Office of the INTEGRITY COMMISSIONER New Brunswick

Bureau du COMMISSAIRE À L'INTÉGRITÉ Nouveau-Brunswick

PRIVACY BREACH REPORTING FORM

***Right to Information and Protection of Privacy Act* (RTIPPA)**

A privacy breach occurs when there is an unauthorized access, use, disclosure or disposal of personal information in the custody of or under the control of a public body. Under the recent amendments to the *Act* and Regulation 2010-111 that came into effect on April 1, 2018, public bodies are now required to notify the affected individuals and the Commissioner's Office of privacy breaches in certain circumstances. We ask that public bodies under the *Right to Information and Protection of Privacy Act* use this form to report a privacy breach to our Office.

WHEN YOU DISCOVER A PRIVACY BREACH:

- Step 1: Contain the Breach
- Step 2: Evaluate the Risks
- Step 3: Notification
- Step 4: Prevention

The first three steps should be undertaken immediately upon discovery of the breach or in very quick succession. Regarding Step 3: Notification and as per s. 4.2(4) of Regulation 2010-111 under the *Act* requires public bodies to notify the individual to whom the information relates and the Commissioner's Office as soon as possible if it is reasonable in the circumstances to believe that the breach creates a risk of significant harm to the affected individual(s). If a public body is unsure whether it is required to notify the affected individual(s) of a privacy breach, please contact us and we will to provide guidance and assistance.

Regarding Step 4: Prevention, this is undertaken once the cause of the breach is known with a view to find and implement longer term solutions to prevent the possibility of a similar breach occurring again in the future.

TO REPORT A PRIVACY BREACH:

- Step 1: Complete this form.
- Step 2: Send the form by fax: 506.453.5963, email: aip-aivp@gnb.ca or regular mail: 230-65 Regent Street, Fredericton, NB E3B 7H8.
- If you have questions, please call us at: 506.453.5965 or 1.877.755.2811 (toll-free).

This form is adapted in part from material prepared by the Office of the Information and Privacy Commissioner for Nova Scotia, "Key Steps to Responding to Privacy Breaches" available online at:

https://foipop.ns.ca/sites/default/files/publications/Key%20Steps%20-%20Full%20-%20Final%20-%202015Oct27_0_0.pdf

and in part from material prepared by the Office of the Information and Privacy Commissioner for Newfoundland and Labrador, "Privacy Breach Reporting Form" available online at:

http://www.oipc.nl.ca/pdfs/PrivacyBreachIncidentReportForm.pdf

OFFICE OF THE INTEGRITY COMMISSIONER
Access to Information and Privacy
230-65 Regent St., Fredericton, NB E3B 7H8
☎ 506.453.5965/877.755.2811 🖷 506.453.5963
aip-aivp@gnb.ca
www.oic-bci.ca

PUBLIC BODY INFORMATION

Name of public body: _____

Contact information (address, telephone number): _____

_____

Contact name and title: _____

Contact's telephone number: _____

Contact's e-mail address: _____

DESCRIPTION OF THE BREACH

What kind of privacy breach occurred? Select all that apply:

- ☐ Unauthorized access to personal information
- ☐ Unauthorized use of personal information
- ☐ Unauthorized disclosure of personal information
- ☐ Unauthorized disposal of personal information
- ☐ Other (please describe):_____

_____

_____

_____

Briefly describe what happened:

_____

_____

_____

_____

Why and how did the breach occur? Please elaborate:

_____

_____

_____

_____

_____

How many individuals are affected by the breach? _____

Format of information involved:

☐ Electronic records: _____

☐ Paper records: _____

☐ Verbal/oral information _____

Date of breach: _____

Date breach was discovered: _____

How was the breach discovered? _____

_____

_____

_____

_____

_____

Location of breach: _____

Type of personal information involved:

- ☐ Name, address, date of birth, etc.: _____
- ☐ Employment information: _____
- ☐ Information about what programs or benefits a person is participating in or receiving: _____
- ☐ Payment or financial information: _____
- ☐ Other, please specify type:_____

CONTAINMENT

Please list the immediate steps taken to contain the breach:

_____
_____
_____
_____
_____

If the information was lost, misplaced or misdirected, was the information found or retrieved? ☐ **Yes** ☐ **No**

Is there any reason to believe that the information was copied or shared? ☐ **Yes** ☐ **No**
Please explain.

_____

Is there a potential that the breach could lead to further privacy breaches? ☐ **Yes** ☐ **No**
Please explain.

_____
_____

Applicable, have the police been notified? ☐ **Yes** ☐ **No**
If yes, who was notified and when? _____
If no, why not? _____

Which other authorities have you notified, if any, and why?

_____

_____

HARM TO AFFECTED INDIVIDUALS AND OTHERS

Please identify the types of harm that may result from the breach. Some relate strictly to the affected individual(s). Before deciding to not notify the affected individuals, please consider whether harm to the public body or other individuals could occur.

- ☐ **Bodily harm** (when the information places any individual at risk of physical harm, such as stalking or harassment)
- ☐ **Hurt, humiliation, damage to reputation or relationships** (associated with the loss of information such as employment information or financial information)
- ☐ **Loss of employment, business, or professional opportunities** (usually as a result of damage to reputation to an individual)
- ☐ **Financial loss, negative effects on a credit record**
- ☐ **Identity theft** (more likely when the breach includes loss of name, contact information, date of birth, Drivers' license number, etc.)
- ☐ **Damage to or loss of property**
- ☐ **Breach of contractual obligations** (contractual provisions may require notification of third parties in the case of a data loss or privacy breach)
- ☐ **Future breaches due to technical failures** (consider involving IT professionals if appropriate to prevent a future similar breach)
- ☐ **Failure to meet professional standards or certification standards** (notification may be required to a professional regulatory body or certification authority)
- ☐ **What is the level of sensitivity of the information involved in the breach?** _____
- ☐ **What is the probability that the personal information involved in the breach has been, is being, or will be misused?** _____
- ☐ **Other** (specify)

  _____

  _____

NOTIFICATION

Have the affected individuals been notified? ☐ **Yes** ☐ **No**

If yes, please describe how and when they were notified:

_____

_____

_____

If no, why not? _____

_____

WHEN AND HOW TO NOTIFY

When: Notification should occur as soon as possible following a breach. If you have contacted law enforcement authorities and have concerns about whether notification should be delayed in order not to impede a criminal investigation, please contact us.

How: The preferred method is direct: by phone, letter, email, or in person. Indirect notification via your website, posted notices in your offices, or published in the local media should generally only occur when direct notification could cause further harm, is prohibitive in cost, or contact information for the affected individuals is lacking. Using multiple methods of notification in certain cases may be the most effective approach.

Considerations Favouring <u>Direct</u> Notification	**Check if Applicable**
The identities of individuals are known	
Current contact information for the affected individuals is available	
Individuals affected by the breach require detailed information in order to properly protect themselves from the harm arising from the breach	
Individuals affected by the breach may have difficulty understanding an indirect notification (due to mental capacity, age, language, etc.)	
Considerations Favouring Indirect Notification	
A very large number of individuals are affected by the breach, such that direct notification could be impractical	
Direct notification could compound the harm resulting from the breach	

SAFEGUARDS

Describe the physical, administrative, and technical safeguards currently in place to protect the personal information in your custody and control relevant to this breach:

☐ **Locked doors**
☐ **Locked filing cabinets**
☐ **Alarm system**
☐ **Policies** (please attach a copy)
☐ **Procedures** (please attach a copy)
☐ **Guidelines** (please attach a copy)
☐ **Training** (please describe)
☐ **Information sharing agreement** (please attach a copy)
☐ **Passwords**
☐ **Encryption**
☐ **Audit controls/access permissions**
☐ **Other:**

_____
_____
_____
_____
_____

CORRECTIVE MEASURES

Based on the cause of the breach, what corrective measures, if any, have been or will be taken to prevent similar breaches from occurring?

_____
_____
_____
_____
_____

OTHER INFORMATION

Please provide any other useful information in relation to this breach that may not be included in this breach reporting form:

_____
_____