Guide to Privacy in an EMERGENCY

ATIPP Office
Department of Justice and Public Safety
May 2017

Introduction

In an emergency situation, information often must be collected or disclosed quickly. Privacy legislation should not stand in the way of saving a life or providing vital assistance to someone in need. This guide sets out what the *Access to Information and Protection of Privacy Act, 2015* *(ATIPPA, 2015)* says about collecting and disclosing information in an emergency.

Please contact the ATIPP Office if:

- you have any questions about this Guide,
- you want to find out more about privacy, or are interested in training on privacy, or
- you are interested in conducting a Privacy Impact Assessment of your emergency program.

The ATIPP office can be reached by phone, email or mail:

4th Floor, East Block
Confederation Building
P.O Box 8700 Station A
St. John's, NL A1B 4J6
Tel: (709) 729-7072
Tel: (877) 895-8891
Fax: (709) 729-2129
atippoffice@gov.nl.ca
www.atipp.gov.nl.ca

We wish to acknowledge the Office of the Privacy Commissioner of Canada and the privacy oversight offices that were involved in developing the Privacy Emergency Kit. Their document was an invaluable guide in developing this Guide to Privacy in an Emergency for Newfoundland and Labrador public bodies.

What is an Emergency?

The *Emergency Services Act* defines emergency as:

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

Some examples include:

- A pandemic
- A flood
- A major fire
- A terrorist attack
- An environmental disaster

They may also include personal situations of an urgent nature including:

- A missing person
- The public must be warned about a dangerous individual who has escaped from prison
- An individual has threatened to harm themselves and requires emergency assistance
- A person is in danger and requires immediate assistance

What is considered an emergency may vary depending on the size, infrastructure or location of a community.

This Guide

This guide applies to public bodies subject to *ATIPPA, 2015*, including government departments, agencies, boards, commissions, health authorities, educational bodies and municipalities.

This guide covers:

- Collecting personal information in an emergency
- Using and disclosing personal Information in an emergency
- Before, during and after an emergency

This guide also covers situations where there is no formal emergency but there is an urgent need to collect, use or disclose personal information.

Collecting Personal Information in an Emergency

What *ATIPPA, 2015* says about collecting information in an emergency

Under most circumstances, *ATIPPA, 2015* requires that personal information be collected directly from an individual. However, the Act says that information may be collected from someone else where:

> *Collection of the information is in the interests of the individual and time or circumstances do not permit collection directly from the individual*

Example

A landslide has made the ground in a community unstable and several streets must be evacuated. You contact the town office in the community and ask for a list of individuals who reside on those streets, so you can confirm they have all been evacuated.

Under normal circumstances, information should be collected directly from the individuals. However, in this situation you need to act quickly in order to act in the interests of these individuals. So it is reasonable to collect information from the town.

Using and Disclosing Information in an Emergency

In an emergency, you may need to disclose personal information in order to inform the public or assist individuals. For example, a town may need to disclose a list of residents to an organization which plans to evacuate a neighborhood.

Disclosure of Information in Public Interest:

Where it is in the public interest, public bodies must, without delay, disclose information about:

- a risk of significant harm to the environment
- a risk of significant harm to the health and safety of the public
- a risk of significant harm to a group of people

Examples:

An oil spill off the coast of Newfoundland and Labrador creates a major environmental disaster

Pollutants have been detected in the water of a town which could be harmful to residents

A series of violent break and enters have occurred in a particular area of a community

Disclosing Personal Information in an Emergency

In most circumstances, public bodies should be cautious about releasing an individual's personal information. However, in emergency situations you may need to release personal information that you normally would not. *ATIPPA, 2015* allows this.

Personal information can be disclosed where:

> *There are compelling circumstances affecting a person's health or safety and notice of disclosure is given in the form appropriate in the circumstances to the individual the information relates.*

So that the next of kin or a friend of the injured, ill or deceased individual may be contacted

To the surviving spouse or relative of a deceased individual where, in the opinion of the head of the public body, the disclosure is not an unreasonable invasion of the deceased's personal privacy

Examples:

An individual is missing and there are concerns about their health. You release personal information about them in order to ask for the public's assistance in finding them.

An individual has been injured on the job and taken to hospital. You ask their co-workers if they know the name and/or contact of the person's next of kin.

Before, During and After an Emergency

An emergency situation is not the time for a detailed analysis of your privacy practices. However, if you have policies in place in anticipation of an emergency, you can incorporate privacy practices at that time.

Before an emergency arises, it is important to do the following:

- identify and understand your legislative authority to disclose personal information and under what conditions
- draft policies and procedures to help staff know what they need to do when they receive a request for personal information from a public body, organization, individual or the media
- consider doing a Preliminary Privacy Impact Assessment on emergency plans or policies. This process is not required, but may help ensure you are following privacy best practices. For more information, please contact the ATIPP Office
- establish a framework to help guide staff in making decisions and in exercising their discretion in disclosing personal information
- ensure personal information you have is accurate, complete and up to date
- develop information sharing protocols, where necessary, with partners who you will work with in times of an emergency, including
    - start and end dates
    - who will have access to personal information
    - how information will be disclosed, who has authority to disclose information and who must authorize disclosures
    - restrictions on information to be disclosed (i.e. information that relates directly to the emergency)
    - information security and how information will be transferred or transmitted
    - destruction/disposal of personal information, including retention timelines
- train your staff to respect privacy in emergency situations
- consider having staff sign confidentiality agreements

During an emergency, you should follow these steps:

- consult your policies and procedures and the decision-making framework which will help you make decisions on if, when and how personal information can be shared
- be ready to make quick decisions in deciding to share personal information in an emergency
- understand your public body's function – it is reasonable to share personal information to carry out your public body's business
- ask questions before sharing information, if there is no information sharing agreement in place with another organization
    - ask the reason(s) the organization is asking for the personal information and its authority for doing so
    - limit how much information you disclose – clarify what information they need and provide only what is needed for emergency purposes
    - clearly explain that the personal information being shared is related to the emergency at hand and should only be used for this purpose
    - ask that organizations handle the personal information they receive with care – the more sensitive the information, the more care should be given
    - when sharing personal information, ensure it is done securely to minimize risk of privacy breaches
- document disclosures of personal information, where possible – this will provide a record of what information was shared, when, to whom, the purpose for disclosure, who authorized the transfer, the legislative authority and any restrictions on how the information was to be handled, retained or returned
- notify individuals of any disclosures, where possible, either prior to or as soon as possible after the information is disclosed

After an emergency, consider:

- notifying individuals of any disclosure of their personal information - If you disclosed personal information because there were compelling circumstances, you should notify those individuals that their information was disclosed
- who received personal information and the amount of personal information that was disclosed
    - Was it appropriate?
    - Should any policies be changed or updated?
    - Are there any ways that you need to better prepare staff to protect privacy in an emergency?
- whether personal information was kept secure during the emergency
    - Was any information lost or stolen?
    - Consider whether you need to report any privacy breaches, and consider whether there were ways to better secure information in the future
- consulting your policies and procedures on resuming normal information handling practices
- updating policies and procedures based on experiences and lessons learned during the emergency, as appropriate

Top Tips

- In an emergency, privacy concerns should NOT stop you from assisting someone.
- Inform the people as soon as possible if you know about a significant risk to the environment, health or safety.
- You CAN disclose personal information where there are compelling circumstances affecting someone's health and safety.
- You CAN disclose personal information in order to contact the relative or friend of someone who is injured, ill or deceased.
- If you are trying to assist someone in an emergency, you CAN collect their personal information from someone else.
- Take reasonable security measures to protect personal information. What is reasonable is not black and white and will depend on the circumstances.
- Make a greater effort to protect sensitive personal information such as financial or medical information. This information should only be disclosed to other people if it is clearly necessary to do so.