OIPC Guidance

Assessing Privacy-Impactful Initiatives During Public Health Emergencies

Contents

INTRODUCTION

The Office of the Information and Privacy Commissioner (OIPC) in Newfoundland and Labrador is responsible for upholding and protecting access to information and protection of privacy rights in the Province of Newfoundland and Labrador. The jurisdiction of the OIPC extends to public bodies subject to the **Access to Information and Protection of Privacy Act, 2015** (ATIPPA, 2015), as well as custodians of personal health information subject to the **Personal Health Information Act** (PHIA).

The safety and security of the public is of grave concern during public health emergencies, like the recent COVID-19 health crisis. In many such crises, the urgency of limiting the spread of any 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 virus and any global threat it may present. In this context, extraordinary measures may be contemplated. Some of these measures may not be voluntary, and perhaps certain measures that are initially voluntary will become mandatory. 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 public bodies and custodians 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 associations, all of which are generally considered sensitive.

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. Public bodies and custodians should still apply the principles of necessity and proportionality, whether in applying existing measures or in deciding on new actions to address any 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 during a public health emergency. How personal information is safeguarded, and how long it is retained after the crisis, is also crucial.

PURPOSE

This guidance identifies key privacy principles that should factor into any assessment of measures proposed during a public health emergency that have an impact on the privacy of residents of the Province of Newfoundland and Labrador. This guidance concludes with a case study that applies the principles discussed.

WHAT IS AN EMERGENCY?

The Emergency Services Act defines emergency in Section 2(g):

> "emergency" means a real or anticipated event or an unforeseen combination of circumstances which necessitates the immediate action or prompt co-ordination of action as declared or renewed by the Lieutenant-Governor in Council, the minister, a regional emergency management committee or a council

For example, the COVID-19 pandemic was declared a provincial health emergency on March 18, 2020 under the Public Health Protection and Promotion Act. When a public health emergency is declared under the Act, the Chief Medical Officer of Health (CMOH) can introduce special measures to protect the health of the population. The Act:

- establishes the authority for the CMOH, a regional medical officer of health or other person acting under the authority of the Act or regulations to collect, use and disclose personal health information;
- identifies the notifications and protections (section 14) that will occur when the CMOH reasonably believes that there is a serious risk to the health of the population;
- addresses rights and confidentiality (Part III); it acknowledges that rights and freedoms may be restricted and that such restrictions should be reasonable in the circumstances; and
- establishes limits on collection, use and disclosure of personal information:
    - the CMOH may refuse to disclose information where the disclosure would result in an adverse effect, such as the violation of privacy and confidentiality rights of an individual (section 14(2)(a));
    - requirement to collect, use and disclose the minimum information necessary to accomplish the identified purpose (sections 15(2) and 16(2)); and
    - must take reasonable steps to ensure personal health information is as accurate, complete and up-to-date as necessary for the identified purpose and that the disclosure is authorized (section 17).

PUBLIC HEALTH EMERGENCIES: ASSESSING NINE PRIVACY PRINCIPLES

1) Legal Authority

Collection (Generally)

Public bodies and custodians must identify the legal authority to collect, use, and disclose personal information. While it is best practice to collect information directly from the individual, both ATIPPA, 2015 and PHIA allow indirect collections in appropriate circumstances. For example:

- Section 62 (1)(d) of ATIPPA, 2015 states, “A public body shall collect personal information directly from the individual the information is about unless…(d)

> collection of the information is in the interest of the individual and time or circumstances do not permit collection directly from the individual."

- Section 31 of PHIA identifies a number of situations where indirect collection is authorized.

Disclosure (Generally)

While obtaining consent for the disclosure of someone's information is the general rule, ATIPPA, 2015 and PHIA are not barriers to the appropriate sharing of personal information in an emergency where consent cannot be obtained. Both Acts have provisions that allow for disclosure in emergencies or when the public interest trumps the protection of privacy.

Section 9(3) of ATIPPA, 2015 states that, "Whether or not a request for access is made, the head of a public body **shall, without delay**, disclose to the public, to an affected group of people or to an applicant, information about a **risk of significant harm** to the environment or to the health or safety of the public or a group of people, the disclosure of which is clearly in the public interest". This section releases the public body from the requirement to obtain consent and overrides all exceptions under the Act.

It should be noted that section 9(3) **requires** release, which is one of the exceptions to protection of personal information (i.e. release is required by law). This release is to be **proactive** and does not require an access request be made.

Sections 34(l) and 40 of PHIA allow use and disclosure when it is to prevent or reduce a risk of serious harm to the mental or physical health or safety of the individual the information is about or another individual, or public health or public safety. While this section does not require release, it frees the custodian from the usual imperative to obtain consent (when not otherwise authorized under the Act to disclose) and to protect privacy.

Repercussions of Inappropriate Disclosure

Often the fear of being sued gives the public body or custodian pause when considering a disclosure of information that would normally be protected. Both ATIPPA, 2015 and PHIA contain sections that shield public bodies and custodians from lawsuits when they act in good faith under the Acts. Further, both Acts stipulate that it is **not** an offence under the Act to disclose information unless such disclosure was contrary to the Act.

ATIPPA, 2015 section 114 establishes that,

> an action does not lie against the government of the province, a public body, the head of a public body, an elected or appointed official of a local public body or a person acting for or under the direction of the head of a public body for damages resulting from: (a) the disclosure of or a failure to disclose, **in good faith,** a record or part of a record or information under this Act or a consequence of that disclosure or failure to disclose

PHIA section 87 states,

> An action does not lie against a custodian, or a person acting for or under the direction of a custodian for damages resulting from the use, collection or disclosure of or a failure to disclose, **in good faith**, personal health information under this Act or a consequence of that use, collection, disclosure or failure to disclose.

Legal Authority - Key Messages

- All public bodies and custodians must continue to operate with lawful authority. This means, for public bodies, such as government departments, municipalities, agencies, boards, and commissions, ATIPPA, 2015 governs their activities. For custodians of personal health information, PHIA applies.
- At the federal level, private-sector organizations that collect, use, or disclose personal information in the course of a commercial activity are subject to the **Personal Information Protection and Electronic Documents Act** (PIPEDA). The federal **Privacy Act** covers personal information-handling policies and practices of federal government departments and agencies. PIPEDA and the **Privacy Act** are under the jurisdiction of the federal Office of the Privacy Commissioner of Canada (OPC).
- Privacy laws apply to personal information, which is information about an identifiable individual. Even when public bodies or custodians use "open" or public sources such as social media to collect personal information, this is still considered a collection under the law. 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 public bodies and custodians take are necessary and proportionate.

OIPC recognizes that a public health emergency 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.

Emergency situations impact appropriate collection. For example, if staff call in sick during a public health emergency, employers should not request a specific diagnosis. However, during the recent pandemic, it would have been reasonable to ask if there was any association with COVID-19, if they had a confirmed diagnosis and/or if they have been advised to self-isolate. Employers may also want to seek guidance from public health on what information should be communicated with staff that may have been in contact with the individual, as well as the larger organization.

Necessity and Proportionality - 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).

OIPC guidance document Privacy Impact Assessments contains key questions for public bodies to consider that can assist public bodies and custodians in assessing the privacy impact of measures to address a public health emergency. Following are two scenarios to assist public bodies in the application of necessity and proportionality:

Scenario - Municipality

- A resident contacts Town/City Hall requesting the civic address of a particular resident, indicating that he has heard they are positive for COVID-19.
- A public health official on official business contacts Town/City Hall seeking confirmation of the civic address of a resident, citing their statutory authority to collect the information.
    - In the first scenario, there is no authority to provide the information. In the second, there is statutory authority for both the municipality to disclose, and the health official to collect.

Scenario – Public Body

- Your public body receives a phone call from the media or a member of the public asking for a list of recent work-related travel by all staff; they note they are concerned about COVID-19.
- Usually, some details of work travel would be released upon request. Specific details of personal travel would not generally be collected or disclosed by the public body. Given the situation, it would be appropriate to ask staff to self-identify if they have recently travelled to an impacted area and release general information (such as the number of staff and the countries visited).

3) Purpose Limitation

Personal information and personal health information collected, used or disclosed to alleviate the public health effects of any pandemic must not be used for other reasons.

Purpose Limitation - Key Messages

- This is particularly important when more personal information or personal health 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.
- Public bodies and custodians should continue to adhere to the minimum amount necessary standard when handling personal information and personal health information. (For more information on this topic, please review the OIPC guidance document on Minimum Amount Necessary Requirement).
- Personal information collected in an emergency situation should be destroyed when the crisis ends, except for narrow purposes such as ensuring accountability for decisions made during the crisis, particularly decisions about individuals. If a public body or custodian wishes to retain information for future evaluation or research, de-identification measures should be implemented. (See also principle nine: Time Limitation)

4) De-identification and Other Safeguarding Measures

Use de-identified or aggregate data whenever possible.

De-Identification and Other Safeguarding Measures - 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.
- Take administrative, technical and physical means to protect the personal information collected. Ensure safeguards are enhanced for sensitive information.

...next page Key Messages continues

De-Identification and Other Safeguarding Measures - Key Messages Continued

- Be especially mindful about the unique challenges with location data.
  - Location data points themselves can lead to re-identification 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 and perhaps impossible to fully anonymize or de-identify.

5) Vulnerable Populations

Consider the unique impacts on vulnerable groups.

Vulnerable Populations - 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 residents about new and emerging measures, on an ongoing basis.

Openness and Transparency - 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.

Open Data - 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.

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.
- Subject to section 112 of ATIPPA, 2015, any bill which may impact access to information or protection of privacy rights shall be subject to consultation with the Commissioner as soon as possible before, and not later than the date notice is given to introduce the bill in the legislature. The Commissioner should be engaged as early as possible in the process so as to allow for sufficient opportunity for the Commissioner to review and comment on the bill without impeding the timeliness of important legislative initiatives.

9) Time Limitation

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

Time Limitation - 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 and personal health information collected in an emergency situation should also be destroyed when the crisis ends, except for narrow purposes such as ensuring accountability for decisions made during the crisis, while de-identifying information retained for research purposes.

PUBLIC HEALTH MEASURES AND PRIVACY RIGHTS WORKING TOGETHER

In an emergency, privacy should not be considered a barrier; it should also not be used as an excuse for inaction. Even in an emergency, privacy principles still apply. Entities are reminded to collect, use, and disclose the minimum information necessary; to safely transmit required information using methods appropriate to the sensitivity of the information being shared; and to take reasonable security measures to protect information.

Public bodies should review decisions made during a public health emergency on a regular basis to ensure that they remain necessary and current. Privacy rights do not need to be a barrier to necessary public health measures. At the same time, emergencies should not be used as an excuse to encroach on privacy rights unnecessarily. This guidance is intended to illustrate how, with care, public health measures and privacy rights can work together.

A CASE STUDY: PROOF OF VACCINATION

Public Bodies Collecting Proof of Vaccination From Employees

The following case study is an example of how the above privacy principles could operate in practice. Following background information, the privacy considerations introduced above are examined in the context of the case study.

During the COVID-19 pandemic, many public bodies required proof of vaccination from employees (including contractors and volunteers) as a condition of returning to the workplace. This case study focuses on public bodies that collected, or considered collecting, information about the vaccination status of employees. The Government of Newfoundland and Labrador issued a Mandatory Vaccine Policy that applied to all provincial government departments, agencies, boards and commissions. Public bodies that were subject to this mandate established processes for collecting, using and disclosing personal information in compliance with ATIPPA, 2015.

This case study does not contemplate collecting vaccination status from individuals seeking services from a public body, nor does it address the legal responsibilities of private companies.

During the COVID-19 pandemic, a provincial vaccine passport was introduced, which provided individuals with a verifiable means of proving they were vaccinated in order to obtain certain categories of services or to enter certain premises. When the QR code of the NLVaxPass was read by the approved NLVaxVerify reader app, all the individual conducting the scan learned is the vaccination status and name of the individual. This offered a ready-made solution to public bodies seeking to obtain proof of vaccination status from employees.

Vaccination Status of Employees

Someone's vaccination status is that person's personal information, therefore any public body that collects the vaccination status of employees must comply with ATIPPA, 2015. At its most basic, public bodies must establish the purpose and authority for any collection, collect the least amount of information to meet the purpose, share it only with those who need to know, keep it secure, and destroy it when no longer needed.

It is important that preliminary details of the program are known prior to a privacy assessment. For example:

- Will the program apply to all employees, or just those in certain positions or locations?
- Will the program be mandatory or voluntary?
- Will the program be part of a larger public health effort such as masking, hand washing and social distancing, or will it be an isolated initiative?
- If employees are expected to be vaccinated, what are the consequences if employees are not?
- Will there be a grace period to allow employees to comply?
- What if an employee seeks an exemption? Public bodies are reminded that there are human rights protections or medical exemptions that may need to be considered, so it is important to have a process in place to consider any such requests;
- Employers may also need to consult collective agreement provisions and involve trade union representatives in the process. They may also wish to refer employees to other resources available, such as an Employee Assistance Program; and
- What vaccinations will be accepted? Vaccines that have received Health Canada or World Health Organization approval? What about an employee who is considered fully vaccinated in another jurisdiction, but not in Newfoundland and Labrador?

PRIVACY CONSIDERATIONS

Identified Purpose

Public bodies considering the collection of vaccination status information from employees must first identify the purpose of the program; what is the program objective? A public body should have a clear and compelling reason for collecting personal information such as vaccination status. The identified purpose of the program should also acknowledge any exceptions and identify any consequences of non-compliance.

As public health emergencies are rapidly evolving situations, public bodies should ensure frequent review of the program to ensure that the purpose is still current and the collection remains justifiable.

Collection

There must be a clear legal authority for each intended purpose of collection. It is possible that clear legal authority for vaccine passports, and possibly for collecting vaccination information for employment purposes, could come from new or existing legislation, or from a public health order. Otherwise, public bodies should look to section 61 of ATIPPA, 2015.

Section 61 establishes the purposes for which public bodies may collect personal information. While it is possible that other sections may apply, it is likely that the majority of public bodies will rely on section 61(c), which states, "No personal information may be collected by or for a public body unless …(c) that information relates directly to and is necessary for an operating program or activity of the public body."

For example, section 4 of the Occupational Health and Safety Act requires employers, including public bodies, to ensure the health, safety and welfare of employees. If a public body's collection relates directly to and is necessary for the health and safety of employees, then that collection would likely be authorized.

Section 62 of ATIPPA, 2015 details how personal information is to be collected. Public bodies seeking vaccination status of employees should collect the information directly from the individual and be prepared to explain the reason and legal authority for collection, as required by section 62(2).

Even if public bodies have the authority to collect personal information, they should collect the minimum necessary for the identified purpose. Will employers be asking employees about their vaccination status, or will they be requesting to see proof of vaccination? If they are asking to see proof, will they be making a copy or just viewing? The public body should also identify what vaccinations will be accepted and be prepared to be presented with documentation from another jurisdiction or potentially in another language. It should also establish clear deadlines for the new requirement and provide time for compliance. Further, public bodies should be prepared to assess requests for exemptions for a medical condition or other protected grounds. These questions should be addressed prior to program launch.

Section 63 requires reasonable efforts to ensure accuracy and completeness. Section 65 requires public bodies to retain such information for at least a year after using it. While public bodies may wish to request that employees show reliable proof of vaccination for the purpose of determining who can return to work, will it be necessary to copy and retain that record? If the accuracy of the information can be determined simply by inspection, it will be more difficult to justify the more privacy invasive action of copying and retaining it.

Use and Disclosure

A public body also needs to identify the authority for use and disclosure of the information it collects, and to always use and disclose only the minimum necessary. Section 66 of ATIPPA, 2015 establishes authority for various uses. One of the most common is 66(1)(a): use for the purpose for which the information was collected, or for a consistent purpose. To be considered a consistent purpose, the use should have a reasonable and direct connection to the purpose, and be necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body.

The ATIPP Office's Protection of Privacy: Policy and Procedures Manual provides useful information on the meaning of use versus disclosure on page 38:

> **Using personal information** usually means using it internally (within the department or agency) for the administration of a project or program. For

example, an individual has provided specific personal information to a department and that department has collected this information for the purpose of permitting that individual to apply for a student loan. Employees in that department may use that individual's personal information for the purposes of evaluating whether or not that individual is eligible for a student loan.

Disclosing personal information means showing, sending, telling or giving someone, another department, agency or organization the personal information in question. Information is disclosed externally when provided outside the original public body (i.e. department or agency or outside the Government of Newfoundland and Labrador). To continue the example above, providing the student's name and address when requested by Canada Revenue Agency may be a valid disclosure of personal information.

Public bodies should consider who in the organization should have access to employees' proof of vaccination information. In many organizations it may be possible to restrict use of the information to a human resources department, to a very few people, or even to the one individual who compiles the list.

Disclosure of personal information is discussed in sections 68 to 71 of ATIPPA, 2015. Public bodies considering disclosure should ensure clear identification of the authority for that disclosure.

Section 72 of ATIPPA, 2015 requires that departments or branches of the executive government must conduct a privacy assessment during the development of a program or service. OIPC strongly encourages any other public body considering collecting information about its employees' vaccination status to conduct a privacy assessment. Even if the statute does not require all Privacy Impact Assessments (PIAs) to be provided to OIPC, we are always happy to provide feedback on courtesy copies that are shared.

Safeguards

Section 64 requires that information be protected with reasonable safeguards; this generally includes administrative, physical and technical measures.

From an administrative perspective, public bodies would be wise to develop a policy that outlines the 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 to be taken if the employee has not had the vaccination; a statement on where information will be stored; a statement containing details about any potential use or disclosure of the information and the individual in the entity responsible for the use or disclosure; and a statement on when the information will be destroyed. In developing policy, public bodies must ensure that the authority for the collection, use, and disclosure of personal information is in compliance with ATIPPA, 2015. Given that public health emergencies are rapidly changing situations, the policy should also include a review schedule.

There should also be technical and physical safeguards. The focus of this discussion is on where records will be stored and who will have access. This is sensitive personal information,

so it should be secured with restricted access throughout all parts of the program. If, for example, employees submit scanned copies of forms to managers, who then pass them along to Human Resources, the information should be protected on the email system, and not retained unnecessarily at intermediate steps. If paper copies are provided, they should be securely stored and transported. If vaccination documentation is stored with other records, such as within personnel files, the public body should critically analyze the retention schedule and decide whether a separate standard should be developed.

Compliance Challenge

Public bodies are reminded that individuals are able to file a privacy complaint with OIPC. If a complaint is received, we will want to know what the public body told its employees about the program. Public bodies are encouraged to be open, clear and transparent in any communication with employees. They should identify an individual who can respond to questions about the program and provide links to resources.

Before Asking for Proof of Vaccination

Any public body considering collecting proof of vaccination from employees should consider the above, along with other applicable legislation, including human rights and employment law. Further, they should consult with employees, unions, and legal counsel. If such a program is developed with sufficient care, the result will not only be effective for the purpose, but will be widely accepted by employees, oversight bodies and the public.

RESOURCES

The case study guidance information was developed using resources produced by other jurisdictions at the Federal, Provincial and Territorial level, as well as resources developed by the UK Information Commissioner's Office. Newfoundland and Labrador resources included legislation (ATIPPA, 2015), Government of Newfoundland and Labrador resources (mandatory vaccination web page, VaxPass web page, Life with COVID web page, public health orders) and the Treasury Board Secretariat's Occupational Health and Safety Policy.

The guidance information on public health emergencies and measures is adapted from a piece published by the Office of the Privacy Commissioner of Canada.

There are many resources available for public bodies and custodians:

- OIPC NL's Website;
- ATIPP Office's Website; and
- Department of Health and Community Services' PHIA Resource page.

CURRENCY

This guidance replaces the following four OIPC resources, which have been removed from our website:

- A Framework for the Government of Newfoundland and Labrador to Assess Privacy-Impactful Initiatives in Response to COVID-19;

- COVID 19 FAQ;
- Public Bodies Collecting Proof of Vaccination from Employees; and
- Don't Blame Privacy – What to Do and How to Communicate in an Emergency.

Office of the Information and Privacy Commissioner
PO Box 13004, Station A
St. John's, NL A1B 3V8
Phone: (709) 729-6309
Toll Free: 1-877-729-6309
commissioner@oipc.nl.ca
https://www.oipc.nl.ca