Office of the Information and Privacy Commissioner for Nova Scotia

Guide to Privacy Breach Notification Letters

Notice to Users

This document is intended to provide general information only. It is not intended nor can it be relied upon as legal advice. As an independent agency mandated to oversee compliance with *FOIPOP*, *MGA* and *PHIA*, the Office of the Information and Privacy Commissioner for Nova Scotia cannot approve in advance any policy, practice, or proposal from a public body, municipality or custodian. We must maintain our ability to independently investigate any complaints or requests for review. The contents of this document do not fetter or bind this office with respect to any matter, including any complaint investigation or other matter respecting which the Information and Privacy Commissioner for Nova Scotia will keep an open mind. It remains the responsibility of each public body to ensure that they comply with their responsibilities under the relevant legislation.

What is the purpose of this Guide?

Over the years, our office has reviewed many privacy breach notification letters that public bodies and health custodians have sent to individuals affected by privacy breaches. We have found that most cause recipients to be confused about why they are receiving the letter, about what happened, what they are expected to do and who they can talk to. The letters regularly provide incorrect information about being able to complain directly to the Office of the Information and Privacy Commissioner at first instance.

This Guide is to assist public bodies and health custodians who have experienced a privacy breach and are considering providing notice to affected individuals, and to give meaningful notice that people will understand.

This Guide should be read in conjunction with our other tool Key Steps to Responding to Privacy Breaches.

It is important to recognize that in Nova Scotia the privacy laws do not require public bodies to provide affected individuals with notification. The *Personal Health Information Act* (*PHIA*) does have some requirements for health custodians to provide notifications. Even where the laws do not require it, public bodies and health custodians should consider notifications to be a 'best practice' and should provide them whenever there is a risk for harm or embarrassment. Without receiving a notification, affected individuals cannot protect themselves. Notification letters should inform individuals and empower them to take action.

When should individuals be notified?

Public bodies/custodians should consider the following when deciding whether to notify individuals about a breach of their information:

- Legislation requires notification – s. 69 and s. 70 of the *PHIA* for example;
- Contractual obligations require notification;
- There is a risk of identity theft or fraud – usually because of the type of information lost, stolen, accessed or disclosed, such as a SIN, banking information, identification numbers;
- There is a risk of physical harm – for example if the breach puts an individual at risk of stalking or harassment;
- There is a risk of hurt, humiliation or damage to reputation – for example when the information lost includes medical or disciplinary records;
- There is a risk of loss of business or employment opportunities – if the loss of information could result in damage to the reputation of an individual, affecting business or employment opportunities; and
- There is a risk of loss of confidence in the public body or organization and/or good citizen relations dictates that notification is appropriate.

See our tool Key Steps to Responding to Privacy Breaches for more information on assessing risk and deciding when to notify.

Notification letters are an important mitigation strategy that has the potential to benefit the public body, health custodian and the individuals affected by a breach. More importantly, prompt notification can help individuals mitigate the damage by taking steps to protect themselves.

While the contents of a notification letter may seem obvious, leaving out important details or using complicated or unclear language can exacerbate the anxiety individuals may feel after being informed of a breach of their personal information.

Below is a list of elements that should be in notification letters as well as some tips and guidance based on our past experiences with breach investigations.

What should be included in the notification?

- Date of the breach;
- Name of the public body - Include the name of the public body that has custody or control of the personal information that was breached. The breached personal information may be in the custody or under the control of more than one public body (e.g., two public bodies share a database that is hacked). In these circumstances, a good practice is to include the name of all public bodies involved in the breach.
- Description of the breach; including the time, location and who was involved;
- Description of the elements of personal information inappropriately accessed, collected, used or disclosed;
- If the breach involved an agent or contractor, name that organization and explain their role in relation to the public body or custodian and explain how and why they had possession of the individual's personal information.

Note: The specific information that was breached for each individual must be provided; often a list is provided that applies to the total scope (letters often state "Information that has been breached *may include*…). Individuals must know what specific information has been breached, not what *may* have been breached, in order to effectively mitigate the risks for themselves.

- If known, a description of possible types of harm that may come to them as a result of the privacy breach, including embarrassment or reputational harm;
- The steps the public body/custodian has taken so far to control or reduce the harm;
- Whether the breach is contained or if the information is still unsecure and the risks are ongoing;
- Where there is a risk of identity theft as a result of the breach, typically the notice should offer free credit monitoring protection as part of the mitigation strategy;
- If credit monitoring protection is being offered, consider attaching an appendix with all of the relevant information related to how to sign up and who to contact if there are problems with signing up;

- Further steps the public body/custodian plans to take to prevent future privacy breaches;
- Steps the individual can take to further mitigate the risk of harm (e.g., how to contact credit reporting agencies to set up credit monitoring, information explaining how to change a personal health number or driver's licence number);
- Contact information of an individual within the public body or health organization who can answer questions or provide further information. If this service is being contracted out, say so, and let recipients of the notification know what organization they will be communicating with;
- The public body's/custodian's complaint process, including the privacy officer's contact information, if the individual wishes to file a breach complaint with the public body/custodian.

Note: The complaint process must be clearly identified as a complaint policy distinct from general questions about the breach or a call centre resource, and that individuals must submit the complaint to the public body/custodian in writing. See "Suggested wording" below.

- The Office of the Information and Privacy Commissioner for Nova Scotia's (OIPC) website address and the fact that individuals have a right to complain to the Information and Privacy Commissioner under the *Privacy Review Officer Act* (*PRO*) and/or *PHIA*, after a complaint has been filed with and responded to by the public body or health custodian.

Note: Before individuals can file a review with the OIPC, they must complete the public body/custodian's complaint process; the OIPC does not have jurisdiction to conduct privacy breach reviews until the internal complaint process has concluded. Individuals have 60 days after receiving the public body's response to their complaint to request a review from the OIPC.

Other considerations and suggestions:

- Anticipate what questions the individuals will have, and include an FAQs as an Appendix.
- Consider who will receive the notification letter and their ability to comprehend the message and take the necessary action(s). Consider providing alternative mechanisms - not everyone has a computer or is tech savvy and some people may need assistance or other options to make contact.
- Do not provide false or misleading information.
- If you are providing contact information for other organizations, explain why. Just providing a list of numbers and websites is not enough.
- Be open, be accountable and be transparent.

- Consider providing updated information as the investigation progresses or once it is completed.
- Use headings to keep the notification letter organized and easier to read. Bold important information such at the contact information to ask questions.
- If the public body, municipality or health custodian has already contacted the Information and Privacy Commissioner, include this detail in the notification letter.
- Where appropriate, recognition of the impact of the privacy breach on affected individuals and an apology.

Suggested wording to describe the complaint and review processes:

If you wish to submit a privacy complaint because of this breach, please provide your complaint in writing to: [Privacy Officer contact info & email]

However, before you file a complaint, I encourage you to contact _____ to ask any questions you have about this breach. You may be satisfied by the information you receive, and a formal complaint may not be required.

If you make a formal written complaint but you feel the pubic body/custodian's response does not resolve the matter, you may request a review of the response to your complaint by the Office of the Information and Privacy Commissioner (OIPC).

You cannot file a privacy complaint with the OIPC first. You must file your privacy complaint with the public body/custodian first.

To request a review of the response to your complaint, you must submit a written request to the OIPC within 60 days of receiving the public body/custodian's response to your complaint.

[Information and Privacy Commissioner website]

Questions?

This document was prepared by the Office of the Information and Privacy Commissioner for Nova Scotia. We can be reached at:

Phone: 902-424-4684

Toll Free (NS): 1-866-243-1564

TDD/TTY: 1-800-855-0511

Fax: 902-424-8303