Privacy Emergency Kit

May 2013

Office of the Privacy Commissioner of Canada

Uncertainty around the sharing of personal information in an emergency situation can result in unnecessary confusion and delays. The consequences of failure can be significant. This has been documented in reviews of the handling of situations such as the Asian Tsunami in 2004 and Hurricane Katrina in 2005.

Privacy laws should not be considered a barrier to appropriate information sharing, nor should they be used as an excuse for inaction. There is a variety of public and private sector privacy legislation at the federal, provincial and territorial levels. These laws govern the collection, use and disclosure of personal information and all of them contain provisions to allow for the sharing of personal information in the event of an emergency.

This guidance is aimed primarily at decision-makers in organizations that are subject to federal privacy laws, but the practices outlined here are largely applicable to organizations in other jurisdictions.

This guidance was developed by the Office of the Privacy Commissioner of Canada in consultation with the privacy oversight offices in Alberta, British Columbia, Manitoba, New Brunswick, Newfoundland and Labrador, Northwest Territories, Nova Scotia, Nunavut, Ontario, Prince Edward Island, Saskatchewan and Yukon. It was developed following the *Resolution on Data Protection and Major Natural Disasters*, which was adopted at the 33rd International Conference of Data Protection and Privacy Commissioners in November 2011.

The purpose of the guidance is to help organizations enhance the timeliness and content of communications during an emergency while giving people confidence that their personal information will be handled appropriately. It contains:

- Frequently Asked Questions About Emergencies and Legal Authorities for Sharing Personal Information
- Before an Emergency: A Checklist for Appropriate Handling of Personal Information
- During an Emergency: A Checklist for Appropriate Handling of Personal Information
- After an Emergency: A Checklist for Appropriate Handling of Personal Information
- Privacy in the Time of a Pandemic: Fact Sheet for Employees (October 2009)
- Privacy in the Time of a Pandemic: Guidance for Employers (October 2009)

Acknowledgements

We would like to thank the Office of the Privacy Commissioner of New Zealand and the UK Information Commissioner's Office for the reference materials they shared with us as well as the Office of the Victorian Privacy Commissioner for their Information Sheet on Emergencies and Privacy (January 2010) which we have adapted to the Canadian context.

Frequently Asked Questions about Emergencies and Legal Authorities for Sharing Personal Information

1. What's an emergency?

In 2011, federal, provincial and territorial Ministers approved the second edition of An Emergency Management Framework for Canada, which defines an emergency as "a present or imminent event that requires prompt coordination of actions concerning persons or property to protect the health, safety or welfare of people, or to limit damage to property or the environment." Emergencies can be natural, technological or human-induced; examples include floods, earthquakes, hazardous material spills, cyber security incidents, pandemics and terrorism.

2. Who's in charge

Within Canada's constitutional framework, the provincial and territorial governments and local authorities provide the first response to the vast majority of emergencies. The federal and provincial/territorial governments have complementary roles in emergency management, and each jurisdiction has emergency management legislation articulating its responsibilities. If an emergency threatens to overwhelm the resources of any individual province/territory, the federal government may intervene at the specific request of the province/territory. Local governments bear a large part of the responsibility for emergency management because of delegated authority and because they are often closest to the event.

Under the *Emergency Management Act*, Public Safety Canada is responsible for exercising leadership relating to Emergency Management in Canada by developing programs, policies and activities in support of emergency management. As such, a variety of resources on emergency management have been developed. The federal response for events affecting the national interest is coordinated by the Government Operations Centre (GOC) on behalf of the Government of Canada. The GOC fulfills its role by providing the Government of Canada and emergency management organizations at the federal, provincial and territorial levels with 24/7 watch and early response, national-level situational awareness and inter-jurisdictional response coordination.

A Pan-Canadian Public Health Network was established by Canada's federal, provincial and territorial Health Ministers in 2005 to help governments work together on public health issues, strengthen Canada's public health capacity and respond to public health events and threats.

3. Are there laws that deal with sharing personal information by government institutions in an emergency?

Yes. Whether it is at the federal, provincial or municipal level, there is typically an exception to consent in privacy legislation that allows disclosure of personal information without consent where "required" or "authorized" by law. "Public interest" disclosure provisions give authority to disclose records where there are specific grounds to believe it is in the public interest to do so.

In order to determine the specific rules and exceptions that apply for lead agencies and assisting organizations in an emergency, it is best to verify the consent requirements of your particular jurisdiction. The rules for

disclosing personal information under the federal *Privacy Act* and under the *Personal Information Protection and Electronic Documents Act* (*PIPEDA)* in an emergency situation are set out in sections 3(a) and 3(b) below.

Local governments often have emergency measures/management bylaws that would include authorities to collect, use and disclose information, including personal information. For example, municipal by-laws may include authority to:

- prepare lists of fatalities, casualties and missing persons;
- co-ordinate response with victims, including families of deceased persons;
- co-ordinate care for persons with special needs;
- identify persons/organizations to contribute to emergency response;
- notify next of kin in the event a municipal employee is injured, missing or killed; and
- identify persons/organizations to receive recognition for contributions to emergency response.

Medical officers of health may have extraordinary powers that override privacy legislation in a pandemic. Also, public health acts may have provisions which override privacy laws in an emergency.

At the federal level, the *Emergency Management Act* of 2007 covers information sharing with other levels of government as well as the private sector. Among other things, the legislation addresses a challenge of modern emergency management by giving the Minister of Public Safety authority to facilitate the authorized sharing of information in order to enhance emergency management. The Department of Public Safety and Emergency Preparedness Act allows the sharing of information to promote public safety objectives.

The Canadian Radio-television and Telecommunications Commission (CRTC) has developed an approach to implement both emergency alert services and telephone-based community notification services. For example, the CRTC has determined that it is in the public interest to allow public authorities to use the telephone numbers and associated addresses contained in 911 databases to improve the effectiveness of telephone-based emergency public alerts, also known as community notification services.

a) How can personal information be disclosed under the federal Privacy Act in an emergency?

The federal *Privacy Act* requires approximately 250 federal government agencies to respect the privacy rights of individuals for the collection, use and disclosure of their personal information.

While obtaining the individual's consent for the disclosure of their information is the general rule, the federal *Privacy Act* is not a barrier to appropriate sharing of personal information by federal government institutions in an emergency where consent cannot be obtained. Section 8 of the *Privacy Act* outlines certain express exemptions which allow for disclosure without consent, for example, for any purpose that is in accordance with any Act of Parliament or regulation.

The *Privacy Act* also allows for "public interest" disclosures of personal information in limited circumstances. Section 8(2)(m) of the Act permits "disclosure of personal information without the consent of the individual where, in the opinion of the head of the institution: (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure; or (ii) disclosure would clearly benefit the individual to whom the information relates."

The broad discretion to disclose in the public interest lies with the head of the government institution. In making this determination, the head must weigh the public interest in disclosure relative to the invasion of

privacy that could result from the disclosure. The exercise of such discretion must be made in good faith, in accordance with principles of natural justice and based on considerations that are related to the statutory purpose.

Although the federal *Privacy Act* specifies that the federal institution needs to notify the Privacy Commissioner in advance of the public interest disclosure, it also recognizes that in certain matters, time is of the essence. Where it is not reasonably practicable for the head of the government institution to inform the Commissioner before the purported disclosure, notification to the Commissioner must be made as soon as possible after the fact.

b) How can personal information be disclosed under Personal Information Protection and Electronic Documents Act *(PIPEDA) in an emergency?*

PIPEDA is federal privacy legislation that applies to the private sector. There is substantially similar legislation to PIPEDA in Alberta, British Columbia, Quebec. There is also substantially similar legislation, with respect to health information custodians, in New Brunswick, Newfoundland and Labrador and Ontario.

In general, disclosing personal information under PIPEDA should be done only with the knowledge and consent of the individual.

Exceptionally, Section 7 of PIPEDA identifies several specific situations where information may be collected, used or disclosed without the knowledge or consent of the individual. For example, the organization may disclose to a government institution if the institution has made a request for the information, identified its lawful authority to obtain the information and the disclosure is requested for the purpose of administering any law of Canada or a province (Section 7(3)(c.1)(iii)).

In addition, an organization may disclose personal information without consent of the individual to a government institution, a part of a government institution, or the individual's next of kin or authorized representative if it is necessary to identify the individual who is injured, ill or deceased. If the individual is alive, the organization has to inform the individual in writing without delay that the disclosure took place (section 7(3)(d.4)).

The more specific "health and security" disclosure provision in section 7(3)(e) of PIPEDA is fairly narrow. This provision allows a disclosure without an individual's knowledge or consent "to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure."

c) How do provincial and territorial privacy laws apply in an emergency?

Several privacy oversight offices across Canada have developed materials to explain how the privacy laws in their jurisdictions apply with respect to the protection of personal information in an emergency.

To be directed to this information, please follow the links provided by each jurisdiction: Alberta, British Columbia, Manitoba, New Brunswick, Newfoundland and Labrador, Northwest Territories, Nova Scotia, Nunavut, Ontario, Prince Edward Island, Saskatchewan and Yukon.

Before an Emergency
A Checklist for Appropriate Handling of Personal Information

☐ 1. Identify legislative authorities.

Understand your legislative authority to disclose and under what conditions.

☐ 2. Draft a policy and procedures.

This will help staff know what they need to do when confronted with a request for personal information from a government body, non-governmental organization, individuals or the media.

- ☐ **Specify the purposes:** If your organization wishes to be in a position to notify an individual's friends and family about their loved ones in emergency or disaster situations, you should include this purpose in your list of purposes for which personal information can be used or disclosed and communicate this fact to your customers/clients through your consent forms and privacy policy. This will provide greater flexibility to disclose personal information to family members and others on compassionate grounds in cases where the narrow conditions for exceptional disclosures cannot be met.

- ☐ **Treat sensitive personal information with added care:** Recognize that sensitive personal information, such as health or financial information, should be handled with additional precautions (e.g. additional scrutiny with respect to limiting purposes for using the information, ensuring secure storage, etc.).

- ☐ **Verify the requirements of your particular jurisdiction for disclosing information about an individual who is deceased:** Privacy laws often set out rules governing the ability to act on behalf of the deceased person. Note that there may still be a consent requirement for the sharing of personal information even if it relates to a deceased person.

  For example, the federal Privacy Act, which applies to federal government institutions, gives the administrator of the estate certain rights but only for the purposes of administering the estate (Section 10 of the *Privacy Regulations*.)

  PIPEDA currently does *not* provide a specific exception that would allow disclosure of personal information to the family of a deceased individual on compassionate grounds. The exception only applies if/where a person's life, health or security is in danger.

☐ 3. Establish a decision-making framework.

Include a decision-making framework on the release of personal information, in line with the organization's broader emergency policy, to cover legislative requirements and to help guide the exercise of discretion in disclosing personal information.

☐ 4. Ensure the quality of your information.

Take steps to ensure personal information held by your organization is accurate, complete and up to date – so it will be of maximum assistance during an emergency.

☐ 5. Establish information sharing protocols where necessary.

If your organization may be in a position to offer assistance, you could establish information-sharing arrangements with emergency management organizations (e.g. a local government organization) to coordinate action within the limits of the applicable legislative authority.

There are several resources that can be consulted on developing information sharing agreements, such as the federal Treasury Board Secretariat's Guidance on Preparing Information Sharing Agreements Involving Personal Information and the Government-to-Government Personal Information Sharing Agreements Guidelines for Best Practice, developed by the Privacy Subcommittee on behalf of the Public Sector CIO Council.

Disclosing organizations should consider the following elements in developing a protocol for data sharing in an emergency:

- ☐ **Set start and end dates:** Be clear about the period during which the data sharing arrangements will be in place and set a clear end date.
- ☐ **Establish who else will have access:** Define and limit the other organizations with which personal information is to be shared. Ensure that the requesting emergency authority explains its reasons for seeking the information.
- ☐ **Set out the decision-making framework:** Based on the authorities for disclosure, establish how the information will be disclosed and who must authorize it.
- ☐ **Identify the personal information data elements that need to be shared at each stage of the authorization process:** This will ensure that what is shared is only what is required for the purpose.
- ☐ **Restrict disclosures to those purposes which relate *directly* to the emergency:** Clarifying how much information is necessary, and tailoring the disclosure to the actual purpose, helps both the disclosing organisation and receiving organisation.
- ☐ **Request that the information be kept separately from the receiving organisation's existing systems.** This will allow it to be securely archived and/or disposed of when no longer needed to respond to, or recover from, the emergency.
- ☐ **Ensure the security of the information:** Specify that the personal information must be secure while in transit and kept securely stored once received (e.g. encryption, technical and administrative access controls.)
- ☐ **Address destruction/disposal:** Set a regime for destruction/disposal of the personal information once the information is no longer needed, in compliance with legislative obligations.

- **Enable access and correction rights:** Establish procedures for allowing individuals to access and, where necessary, correct their personal information.

- **Identify someone to answer questions and respond to complaints:** Ensure there are policies and procedures to handle complaints and the process by which individuals and the Privacy Commissioner will be notified if there is a privacy breach.

6. Train your people how to respect privacy in an emergency situation.

Provide training to the emergency response organization on privacy generally, but also specifically on how to deal with privacy in an emergency situation.

Including personal data sharing scenarios in your broader emergency training plans will help your organization develop a better understanding of the decisions that may need to be made and how to apply the relevant policies and procedures.

7. Consider how you will make the transition from the official end of an emergency to the resumption of normal information handling practices.

Establish procedures to deal with the transition period between the official end to the emergency and the resumption of normal information handling practices. Consider that, when the official emergency period ends, it is unlikely to mean an end to the extraordinary circumstances facing the people, businesses and agencies affected.

During an Emergency
A Checklist for Appropriate Handling of Personal Information

☐ 1. Consult your privacy policies and procedures and use the decision making framework.

Follow your policy and procedures and use the decision-making framework established before the emergency to help guide decisions and actions. Identify and locate the individuals in your organization who have the appropriate delegated authority to release personal information in exceptional circumstances.

☐ 2. Be responsive and ready to act.

Not all situations can be planned for and you may decide or be asked to share personal information in situations that are not governed by the usual rules and procedures. Remember, it is reasonable to share health information to carry out a statutory function (like being a first responder) or helping the individual when they are not able to give consent.

For example, someone's family or friends may ask you whether their loved one was affected by, or escaped, the incident or perhaps their whereabouts. If your organization has included this purpose in the list of purposes for which personal information can be used, it will provide you with flexibility to respond in such situations.

☐ 3. Where there is no information sharing protocol in place, get answers on key information handling questions before disclosing to another organization.

Ideally, you would have an information sharing protocol in place with the organization requesting information, but this is not going to be possible in all situations. Before disclosing personal information:

- ☐ **Ensure the organization explains its reasons for seeking the personal information and its authority to do so.** This will give your organization added confidence about making the disclosure under your decision-making framework.

- ☐ **Minimize the disclosure:** Clarify how much personal information is necessary, and tailor the disclosure to the actual purpose to minimize the amount of personal information to be disclosed. Disclosures of personal information should be restricted to those purposes which relate *directly* to the emergency. This should reflect the approach of your information sharing/privacy plan.

- **Limit the purposes of its use:** Ensure that recipients of the information clearly understand that the personal information is being disclosed for limited purposes related to an emergency only.

- **Ensure sensitive personal information will be treated with additional care:** Sensitive personal information, such as health or financial information, should be treated with additional precautions (e.g. additional scrutiny with respect to limiting purposes for using the information and ensuring secure storage).

- **Address security:** Ensure that the personal information will be transmitted and stored securely to protect it from misuse, loss, unauthorized access, modification or disclosure.

4. Make an effort to document any disclosures of personal information.

Where possible, make a record of any disclosures:

- the personal information that was disclosed;

- when it was provided;

- to whom it was given;

- the purposes for which it was disclosed;

- who authorized the transfer;

- the legislative authority under which it was provided; and
- any restrictions on how it is to be handled later, such as how long it is to be retained and whether it is to be returned.

5. Notify individuals of any disclosures.

Where possible, notify individuals, or next of kin, in writing about personal information disclosed, for emergency purposes, prior to or as soon as possible thereafter.

After an Emergency
A Checklist for Appropriate Handling of Personal Information

When the official emergency period ends, this is unlikely to mean an end to the extraordinary circumstances facing the people, businesses and agencies affected. However, it may be difficult to determine the length of time required to keep on following emergency procedures related to data sharing.

☐ 1. Consult your privacy policies and procedures on resuming normal information handling practices.

Follow the procedures your organization has established to deal with the transition period between the official end to the emergency and the resumption of normal information handling practices.

Organizations should be aware that they may need to continually be assessing whether an emergency exists.

Normal rules and procedures for collecting, using and disclosing personal information should resume as soon as possible following the end of the emergency, but the date should be one a reasonable person would expect in the circumstances. Notice about resuming normal rules should be widely publicized.

☐ 2. Follow up on the information you disclosed.

Make inquiries to determine whether the information was used correctly, in accordance with the legislative requirements and organizational policies.

☐ 3. Evaluate and update your policies and practices as required.

Review the policies, procedures and training, analyze how effective they were and determine whether there is any scope for improvement.

Update policies and procedures, protocols, sharing agreements and training with respect to privacy practices as required.