



OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER

NEWFOUNDLAND AND LABRADOR

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

Updated April 2020



Overview

- When an emergency, like a pandemic, arises people want to act quickly and efficiently – the last thing they should be tripping over is privacy. But wait! “Privacy is important.” “Privacy must be protected.” “I don’t want to get sued for breaching someone’s privacy.”
- This slide deck is intended to shine some light on where the communication line is when privacy and urgent circumstance collide. The goal is to demonstrate how to not unnecessarily violate privacy, while also preventing unwarranted concerns from slowing response times.



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
- COVID-19 has been declared a pandemic by the World Health Organization; it was declared a provincial health emergency on March 18, 2020.



Public Health Protection and Promotion Act

- When a public health emergency is declared under the *Public Health Protection and Promotion Act*, the Chief Medical Officer of Health (CMOH) can introduce special measures to protect the health of the population.
- Part III of the *Act* addresses rights and confidentiality; it acknowledges that rights and freedoms may be restricted.
 - Such restrictions should be reasonable in the circumstances.



Public Health Protection and Promotion Act

- Establishes the authority for the CMOH, a regional medical officer of health or other person acting under the authority of this *Act* or the regulations to collect, use and disclose personal health information.
- Notification and Protection (section 14) will occur when the CMOH reasonably believes that there is a serious risk to the health of the population.



Privacy Considerations

- The *Act* establishes limits:
 - 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)).
 - 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).



What does the *Access to Information and Protection of Privacy Act, 2015* and the *Personal Health Information Act* say?



General Rule - Collection

- While it is best practice to collect information directly from the individual, the *Access to Information and Protection of Privacy Act, 2015* and *Personal Health Information Act* both allow indirect collections in appropriate circumstances:
 - *ATIPPA, 2015* section 62. (1) 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.
 - *PHIA* section 31 identifies a number of situations where indirect collection is authorized.



What to Collect

- Emergency situations impact appropriate collection.
 - In general, when staff call in sick, employers should not request a specific diagnosis.
 - During a pandemic, it would be reasonable to ask if there was any association with COVID-19.
 - Have they been advised to self-isolate?
 - Do they have a confirmed diagnosis?
 - If a staff member is off because of COVID-19, 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.



General Rule - Disclosure

- 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* (*ATIPPA* and *PHIA*) have provisions that allow for disclosure in emergencies or when the public interest trumps the protection of privacy.



ATIPPA, 2015

- Section 9(3) of the *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*.



ATIPPA, 2015

- Of note – section 9(3) **requires** release – which is one of the exceptions to protection of personal information (i.e. release is required by law).
- Further, the release is to be **proactive** and does not require an access request be made.



PHIA

- Sections 34(1) and 40 of *PHIA* allow use and disclosure when it is:
 - to prevent or reduce a risk of serious harm to*
 - (i) the mental or physical health or safety of the individual the information is about or another individual, or*
 - (ii) 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 Release

- Often the fear of being sued gives the public body or custodian pause when considering releasing 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*.



Repercussions of Release

- *ATIPPA, 2015* section 114 states:
 - 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...



Repercussions of Release

- *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.



Repercussions of Release

- Also – both *Acts* stipulate that it is **not** an offence under the *Act* to disclose information unless such disclosure was contrary to the *Act*.
- Both *Acts* provide for emergency release, therefore it would not be contrary to *Acts*.
- Further, even if the release was done in error:
 - *ATIPPA, 2015* requires the act to be wilful, and
 - *PHIA* requires proof that the custodian did not take all reasonable steps to prevent the contravention before release or failure to protect becomes an offence.



Remember

- Use common sense
- Privacy Principles still apply:
 - Collect, use and disclose the minimum information necessary.
 - Avoid publicly identifying individuals unless absolutely necessary; may stop others from coming forward.
 - Instead, provide details such as location, time period impact and date to assist in identifying others that may have been exposed.
 - Safely transmit the required information using methods appropriate to the sensitivity of the information being shared.



To Summarize

- In an emergency, privacy should not be considered a barrier; it should also not be used as an excuse for inaction.
- Inform the appropriate people as soon as possible if you learn about a significant risk to health or safety.
- Take reasonable security measures to protect personal information.



Scenarios - 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 reputable public health official on official business contacts Town/City Hall seeking confirming of the civic address of a resident.
 - In the first scenario, there is no authority to provide the information. In the second, there is a legislative 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 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).



Questions



- If you have questions about this slide deck, please contact the OIPC:
 - 709-729-6309; toll free 1-877-729-6309; or commissioner@oipc.nl.ca
- Custodians can also contact the Department of Health and Community Services (see their [PHIA Resource Page](#))
- Public bodies can also contact the [ATIPP Office](#), Department of Justice and Public Safety.
- If you have questions about COVID-19, see the Department of Health and Community Services' [resource page](#).



Other Resources

- ATIPP Office's [Guide to Privacy in an Emergency](#)
- Office of the Privacy Commissioner of Canada's [Privacy and COVID-19 Outbreak](#)