destroy the information or render it non-identifying (section 35).

Safeguarding

Organizations subject to PIPA are required to make reasonable security arrangements to protect personal information against unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction (section 34).

Using a single customer sign-in sheet can disclose personal information about one customer to others.

Organizations should consider how they can collect and retain the customer's personal information in a manner that does not disclose it to others, and ensure that access to this information is strictly controlled by certain employees (e.g. not all employees have access to the information).

Customer Rights

If a customer is unclear about why they are being asked to provide personal information, they can ask in what circumstances their information will be used and disclosed. Customers also have a right under PIPA to request access to their own personal information. They may also make a complaint to the OIPC if they believe that their personal information was improperly collected, used or disclosed.

Source: https://www.oipc.ab.ca/resources/pandemic-faq-customer-lists.aspx

Office of the Privacy Commissioner of Canada – Appearance before the House of Commons Standing Committee on Industry, Science and Technology (INDU) on contact tracing applications

May 29, 2020
Ottawa, Ontario

Opening Statement by Daniel Therrien
Privacy Commissioner of Canada

Thank you chair and committee members for your invitation to discuss tracing applications, which is one of the approaches being studied in Canada and elsewhere to ensure a safe return to a more normal life.

Please note that the expression “tracing applications” is used in public speech to describe various mobile applications as public health tools. Some are designed for conducting true contact tracing while others have the ultimate goal of informing users and giving them advice based on their level of risk.

Protecting both public health and privacy

During this public health crisis due to COVID-19, the health and safety of Canadians is a key concern. It is natural for governments and public health authorities to try to find ways, including technological means, to better understand and control the spread of the coronavirus.

In this context, the Office of the Privacy Commissioner has suggested a flexible and contextual approach in its enforcement of privacy laws. We strongly believe that it is possible to use technology to protect both public health and privacy. Technology in itself is neither good nor bad. Everything depends on how it is designed, used and regulated.

When properly designed, tracing applications could achieve both objectives simultaneously, in terms of public health and the protection of rights. If implemented inappropriately, they could lead to surveillance by governments or businesses that exceeds public health needs and is therefore a violation of our fundamental rights.

App design is key to the protection of rights

Appropriate design of technologies such as tracing applications depends on respect for some key privacy principles recommended in the OPC’s Framework to Assess Privacy-Impactful Initiatives in Response to COVID-19, and in a Joint Statement by Federal, Provincial and Territorial Privacy Commissioners on contact tracing applications.

In the interest of time, I will focus here on six of these principles.

First, purpose limitation: personal information collected through tracing applications should be used to protect defined public health purposes and for no other purpose.

Second, these applications should be justified as necessary and proportionate and, therefore, be science-based, necessary for a specific purpose, tailored to that purpose and likely to be effective. Third, there must be a clear legal basis for the use of these applications and use should be voluntary,

as this is important to ensure citizens' trust. Use should therefore be consent-based and consent must be meaningful.

Fourth, these exceptional measures should be time-limited. Any personal information collected during this period should be destroyed when the crisis ends and the applications de-commissioned.

Fifth, transparency: governments should be clear about the basis and the terms applicable to these applications. Privacy Impact Assessments or meaningful privacy analysis should be completed, reviewed by privacy commissioners, and a plain-language summary published proactively.

Sixth, accountability: governments and companies should be accountable for how personal information will be collected, used, disclosed and secured. Oversight by an independent third party, such as privacy commissioners, would enhance citizens' trust.

Current crisis heightens need for law reform

While governments have stressed the importance of privacy in the design of tracing applications, several of the principles I have mentioned are not currently legal requirements in our two federal privacy laws. So, for instance, nothing currently prevents a company from proposing an app that is not evidence-based and use the information for commercial purposes unrelated to health protection, provided consent is obtained, often in incomprehensible terms. A government could also partner with that company.

The current health crisis has made clear that technologies can play a very useful role in making essential activities safe. This meeting is about contact tracing but potential benefits are much wider: for instance, let us think about virtual medicine or e-education.

What we need, more urgently than ever, are laws that allow technologies to produce benefits in the public interest without creating risks that fundamental rights such as privacy will be violated. And because of the growing role of public-private partnerships in addressing situations such as the COVID crisis, we need common principles enshrined in public-sector and private-sector laws.

Source: https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2020/parl_20200529/

AB IPC – Commissioner Releases Report on ABTraceTogether Contact Tracing App

The Office of the Information and Privacy Commissioner of Alberta (OIPC) released a report today on its review of the ABTraceTogether privacy impact assessment (PIA). The PIA was submitted by Alberta Health (AH), and endorsed by Alberta Health Services (AHS), as required by Alberta's *Health Information Act* (HIA).

"With the global attention on contact-tracing apps during the COVID-19 pandemic, I prioritized my office's review of ABTraceTogether and took the additional step of publishing this report in the interests of transparency. While I am not in a position to endorse a particular technology solution, we found Alberta Health was mindful of privacy and security in deploying the app," said Information and Privacy Commissioner Jill Clayton.

In particular, the review highlighted ABTraceTogether's clear purpose to supplement already established contract-tracing processes, AH's consent-based approach, limited collection of health or personal information when registering to use the app, and AH's efforts to mitigate the risk of secondary use of information collected by the app, specifically for quarantine enforcement.

"Despite the positive aspects, I have ongoing concerns related to the functionality of ABTraceTogether on Apple devices. We recognize the challenges AH has faced in this regard, since the safeguards required are out of its control. Nonetheless, given the need to run ABTraceTogether in the foreground on Apple devices, there is a security risk. Running the app on Apple devices requires a device to remain unlocked, which significantly increases risk in case of theft or loss," said Clayton.

The risk on Apple devices increases for employers in the public, health and private sectors that have obligations to reasonably safeguard health or personal information under Alberta's three privacy laws – the *Freedom of Information and Protection of Privacy Act*, HIA and *Personal Information Protection Act*.

For employers that provide employees with devices or allow employees to use their own devices for work purposes, and those devices store or otherwise make accessible health or personal information (e.g. email or cloud service portals), the risk for running the app on Apple devices represents a potential contravention for failure to safeguard under Alberta's privacy laws.

The OIPC accepted the ABTraceTogether PIA with recommendations. Acceptance of the PIA acknowledges that AH has taken reasonable steps to protect privacy. Acceptance is not a waiver or relaxation from legislated requirements.

There were several findings and recommendations in the report. Some recommendations relate to clarifying inconsistencies found between documentation provided during the PIA review and what is made available publicly. The OIPC also recommended AH to continue to report publicly on the use and effectiveness of ABTraceTogether, and on its plans to dismantle the app when the time comes.

Contact
Scott Sibald (780) 422-9048

Source: https://www.oipc.ab.ca/news-and-events/news-releases/2020/commissioner-releases-report-on-abtracetogether-contact-tracing-app.aspx

Office of the Privacy Commissioner of Canada – Joint statement on global privacy expectations of Video Teleconferencing companies

July 21, 2020

Introduction

This is an open letter to companies providing Video Teleconferencing (VTC) services. We write to you as a subset of the global privacy regulatory community, with responsibility for protecting the privacy rights of citizens across the world.
Privacy concerns

Use of VTC to stay connected is not new. But as a result of the Covid-19 pandemic, we have seen a sharp increase in the use of VTC for both social and business purposes, including in the realm of virtual health and education, which can involve the sharing of particularly sensitive information, for particularly vulnerable groups. This increase in use exacerbates existing risks with the handling of personal information by VTC companies, and also creates new ones.

Reports in the media, and directly to us as privacy enforcement authorities, indicate the realisation of these risks in some cases. This has given us cause for concern as to whether the safeguards and measures put in place by VTC companies are keeping pace with the rapidly increasing risk profile of the personal information they process.

This letter

The purpose of this open letter is to set out our concerns, and to clarify our expectations and the steps you should be taking as VTC companies to mitigate the identified risks and ultimately ensure that our citizens' personal information is safeguarded in line with public expectations and protected from any harm.

Note that this is a non-exhaustive list of the data protection and privacy issues associated with VTC. It is intended to remind you of some of the key areas to consider given the increased use of your VTC services.

You should still regularly review your thinking on key privacy questions through privacy impact assessments. Where risks cannot be mitigated, we expect organisations to consult with their privacy regulator(s) to explain the specific risks identified and work through possible solutions on how these might be addressed.

Principles

1. Security

With personal information driving our digital economies, cyber-risks and threats to data-security are in a constant state of morphing and evolution. Today's security measures may soon become outdated and compromised by emerging threats. Data-security is a dynamic responsibility and vigilance by organizations is paramount.

During the current pandemic we have observed some worrying reports of security flaws in VTC products purportedly leading to unauthorised access to accounts, shared files, and calls.

In a world of global conversations, with personal information and private communications passing through many countries, we believe VTC providers should have certain security safeguards in place as standard, which would generally include: effective end-to-end encryption for all data communicated, two-factor authentication and strong passwords.

Such security measures should be given extra consideration by organisations who provide VTC services for sectors that routinely process sensitive information, such as hospitals providing remote medical consultations and online therapists, or where the VTC platform allows sharing of files and other media, in addition to the video/audio feed.

Your organisation should remain constantly aware of new security risks and threats to the VTC platform and be agile in your response to them. We would anticipate that you routinely require users of your platform to upgrade the version of the app they have installed, to ensure that they are up-to-date with the latest patches and security upgrades.

Particular attention should also be paid to ensuring that information is adequately protected when processed by third-parties, including in other countries.

2. Privacy-by-design and default

If data protection and privacy are merely afterthoughts in the design and user experience of a VTC platform, it increases the likelihood that you may fall short of the expectations of your users in upholding their rights. For instance, we have seen this manifest itself in well documented accounts of unexpected third-party intrusion to calls.

You should ensure that you take a privacy-by-design approach to your VTC service. This means making data protection and privacy integral to the services you provide to the customer. Always consider, as a starting point, the most sensitive information that could potentially be shared on your platform, and adopt the most privacy-friendly settings as default (similar to the **principle of least privilege** in cyber security). People who use your platform for less sensitive conversations or content sharing can adjust these settings to suit their requirements.

Simple measures to achieve this include:

- creating privacy conscious default settings that are prominent and easy to use, including implementing strong access controls as default, clearly announcing new callers, and setting their video / audio feeds as mute on entry;
- implementing features that allow business users to comply with their own privacy obligations, including features that enable them to seek other users' consent; and
- minimising personal information or data captured, used and disclosed by your product to only that necessary to provide the service.

VTC providers should also undertake a privacy impact assessment to identify the impact of their personal information handling practices on the privacy of individuals, and implement strategies to manage, minimise or eliminate, these risks.

3. Know your audience

During the Covid-19 pandemic, we have seen many examples of VTC platforms being deployed in contexts for which they were not originally designed. This can create new risks that you may not have anticipated prior to the current crisis.

Therefore, make sure that you review and determine the new and different environments and users of your VTC platform as a result of the pandemic. This is particularly important when it comes to

children, vulnerable groups, and contexts where discussions on calls are likely to be especially sensitive (in education and healthcare for example), or when operating in jurisdictions where human rights and civil liberty issues might create additional risk to individuals engaging with the platform. Consider what the data protection and privacy and requirements are for all contexts in which your platform is now in use, and implement appropriate measures and safeguards accordingly.

4. Transparency and fairness

As a result of several high-profile privacy breaches over recent years, there is heightened community awareness and expectations regarding how organisations handle personal information and use data in today's global digital economy. This is no different when it comes to VTC platforms. Failing to tell people how you use their information, and not considering whether what you are doing is expected and fair, may lead to a violation of the law and of the trust of your users.

You should be up-front about what information you collect, how you use it, who you share it with (including processors in other countries), and why – even if you do not consider the collection, use or sharing of that information to be particularly significant yourself, it is still important that its use is honestly communicated to the customer at all times. This is particularly the case when what you do with people's information is unlikely to be expected because it would not be seen as a core purpose of the VTC service. This information should be provided pro-actively, be easily accessible and not simply buried in a privacy policy. Where user consent regarding the handling of personal information is required, you should ensure that such consent is specific and informed.

Consider how any changes you make to future versions of the platform will affect all of the above. Assess their impact and consider whether it is important to make users aware of these changes. This will allow them to make informed decisions about how they use your platform moving forward.

5. End-user control

End-users may often have little choice about the use of a VTC service if a particular platform has been purchased, or is being exclusively utilised, in a given work-place, school or other setting. Some of the more novel features of VTC platforms may raise the risk of covert or unexpected monitoring.

While the companies and institutions using your VTC platform have their own data protection, privacy, and broader legal and ethical considerations in making decisions about the use of monitoring features, you should take your own steps to ensure that end-users of your service are empowered by having appropriate information and control.

For instance, if you offer a VTC platform that allows the host to collect location data, track the engagement or attention of participants, or record or create transcripts of calls, you should ensure that the use of these features is clearly indicated to those on the call when they are activated (through icons and pop-ups, for example). Where possible, you should also include a mechanism for end-users to choose not to share that information, for example via opt-out, noting that opt-in mechanisms might be more appropriate in certain instances.

Summary

We recognise that VTC companies offer a valuable service allowing us all to stay connected regardless of where we are in the world; something that is especially important in the midst of the current Covid-19 pandemic. But ease of staying in touch must not come at the expense of people's data protection and privacy rights.

The principles in this open letter set out some of the key areas to focus on to ensure that your VTC offering is not only compliant with data protection and privacy law around the world, but also helps build the trust and confidence of your userbase.

We welcome responses to this open letter from VTC companies, by 30 September 2020, to demonstrate how they are taking these principles into account in the design and delivery of their services. Responses will be shared amongst the joint signatories to this letter.

Originally signed by:

Elizabeth Hampton
Deputy Commissioner
Office of the Australian Information Commissioner
AUSTRALIA

Brent R. Homan
Deputy Commissioner
Compliance Sector
Office of the Privacy Commissioner of Canada
CANADA

Paul Canessa
Information Commissioner
Gibraltar Regulatory Authority
GIBRALTAR

Stephen Kai-yi Wong
Privacy Commissioner for Personal Data
HONG KONG, CHINA

Adrian Lobsiger
Federal Data Protection and Information Commissioner
SWITZERLAND

James Dipple-Johnstone
Deputy Commissioner
Regulatory Supervision
Information Commissioner's Office
UNITED KINGDOM

Source: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/let_vc_200721/

ON IPC – Working from home during the COVID-19 pandemic: FACT SHEET

Many government and public sector organizations had to close their offices with little advance notice because of the public health crisis brought on by COVID-19. People are working from home, many I makeshift conditions that were never planned or anticipated. This creates the potential for new challenges and risks to privacy, security, and access to information.

Although this is an unprecedented and rapidly changing situation, Ontario's access and privacy laws continue to apply. As a result, your organization must take timely and effective steps to mitigate the potential risks associated with this new reality. This fact sheet outlines some best practices to consider when developing a work-from-home plan that protects privacy and ensures access to information.

Work from home Policies

You should work with your information technology, security, privacy, and information management staff to review and update any existing work- from-home policies to adequately address the risks to access, privacy and security, as they may have evolved since originally drafted.

If you do not have such policies in place, you should create them by adapting your existing privacy, security, and data access policies to the unique features of the current context where virtually everyone is working from home.

Communicating with your staff

You should remind your staff:

- that the legislative requirements and corporate policies and practices related to access, privacy, security, and information management continue to apply when working from home
- to immediately report any information security incidents and privacy breaches (that is, when personal information is lost or stolen, or collected, used, or disclosed without authorization)

You should provide your staff with:

- updated contact information for key individuals who can provide technical, and administrative support (for example, information technology, security, records management, freedom of information, and privacy staff)
- alerts to fraud, phishing scams, and other malicious cyberattacks, and practical guidance on how to identify and defend against them (for example, how to pick up on some tell-tale signs of fraudulent emails and reminders not to click on attachments or links from unknown sources)

See the IPC's *Protect Against Phishing* Fact Sheet for best practices, **https://www.ipc.on.ca/wp-content/ uploads/2019/07/fs-tech-protect-against-phishing-e.pdf**

Remote access to networks and information

If possible, enable secure remote access to your networks, databases, and email accounts (for example, by requiring staff to use strong access controls such as multi-factor authentication, and a virtual private network (VPN) with end-to-end encryption).

Where secure remote access is available, prohibit your staff from:

- using unsecured WiFi
- removing personal information from the office (electronic and/or hardcopy) without prior approval

In light of the heightened risks associated with your staff working from home, you should review your organization's access controls to ensure staff only have access to the minimum amount of personal information they need to do their jobs.

Technological devices and related software

Work-issued devices

You should identify the specific technology and other resources (such as laptops, mobile phones, secure USB drives, printers, software applications, etc.) your staff requires to carry out their functions at home.

Ideally, your organization should provide them with the software and hardware they need when working from home. This will greatly reduce the privacy and security risks that can arise when staff use their own personal devices, such as non-industry standard or out-of-date security software, and shared devices.

Your work-issued devices should have up-to-date security software, applications, and other necessary resources installed to ensure that your staff can do their jobs while protecting privacy and security.

Work-issued devices and installed software should be properly configured, preferably by your information technology staff. If the use of external communication platforms and cloud service tools is permitted or required, ensure that your staff understands how to safely install, configure, and use them. For example, video conferencing sessions should have password-restricted access controls and appropriate limits on screen sharing and recordings.

Staff should not download or install programs or apps on work-issued devices without prior approval. Many popular programs and apps are known to have security vulnerabilities that can expose your organization to unnecessary risk.

Personal devices

If you are not in a position to issue technology equipment and related resources to everyone and some staff must use personal devices for work-related purposes, consider what measures should be in place to strengthen the protection of the information accessed, used, and saved on those devices.

For example, the security software installed on home computers may not be equivalent to the software used at your office and may require upgrading.

If your staff must use their personal devices for work purposes:

- remind them to take appropriate precautions to protect personal information, including ensuring necessary security features are installed, anti-virus software is enabled and updated, and WiFi connections are secure
- in the absence of secure remote access tools, require staff to appropriately segregate and secure all work-related records stored on any shared device used at home (for example, save password protected files on personal devices in a separate location from personal

records so other family members cannot access them

- develop a plan to manage the secure destruction of work-related records following applicable retention periods

Communicating by email
To the maximum extent possible, ask your staff to use only work-issued email accounts.

Remind your staff to take steps to protect any records containing personal information before sending emails, by:

- securing personal information on work-related or personal devices (for example, by encrypting or password protecting document attachments and sharing passwords separately through a different channel or message)
- if securing personal information is impossible, obtaining prior consent from the individual to whom the personal information relates before sending
- verifying the recipient's identity and making sure to correctly address emails to avoid misdirection (for example, by sending test emails in advance to ensure they reach the intended recipient)
- verifying that emails only contain content relevant to the intended recipient

Home workspaces
Advise your staff to set up a private workspace in their home or at a location to be agreed upon with their manager.

Require staff to take all reasonable measures to ensure screen content is not viewable and phone or video conversations involving personal or other sensitive information cannot be overheard by others in the home or other agreed-upon workspace.

Remind your staff to:

- secure work-issued and personal computing devices when not in use or when left unattended
- never leave their computing devices visible and unsecured outside the home
- not work in public places where there are higher risks of eavesdropping and equipment loss and theft
- appropriately use password protection and encryption on their devices

Paper and other formats of records
Remind your staff to take appropriate precautions to protect paper records and other formats containing personal information (for example, photos, audio or video recordings, hard drives and USBs), including by:

- not leaving personal information unattended or unsecured when away from the workspace
- securely storing all records containing personal information regardless of the format
- not printing records containing personal information, unless necessary
- not throwing out paper records containing personal information (for example, by putting them in the garbage or recycling)

- securely retaining personal information, if unable to follow required secure destruction protocols at home, until such time as access to secure shredding services can be obtained

Your organization should develop a plan to ensure the secure destruction of any records with personal information, regardless of format, following applicable retention schedules. The plan may include allowing staff access to office shredding facilities when it is safe to do so.

Access to information rights

Your organization's obligations to enable access to information and ensure reasonable measures are in place to document and preserve records continue to apply when your staff are working from home.

To ensure that your organization complies with these obligations, you should remind your staff:

- that all work-related records continue to be subject to access to information laws, regardless of whether they are retained on work- issued or personal computing and storage devices
- to record business activities, including keeping accurate records of all key business decisions and retaining all business records
- of the importance of good record management practices, such as the use of approved file naming conventions so records can be managed properly and easily located
- to digitize and transfer all business records to work-related systems and repositories, as soon as possible
- to appropriately back-up business records if using personal computing and storage devices

Longer-term strategy

To continue meeting your evolving operational needs, while complying with applicable access and privacy legislation, your organization should create a long-term work-from-home strategy.

Accompanying policies, practices, and remote training should address key issues such as:

- use of personal computing devices
- how to recover business records and other informational assets from staff who depart from the organization during the pandemic
- secure transfer and retention of records including personal information
- secure disposal of records and devices, including personal devices, used for work-related purposes during the pandemic
- migration of records and devices back to the office, and update of corporate files and record repositories
- managing freedom of information requests including requirements to conduct a reasonable search for records
- monitoring and evaluating the effectiveness of access and privacy (including security) measures in a remote work context and enabling continuous improvement of such measures based on practical, learned experiences

Source: https://www.ipc.on.ca/wp-content/uploads/2020/07/fs-privacy-work-from-home.pdf

ON IPC – Back to School … well, sort of

Sep 15 2020

After what some parents have called 'the longest Spring Break ever,' September is here, and schools across the province are re-opening their doors, in part. It's been heartening to see kids smiling from ear to ear, even with their masks on, eager to see their friends and teachers again. The courage in their voices affirms that they're prepared to learn and determined to adapt to whatever novel and experimental approaches come their way.

But this year's classrooms will look and feel a lot different, with many kids staying home for their own safety and that of their families, preferring to participate in online learning.

Given the current context, many schools across Ontario have had to accelerate their use of online learning platforms. Under Ontario's municipal privacy law, school boards are accountable for ensuring that online tools do not improperly collect, use, or disclose students' personal information.

But some of these tools don't always have adequate privacy and security protections. Parents may be justifiably concerned about the security features of some surveillance tools that can take over home computer cameras or microphones, and record their children outside the classroom. Parents may legitimately worry about some education software programs that collect excessive behavioral data and generate student profiles to predict intelligence or likely success rates, which then get shared with third parties without proper authorization.

While these online learning tools existed before COVID-19, their deployment on a grand scale has a sharp way of focussing the mind on their attendant risks.

Our *Guide to Privacy and Access in Ontario Schools* provides a number of best practices for schools and school boards to consider when selecting and using online learning platforms. These include:

- developing and implementing policies that evaluate, approve, and support online tools
- providing privacy and security training and ongoing support for teachers and staff
- notifying students and parents in a timely, clear and concise manner about the personal information that may be required by the online platform
- allowing students or parents to opt out of using the online platform or certain features, where feasible

In addition, we have developed a series of IPC fact sheets to help school boards, teachers, administrators, and parents navigate the new frontiers associated with virtual classrooms and e-learning.

Online learning platforms are powerful tools, and never have they proven to be so important as now. Having strong privacy policies and effective security safeguards in place can help students, parents, teachers, and school boards get this school year off to a good start.

Patricia

Source: https://www.ipc.on.ca/back-to-school-well-sort-of/

NFLD Labrador IPC – Information and Privacy Commissioner Comments on Provincial COVID Alert

Office of the Information and Privacy Commissioner
September 3, 2020

Following productive discussions with the Department of Health and Community Services and the Newfoundland and Labrador Centre for Health Information, we have concluded our review of the COVID Alert exposure notification application and support use of the app.

The OIPC has been engaged from an early stage on the development of COVID Alert. Although the federal government led the development of this app, the Privacy Commissioner of Canada and the Ontario Information and Privacy Commissioner ensured that privacy commissioners across Canada were consulted. Its development is consistent with the privacy principles expressed by federal, provincial and territorial privacy commissioners in a May 7 joint statement. The app being launched today was developed based on a protocol developed by Google and Apple and, while it leverages federal work, the version launched here has been customized for this province.

The app is based on a protocol that does not involve the collection of personal information by the government or any company, as the technology has been designed to ensure the data is anonymized. It has been subject to scrutiny by privacy and cybersecurity experts around the world. The app demonstrates that modern technology can meet an emerging need without the mass collection of personal information. Through adoption of this app, the government has established a high standard as it moves into more e-services.

“It is my job to critically examine new government-led programs or legislation to determine if they meet privacy protection requirements entrenched in our legislation. In this case, I am happy to say that the privacy questions we have raised to date have been satisfactorily answered,” says Commissioner Harvey. “I will download this app and use it myself.”

Downloading and using the app must be entirely voluntary. This is an important civil liberties issue. The OIPC encourages the provincial government to consider enacting legislation to prohibit anyone, public or private, from requiring use of the app as a condition for the provision of goods, services, entry into a premises or facility, or into the province itself.

The OIPC expects the Department to evaluate adoption and implementation of the app to ensure that it functions as intended and continues to meet the identified need.

“I support the use of this exposure notification app as a privacy-sensitive use of modern technology to confront a novel and rapidly emerging problem. This app will only work if people trust it and people will only trust it if their privacy is protected,” said Harvey. “Putting privacy first in the development of this app is good for our fight against COVID and an excellent example for the development of other digital public services.”

Media contact
Sean Murray
Director of Research and Quality Assurance
709-729-6309

Source: https://www.gov.nl.ca/releases/2020/oipc/0903n04-2/

Other Organizations

Global Privacy Assembly (GPA) – Achieving privacy by design in contact tracing measures

21 MAY 2020

A statement by the Global Privacy Assembly's Executive Committee

Background
Data protection and privacy authorities around the world are working together with public bodies and commercial organisations to respond to and manage the global COVID-19 pandemic. Our March 17, 2020 statement observed that GPA member authorities operate under data protection and privacy laws that enable the use of data to protect public health, while also protecting the public's personal data in a way that the public expects.

GPA authorities are working to assist public bodies and organisations to understand what good practice looks like in a pandemic. We are therefore encouraged to hear that many member authorities have, since our March statement, been engaged by organisations and public bodies in a common effort to overcome COVID-19. This acknowledges the need to work constructively to ensure privacy is protected as we seek solutions to this public health crisis.

COVID-19 contact tracing and public trust
Many authorities are at this time advising, reviewing and consulting on contact tracing measures. The issues being considered around the world are similar and revolve around universal data protection and privacy principles.

Contact tracing has historically been a vital pandemic response tool. Many governments around the world wish to harness technology to automate traditional contact tracing methods, which may be labour-intensive. Smart phone contact tracing apps are therefore being designed and rolled out globally.

We are issuing this statement about contact tracing measures being implemented around the globe because we recognise that public trust and confidence in the way personal information is handled and protected is a necessary precondition for their success. Whilst the public interest case is strong, protecting privacy and acting in accordance with public expectations is part of achieving the solution.

The success of contact tracing apps will depend on the trust of individual members of the public that their privacy will be protected appropriately and wider ethical considerations have been addressed. Uptake may be higher if governments and organisations transparently demonstrate that privacy risks have been adequately addressed. Authorities are playing their part in achieving fit-for purpose privacy protections, and wherever possible are prioritising consultation requests about COVID-related measures.

Privacy considerations in contact tracing design, implementation and operation
The value of privacy by design lies in ensuring privacy is carefully considered when developing new technologies in the interests of protecting public health. The data and privacy protection work of GPA authorities not stand in the way of innovation, rather privacy by design is a key enabler for both ethical and lawful innovation and the protection of personal data.

Privacy and data protection impact assessments (DPIAs) help ensure public bodies and organisations take a privacy by design approach by documenting in advance what their intended use of data is and how this can inform limitation in data collection, identifying the risks that their use of data could

create, and developing strategies to mitigate those risks to inform the design. In conducting this impact assessment, organisations may need to consult and engage with their intended user base and with regulators. DPIAs should also be clear about other possible current and future uses of the data, such as for research in the public interest. A DPIA can also be iterative, updated as needed, and provide opportunities for further engagement and public debate when it is made available for wider scrutiny.

In the current circumstances of the pandemic, measures are being developed as a direct response to these extraordinary circumstances. Time limitation is therefore also critical in establishing public trust in these responsive measures.

The following questions are addressed to organisations and governments engaged in contact tracing measures and can inform the development of contact tracing apps to ensure personal information is protected and the impact on privacy is minimised:

- Have you adopted a privacy by design approach?
- Have you conducted an assessment of the privacy risks? Is this assessment up to date?
- Have you addressed the security, safeguards, and necessity of both centralised and decentralised models?
- Have you had open and constructive engagement with your data protection authority?
- Are you being transparent with users, including providing a clear privacy statement or notice where required by law?
- Are you being transparent in a way that facilitates public debate?
- Is your contact tracing app temporary and will data be deleted when no longer required?
- Do you intend to retain data for research in the public interest? If so, what privacy protections have been adopted and is anonymisation envisaged at design stage?
- Do you have a process in place to revisit privacy implications if features are proposed to change?

Looking ahead to other COVID-19 measures and privacy

Some governments around the world are contemplating other pandemic responses involving personal information such as immunity passports, temperature checks and customer identification requirements. The principles set out in this statement also apply to these and other measures that may be considered, and further clarifying statements on those measures will be issued as required. The GPA will continue to listen to concerns from its member authorities to ensure our efforts address the most pressing issues being brought to the attention of GPA authorities by those working on COVID-19 measures.

– GPA Executive Committee

Source: https://globalprivacyassembly.org/contact-tracing-statement/

Global Privacy Assembly (GPA) – Statement by the GP Executive Committee on the Coronavirus (COVID-19) pandemic

17 MAY 2020

The Executive Committee of the Global Privacy Assembly (GPA) recognises the unprecedented challenges being faced to address the spread of Coronavirus (COVID-19).

Addressing these challenges requires coordinated responses at national and global levels, including the sharing of personal information as necessary by organisations and governments, as well as across borders.

We are confident that data protection requirements will not stop the critical sharing of information to support efforts to tackle this global pandemic. The universal data protection principles in all our laws will enable the use of data in the public interest and still provide the protections the public expects. Data protection authorities stand ready to help facilitate swift and safe data sharing to fight COVID-19.

Health data is considered sensitive across many jurisdictions, but work between data protection authorities and governments means we have already seen many examples of national approaches to sharing public health messages; of using the latest technology to facilitate safe and speedy consultations and diagnoses; and of creating linkages between public data systems to facilitate identification of the spread of the virus.

We issue this statement today to set out our support for public bodies and health practitioners to be able to communicate directly with people, and scientific and government bodies to coordinate nationally and globally, to tackle the current COVID-19 pandemic.

Our data protection and COVID-19 resources page provides the latest guidance and information from GPA members.

– GPA Executive Committee

Elizabeth Denham CBE, GPA Chair and UK Information Commissioner

Marguerite Ouédraogo Bonané, President of CIL, Burkina Faso

Angelene Falk, Information Commissioner and Privacy Commissioner, Office of the Australian Information Commissioner

Raymund Enriquez Liboro, Privacy Commissioner and Chairman, Philippines National Privacy Commission

Eduardo Bertoni, Director of the National Access to Public Information Agency, Argentina

Besnik Dervishi, Information and Data Protection Commissioner, IDP Albania

Francisco Javier Acuña Llamas, President Commissioner, National Institute for Transparency, Access to Information and Protection of Personal Data (INAI), Mexico

John Edwards, Privacy Commissioner, Office of the Privacy Commissioner, New Zealand

Global Privacy Assembly (GPA) – Executive Committee joint statement on the use of health data for domestic or international travel purposes

31 MARCH 2021

The Global Privacy Assembly (GPA) Executive Committee has today published a joint statement on the importance of privacy by design in the sharing of health data for domestic or international travel requirements during the COVID-19 pandemic.

Data protection and privacy authorities highlight the importance of privacy by design in the sharing of health data for domestic or international travel requirements during the COVID-19 pandemic

Background

Governments around the world are implementing measures to stop the spread of COVID-19 whilst also planning for a return to full economic and social activity across borders. For many domestic or international passengers, this has meant sharing health information such as a negative COVID-19 test result or vaccination status as a prerequisite of travel. Digital 'health passports' and 'health codes' have also been proposed.

The potential sharing of these elements of health data, on a mass scale across borders, and across a range of entities, is unprecedented. Digital technology provides the opportunity to do this at speed and scale. Whilst such steps may potentially be justifiable on public health grounds, the sharing of this sensitive information can and should be done in a privacy protective manner. Technology will offer both risks and opportunities to build protections for individuals. Innovation can go hand in hand with privacy.

Since the start of the pandemic, members of the Global Privacy Assembly have advised governments, private enterprises, charities and non-governmental organisations on the design and development of systems that allow the processing of personal health data in a manner that best protects privacy. This statement seeks to complement efforts made at a national or regional level, and contribute to a positive, co-ordinated privacy outcome internationally, reflecting common global principles of data protection and privacy, including privacy by design and default.

Building public trust by protecting privacy

In order to build trust and confidence in the way in which health data is processed for travel purposes, individuals need to be assured that: their data is handled securely; the data demanded of them is not excessive; they have clear and accessible information to understand how their data will be used; there is a specific purpose for the processing; their data will be retained for no longer than is necessary.

The Global Privacy Assembly Executive Committee recalls that while data and technology can be important tools to help fight the COVID-19 pandemic, they have intrinsic limitations and can merely leverage the effectiveness of other public health measures and need to be part of a comprehensive public health strategy to fight the pandemic. The principles of effectiveness, necessity, and proportionality must guide any measure adopted by government and authorities that involve processing of personal data to fight COVID-19. [1]

The Global Privacy Assembly Executive Committee therefore urges governments, and other organisations responsible for processing health data for the purposes of international travel,

to consider and pay due regard to the following principles, which reflect common global data protection principles and practice:

- The processing of health data as a prerequisite of international travel may be justifiable on the grounds of protecting public health, but considering privacy risks at the outset is vital.
- 'Privacy by design and default' principles should be embedded into the design of any system, app or data sharing arrangements regarding the processing of health data for the purposes of international travel. A formal and comprehensive assessment of the privacy impact on individuals before the commencement of any processing is the best method of ensuring data protection by design principles are implemented in practice and underlying risks are mitigated appropriately. Organisations should seek advice or consult guidance from data protection and privacy authorities on this issue.
- Personal data collected, used or disclosed to alleviate the public health effects of COVID-19 require a clearly defined purpose. The purpose should be specific within the broad context of the public health measure. Personal data must not be used in a manner incompatible with this purpose.
- All organizations must operate under relevant and appropriate lawful authority, ensuring that they only process health data when it is necessary and proportionate to do so.
- The data protection rights of vulnerable individuals, who may not be able to use, or may not have access to, electronic devices, must be protected, and alternative solutions should be considered to ensure that such individuals do not suffer discrimination. Similarly, the data protection rights of those who due to their age, possible health risks or other underlying conditions cannot be vaccinated should also be protected.
- Individuals should be informed of how their data is being utilised, by whom and for what purpose, providing clear and accessible information, recognising the geographical, cultural and linguistic diversity of the people of society who will wish to travel.
- Organisations should collect the minimum health information from individuals or other sources that is necessary for their contribution to protection of public health.
- Measures should be used to address the risks of directly sharing information from health records for travel purposes – privacy by design approaches can include federated identity systems and device level processing.
- The cyber security risk of any digital systems or apps must be fully assessed, taking full account of the risks that can emerge from different actors in a global threat context.
- Organisations should consider carefully for how long data should be retained, and design a retention schedule for the safe deletion of information once it is no longer required.
- Sunset clauses should be built into the design of such schemes, foreseeing permanent deletion of such data or databases, recognising that the routine processing of COVID 19 health information at borders may become unnecessary once the pandemic ends.

The schemes should also be reviewed periodically to ensure that the processing remains necessary and proportionate whilst the pandemic is ongoing.

Source: https://globalprivacyassembly.org/gpa-executive-committee-joint-statement-on-the-use-of-health-data-for-domestic-or-international-travel-purposes/

Canadian Council of Parliamentary Ombudsman calling for cautious approach to vaccination certification schemes

May 26, 2021

As countries around the world, and some jurisdictions in Canada contemplate how or if certification of COVID-19 vaccination status will be implemented in daily life, Canadian Ombudsman are stressing a cautious approach that places fairness at the heart of any potential vaccination certification system that is applied to public services.

The Canadian Council of Parliamentary Ombudsman (CCPO) issued a guidance document today aimed at provincial and territorial public sector organizations under the jurisdiction of Ombudsman across the country. This includes agencies and government ministries providing services such as public education, housing, and health services.

“Although we are not seeing yet that people are having to show vaccination status to receive public services in Canada, with the guidance we are providing, we want to plant the seed both with public organizations, and with the public, that if this does start to happen it is done in a way that is fair, reasonable and just,” said Bill Smith, President of the CCPO and Ombudsman for Nova Scotia.

The guidance document calls on provincial and territorial governments to consider key fairness principles when contemplating COVID-19 vaccination certification approaches including:

- Clear direction for the use of vaccination certification must be given by government via legislation or publicly available policy.
- Any vaccine certification program must be evidence-informed and all decisions must be subject to review and appeal processes.
- Accommodations must be made for those who have not received the vaccine, including alternative service delivery options.
- Decisions about restricting access to a service based on a person’s vaccination status must be done in a transparent, procedurally fair manner and be clearly communicated to the affected person in an accessible way.

“Implementing new measures such as vaccine passports runs the risk of creating a lot of confusion, concern and formal complaints,” said Smith. “This guidance today serves as a reminder that may help prevent unfairness from occurring if this is something governments decide to apply to their public services.”

CCPO Media contact:
Sara Darling | 778-679-2588 | sdarling@ombudsperson.ca

Source: https://ombudsman.novascotia.ca/news-releases/canadian-council-parliamentary-ombudsman-calling-cautious-approach-vaccination

Canadian Council of Parliamentary Ombudsman – Fairness Principles for Public Service Providers Regarding the Use of COVID-19 Vaccine Certification

May 2021

These guidelines are intended for:

- ✓Provincial/territorial governments
- ✓Other public bodies under the jurisdiction of the Ombudsman

These guidelines are not intended for:

- × Federal government
- × Indigenous governments
- × International travel procedures
- × Private sector

These guidelines are directed to public organizations and are not intended to replace public health guidance.

Governments around the world are considering, or are currently in the process of implementing, vaccine passports or certificates[3] to allow individuals to prove vaccination against COVID-19 and gain access to certain services. Should municipal or provincial/territorial governments in Canada decide to implement vaccine certificates or passports to allow access to public services, the following principles are offered to help guide public sector organizations to proactively ensure fairness in their application. As a basic premise, and in keeping with the principles of administrative fairness, there should be no oppressive or unreasonable barriers to accessing services offered by provincial/territorial and municipal governments based on a person's vaccination status; government and other public services must be accessible to all.

These administrative fairness principles have been developed by the Canadian Council of Parliamentary Ombudsman (CCPO). The CCPO is comprised of provincial and territorial Ombudsman, whose mandate is to ensure people are treated fairly in the delivery of public services. By following these fairness principles, those who deliver public services are more likely to achieve fair administration in the use of vaccine certification should it be introduced in Canada.

1. **If vaccine certificates or passports are implemented in Canadian provinces and territories, governments must provide clear direction on their application and use to all entities providing services to the public, either via legislation or publicly available policy.**

Decisions to restrict an individual's access[4] to services based on vaccination status must be made

[3] Vaccine passport is the common term used to describe the process for proving vaccination status and confirming immunity against communicable diseases such as COVID-19. Other names for such certification may be used in different jurisdictions, such as vaccination certificate, immunity passport, or digital proof of vaccination.

[4] The term "access" used throughout this document refers specifically to in-person access to public services delivered by municipal, provincial and territorial governments in Canada. Remote access to these services should not be affected in any way by a person's COVID-19 vaccination status.

fairly and consistently by public service providers. As such, if an individual's vaccination status is considered relevant to the receipt of public services, it is critical that government provide clear guidance to decision makers through legislation or policy in order to prevent arbitrary, unlawful, unjust, or unreasonable decisions from being made. The criteria for obtaining such vaccine certification must be clearly established in such legislation or policy, communicated to the public, evidence-based, and subject to review or appeal. Provincial or territorial governments may create this legal or policy framework for the use of vaccine certificates or passports, but, in the interests of policy consistency, any such policy should apply to the broader public sector.

2. Government policy regarding the use of vaccination certificates or passports must be evidence-informed and subject to regular review.

Because the scientific and medical evidence for each COVID-19 vaccine continues to evolve, and the duration of protective immunity and vaccine efficacy remains uncertain at this time, public organizations must make decisions regarding the ongoing requirement for vaccination status based on current advice from appropriate public health officials and the associated scientific data. There should be a continuous assessment of whether there continues to be risk of transmission by those who have been vaccinated – and if so, an explanation of the rationale for continued use of such vaccine certificates or passports. Until further information is available and public health restrictions are lifted or loosened, public organizations should consider whether they can continue to provide adequate services using the same methods employed throughout the pandemic (such as through telephone and online delivery) with no disruption in service delivery.

3. Determining access to public services based on vaccination status cannot be contrary to the pre-existing laws of the relevant jurisdiction.

The unprecedented global pandemic cannot allow the lessening of legal frameworks in place that serve to protect individuals, such as privacy and human rights law. These laws must be considered when deciding whether to require proof of vaccination for access to a public service, and adequate consultation with relevant stakeholders and regulators should be conducted in each jurisdiction.

4. If introduced, vaccine certification must be made available in a way that is equitable and accessible to everyone.

While digital technology such as smart phones may be able to provide some individuals with immediate access to their personal health information (including their immunization records), this information must be made accessible in multiple ways. This means ensuring that there are alternative methods, such as paper records, for individuals to prove they have been fully vaccinated against COVID-19 and pose a reduced risk to public health. In addition, if tests for COVID-19 will be required to gain in-person access to a public service, these tests must be free, easily accessible and available to all those who may require them in the pursuit of receiving such service.

5. Requirements to disclose vaccination status in order to access public services must be proportionate to the type of service being provided, the associated risk to individuals and the risk posed to public health.

The decision to require vaccination status prior to receiving a public service must be proportionate to the nature of the service being provided and the risk of transmission of the COVID-19 virus. Similarly, where restrictions on an individual's liberty have been imposed based on their vaccination status (such as self-isolation requirements for inmates upon admission to a correctional centre), these must also be proportionate to the level of risk involved and reviewed regularly to determine whether or not they continue to be necessary, as they could be viewed as arbitrary and unfair.

6. **Accommodations must be made for those who have not received the vaccine.**

There are many individuals who may not be able to receive the COVID-19 vaccine (including as a result of the phased roll-out) and there are also those who will choose not to receive the vaccine. In these circumstances, public services should not be restricted on the basis of vaccination status. Instead, reasonable accommodations must be made for those individuals to receive services, and alternative methods of service delivery should be available to them.

7. **Public organizations should provide clear guidance to their staff to assist them in making and communicating decisions to limit access to services based on vaccination status.**

Decisions about limiting access to public services can be complex and challenging for front-line staff, particularly in the rapidly changing situation of the pandemic. Organizations should provide proper guidance to their staff to help them exercise discretion fairly and allow for some flexibility and accommodations to be made to standard policy. This guidance should ideally include information about the factors to consider when making accommodations, any limits to their discretion in determining such exceptions to the rule, and contact information for a resource within the organization where front-line staff can obtain further assistance or advice.

8. **Decisions about restricting access to a service based on a person's vaccination status must be done in a transparent, procedurally fair manner and be clearly communicated to the affected person in an accessible way.**

Individuals who are denied service or have limited access based on their vaccination status must have the ability to communicate with a representative of the service provider to discuss the matter and communicate their concerns. To facilitate this, adequate notice about the requirement to disclose vaccination status to access the service must be provided to the individual in advance. This notice should contain:

- clear reasons for the requirement to disclose vaccination status;
- the criteria used to make the decision that led to the requirement;
- the consequences for declining to provide information about vaccination status;
- information about how to access the service without disclosing vaccination status; and
- the name or title of a contact person at the organization who can answer questions and address any concerns about the requirement.

In addition, general policy regarding any requirements to prove vaccination status in order to access a service should be made publicly available on the organization's website.

9. **When decisions are made to deny or limit public services to those who may not be able to prove vaccination status, they must be informed of their right to appeal and be provided with information about the appeal process available.**

Decisions to limit or restrict services can have a significant negative impact on individuals. As such, procedural fairness also requires that those who suffer such an impact be informed of their right to appeal to the service provider for an exception to the proof of vaccination requirement based on their individual circumstances. Any decision made on appeal must provide clear and meaningful reasons to the affected individual.

10. If vaccine certificates or passports are implemented, government must ensure that independent oversight is in place.

Independent oversight of government is an essential aspect of Canada's democratic system. Particularly in times of significant and constant change, and when governments are taking such extraordinary steps to protect the health of individuals, oversight of government decisions is needed to ensure that government is accountable to the public it serves. Furthermore, should vaccine certification be introduced in Canada, municipal, provincial and territorial governments would benefit from proactive engagement with oversight bodies such as the Ombudsman. The members of the CCPO welcome the opportunity to consult with government to proactively identify fairness issues that may arise should vaccine certification be introduced in Canadian provincial/territorial jurisdictions. Governments may also reference, and find useful, the Fairness by Design self-assessment guide created by the CCPO for public organizations to proactively evaluate the fairness of their programs and policies.

Source: https://ombudsman.novascotia.ca/sites/default/files/documents/CCPO-Fairness-Principles_Vaccine-Passport-EN.pdf

Statement on the Government of Canada's vaccine passport for travel initiative

October 22, 2021

Privacy Commissioner of Canada Daniel Therrien released the following statement regarding the Prime Minister's announcement about a standardized Canadian COVID-19 proof of vaccination for travel:

> The federal government has consulted our office on the standardized proof of vaccination for travel initiative (vaccine passports) and we have had a number of constructive discussions with government officials over the last few months.
>
> Vaccine passports may offer significant public health benefits but they remain exceptional measures. They should only be imposed after careful consideration of privacy and other human rights principles.
>
> Earlier this year, our office, along with our provincial and territorial counterparts, issued a joint statement on privacy and COVID-19 vaccine passports.
>
> In particular, the statement says that in order to be justified, vaccine passports must be necessary to achieve their intended public health purposes. Their effectiveness in achieving these purposes should also be evidence-based.
>
> Further:
>
> - the privacy risks associated with the initiative must be proportionate to the public health purposes;
> - the personal information collected should be limited to that which is necessary for the intended public health purposes;
> - the information should be used only for the intended public health purposes and no other; and
> - the initiative should be time limited.
>
> The government has provided us with information relevant to each of these criteria. As mentioned, we have had constructive discussions with government officials about these issues.
>
> That being said, in recent days, our office has received a number of complaints related to the government's COVID-19 vaccination requirement for federal public servants. We will therefore be investigating the application of privacy principles in this context.
>
> Although the initiatives are distinct, the principles applicable to vaccine passports for travel and to the vaccination requirement for federal public servants are the same. It would therefore be inappropriate to offer conclusions until we have completed our investigations.
>
> Given the complaints about the public service vaccination requirement are now the subject of ongoing investigations, no further details can be provided.

Source: Statement on the Government of Canada's vaccine passport for travel initiative - Office of the Privacy Commissioner of Canada