Protection of Privacy

Privacy Breach Protocol

March 2015

Newfoundland Labrador

TABLE OF CONTENTS

1. Introduction

The Access to Information and Protection of Privacy (ATIPP) Office has created the *Privacy Breach Protocol* to assist you in making key decisions when dealing with a privacy breach.

Each public body that collects, uses and discloses personal information is responsible for handling personal information in its custody or control. Where individual(s) are affected by a privacy breach, the public body must consider whether notification of the affected individuals is appropriate.

This protocol will guide you through decision-making steps setting out how to respond to a privacy breach:

- Contain the Breach
- Evaluate the Risks
- Notify Affected Individuals (if appropriate)
- Prevent Future Breaches

2. Privacy Breach Defined

A privacy breach occurs when there is unauthorized access, collection, use, disclosure or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of the *Access to Information and Protection of Privacy Act* ("ATIPP Act").

The most common privacy breaches occur when personal information of customers, patients, clients or employees is stolen, lost or mistakenly disclosed. For example, a privacy breach occurs when a computer containing personal information is stolen or personal information is mistakenly provided to the wrong person.

3. Responding to a Privacy Breach

Step 1: Contain the Breach

You should take immediate action to contain the breach:

- Contain the breach – Immediately stop the unauthorized practice, recover the records, and shut or correct weaknesses in physical security. If the breach is unauthorized access to an IT asset, such as a computer, server or network,

you MUST shut down the affected asset and contact the OCIO (or your IT representative) immediately.

- **Immediately contact your supervisor who will advise your departmental Executive,** including Minister and Deputy Minister; Communications Director; as well as Cabinet Secretariat, where appropriate; and your delegated Privacy Analyst in the ATIPP Office.

- **Download the *Privacy Breach Reporting Form*** from the ATIPP Office website and submit it to your Senior Privacy Analyst with the ATIPP Office and the Office of the Information and Privacy Commissioner (OIPC).

- If there is a risk of criminal harm, you should **immediately contact the RNC or RCMP**.

Step 2: Evaluate the Risks

Evaluating potential risks to affected individuals is important in order to understand the scope of the breach and how it may affect those individuals whose information was subject to a breach. In order to evaluate the potential risks, consider the following:

Personal Information Involved

- What types of information are involved in the breach? Generally, the more sensitive the information, the higher the risk.
- Can the information be used for fraudulent or otherwise harmful purposes? (Social Insurance Numbers and financial information, for example, can be used for identity theft).

Cause and Extent of the Breach

- What is the cause of the breach?
- Is there a risk of ongoing or further exposure of the information?
- How much information was collected, used or disclosed without authorization?
- How many individuals are likely to receive or have access to the information that was breached?
- Is the information protected by encryption or other means rendering it not readily accessible?
- What steps have already been taken to minimize the harm?

Individuals Affected by the Breach

- How many individuals are directly affected by the breach?

- Who was affected by the breach: employees, citizens, clients, other public bodies?

Foreseeable Harm from the Breach

- Is there any relationship between the unauthorized recipients and the information involved in the breach?
- What is the risk of harm to **affected individuals** as a result of the breach?
    - security risk (e.g. physical safety)
    - identity theft or fraud
    - loss of business or employment
    - hurt, humiliation, damage to reputation or relationships
- What is the risk of harm to the **public body** as a result of the breach?
    - loss of trust in the public body or organization
    - loss of assets
    - financial exposure
    - contractual and/or other legal obligations (contact your solicitor)
- What is the risk of harm to the **public at large** because of the breach?
    - risk to public health
    - risk to public safety

Step 3: Notification

A key consideration in deciding whether notification is necessary should be the mitigation of harm to any individuals whose personal information has been inappropriately collected, used or disclosed as a result of the breach.

Notify the ATIPP Office and the OIPC

When a privacy breach occurs, you must notify and submit a privacy breach reporting form to:

- The ATIPP Office - send to the Senior Privacy Analyst assigned to your public body. If you are unsure who the Senior Privacy Analyst assigned to your public body is, please send the form to the ATIPP Office by email (ATIPPOffice@gov.nl.ca); fax (729-2226) or contact the Office by phone (729-7072 or 1-877-895-8891).
- The OIPC - send the report by email (commissioner@oipc.nl.ca); fax (729-6500) or contact the Office by phone (729-6309 or 1-877-279-6309)

Notify Affected Individuals (if required or appropriate)

If there is a risk of significant harm cause by the breach, you are required to notify the individuals affected. When determining if notification is required or appropriate, consider the questions below:

Questions to Consider	Yes	No
Contractual and/or legal obligations Do you have contractual and/or legal obligations to notify affected individuals in the case of a privacy breach or loss of data?	☐	☐
Sensitivity of personal information breached Would a reasonable person consider the information breached to be sensitive? Some examples include:		
Medical information	☐	☐
Allegations relating to a crime	☐	☐
Criminal record	☐	☐
Employment or educational history	☐	☐
Risk of identity theft Is there a reasonable risk of identity theft or other fraud for affected individuals? Please check all applicable personal identifiers involved in the privacy breach:		
Social Insurance Number (SIN)	☐	☐
Driver's License Number	☐	☐
Medicare Plan Number (MCP)	☐	☐
Other Identifying Number (Please specify) _____	☐	☐
Credit or Debit Card Number	☐	☐
Other Information that could be used for fraudulent purposes (Please specify) _____	☐	☐
Risk of physical harm Is there a reasonable risk of physical harm, stalking or harassment for affected individuals?	☐	☐

Questions to Consider	Yes	No
Risk of hurt, humiliation, damage to reputation Is there a reasonable risk of hurt, humiliation or damage to the reputation of affected individuals? *Risk to reputation may be a concern if the breach includes mental health records, medical records or disciplinary records.*	☐	☐

Notifying Affected Individuals

As mentioned above, notification of affected individuals must occur if there is risk of significant harm. Some considerations in determining whether to notify individuals affected by the breach include:

- Contractual and/or other legal obligations requiring notification
- Sensitivity of the personal information breached
- Risks of identity theft or fraud (usually due to the type of information lost, such as Social Insurance Number and/or financial information)
- Physical harm (if the loss puts an individual at risk of being stalked or harassed)
- Risk of hurt, humiliation or damage to reputation (i.e. disciplinary or medical records)

When and How to Notify

When: If notification is to take place, it should occur as soon as possible following the breach. However, if you have contacted law enforcement authorities, you should determine from those authorities whether notification should be delayed so criminal investigation is not impeded.

How: The preferred method of notification is direct (i.e. by phone, letter or in person) to affected individuals. Indirect notification (i.e. website information, posted notices, media) should generally occur only where direct notification could cause further harm, is cost prohibitive and/or there is insufficient contact information. Using multiple methods of notification in certain cases may be the most effective approach depending on the circumstances surrounding the breach (e.g. the availability of contact information for those affected and the sensitivity of the personal information).

The tables below set out factors to consider in deciding how to notify the affected individuals.

Considerations Favoring DIRECT Notification	Check if Applicable
The identities of the affected individuals are known	☐
Current contact information for the affected individuals is available/can be obtained	☐
Affected individuals require detailed information in order to properly protect themselves from harm resulting from the breach	☐
Affected individuals may have difficulty understanding an indirect notification (due to mental capacity, age, language, etc.)	☐

Considerations Favoring INDIRECT Notification	Check if Applicable
The number of affected individuals is large making direct notification impractical	☐
Direct notification could compound the harm to the individual resulting from the breach	☐

What to Include in the Notification

The information in the notification should assist the affected individual in reducing or preventing harm that could be caused by the breach. It should include the information below:

Information Required in the Notification	Check if Included
Date of the breach	☐
General description of the breach	☐
Description of the information: Provide an overview of the information that was	☐

inappropriately accessed, collected, used or disclosed. *The information should be general and should <u>not</u> include the personal information that was breached. For example, you can say that the individual's date of birth was inappropriately disclosed, but you would not state the individual's actual date of birth in the notification.*	
Steps taken so far to control or reduce the harm	☐
Future steps planned to prevent further privacy breaches	☐
Steps the individual can take: Provide information detailing how individuals can protect themselves in light of the breach (e.g. contact credit reporting agencies to set up a credit watch, explain how to change a personal health number or driver's licence number)	☐
Organization contact information for further assistance: Provide contact information for someone within your organization who can answer questions, provide additional information and offer assistance to affected individuals	☐
Information and Privacy Commissioner: Provide OIPC contact information and notify individuals of their right to make a complaint to the OIPC	☐

Others to Contact

Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider whether the following authorities or organizations should also be informed of the breach:

Additional Notifications to Consider	Check if Applicable
Law Enforcement if theft or other crime is suspected Law enforcement may request a temporary delay in notifying individuals for investigative purposes. It is	☐

important to discuss these matters with your Privacy Analyst and departmental solicitor.	
Professional or regulatory bodies You should contact any professional or regulatory bodies, if they require notification.	☐
OCIO / IT Staff If the breach was a data breach or the result of an information technology failure, you must contact the OCIO or your appropriate IT support staff. Additional contact with third parties may be required to ensure correction or repair of a technical issue.	☐

Step 4: Prevent Future Breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, you should:

- thoroughly investigate the cause of the breach -- this could require a security audit of both physical and technical security;
- develop or improve, as necessary, adequate long term safeguards against further breaches;
- review your policies and update them to reflect the lessons learned from the investigation;
- audit at the end of the process to ensure that the prevention plan has been fully implemented; and,
- train all staff to know the organization's privacy obligations under the *ATIPP Act.*

4. ATIPP Office Contact Information

If you have any questions regarding this document, or privacy in general, please contact us:

Access to Information and Protection of Privacy Office

Office of Public Engagement

5th Floor, West Block, Confederation Building

P.O. Box 8700

St. John's, NL

A1B 4J6

Tel: (709) 729-7072

Fax: (709) 729 -2226

Toll Free: 1-877-895-8891

Website: http://www.atipp.gov.nl.ca/