SAFEGUARD

A quarterly newsletter published by the Office of the Information and Privacy Commissioner

Volume 9, Issue 3 August 2025

Contact Information

Office of the Information and Privacy Commissioner

Mailing Address:
PO Box 13004, Station A
St. John's, NL A1B 3V8

Telephone:

709-729-6309

Toll Free in Newfoundland and Labrador:

1-877-729-6309

Email:
commissioner@oipc.nl.ca

Website:
www.oipc.nl.ca

Follow us on social media!

LinkedIn:
https://Linkedin.com/company/oipc-nl

This Issue:

Updates: New Guidance Issued

The Office of the Information and Privacy Commissioner (OIPC) has released new guidance titled "Assessing Privacy-Impactful Initiatives During Public Health Emergencies".

This guidance document combines a number of resources developed during the COVID-19 public health emergency, with updates to reflect learnings for any future public health emergencies. With this updated document, OIPC is removing three resources from our website:

- COVID-19 FAQ;
- Public Bodies Collecting Proof of Vaccination from Employees; and
- A Framework for the Government of Newfoundland and Labrador to Assess Privacy-Impactful Initiatives in Response to COVID-19.

Custodians with questions or feedback on this new resource are welcome to reach out to our Office by calling 709-729-6309 or emailing commissioner@oipc.nl.ca.

Reminder: Update your Notification Letters!

Some individuals impacted by breaches have been receiving notification letters listing our old address. Custodians are reminded that our new physical address is:

20 Crosbie Place, Beothuck Building, St. John's NL.

And our mailing address remains the same:

P.O. Box 13004, Station A, St. John's, NL, A1B 3V8.

Custodian's Response to Correction Requests

This article concludes our series that examines custodian's obligations when in receipt of access or correction requests. Our prior article, published in the May edition of Safeguard, focused on access requests, while this article focuses on correction requests.

When an individual who has been granted access to their personal health information (PHI) identifies incorrect PHI within their record, the individual is able to request a correction as per section 60(1) of PHIA. This request can be submitted in writing or verbally at no charge to the individual. It is the responsibility of the custodian to take reasonable steps to confirm the individual's identity in order to process a request to correct PHI.

As per section 62, a custodian must respond to a PHI correction request no more than 30 days after receiving it. However, a custodian may extend the time limit by an additional 30 days where:

- meeting the original due date would unreasonably interfere with the operations of the custodian, or
- the information that is the subject of the request for correction is located in numerous records so that the request cannot be completed within the original 30 days.

Should a custodian extend the original response time by 30 days, the custodian must give the requestor written notice of the extension along with reasons for the extension. A custodian must respond to the individual's request as soon as possible and no later than the expiration of the extended time limit.

Section 62 of PHIA establishes expectations of custodians when responding to correction requests. Requests for corrections must be granted where the individual making the request demonstrates that the record is incomplete or inaccurate for the purposes for which the custodian uses the information and gives the custodian the information necessary to enable the custodian to correct the record. Inaccurate information is mistaken or wrong information that doesn't reflect the true state of something (for example, the injury was to the left arm but the record states that the injury was to the right arm). Incomplete information is information that is incomplete, missing, or overlooked.

NOTE: An opinion is not incomplete or inaccurate information if it accurately reflects the views of the individual who recorded the information at the time.

When a request for correction is granted, then under section 63 the custodian must make the correction and provide written notification to the individual that it has been made. The custodian must also provide written notice of the requested correction, to the extent reasonably possible, to any person the custodian had disclosed the information within the 12 month period immediately preceding the request (for example, WorkplaceNL or a health care professional to whom a referral was made), unless the custodian reasonably believes that the correction will not impact the ongoing provision of health care or other benefits.

Custodians may refuse to make the correction if:

1. the record was not originally created by the custodian and the custodian does not have sufficient knowledge, expertise and authority to correct the record. This is a two-part test: the custodian must demonstrate that the record was not originally created by the custodian and that the custodian does not have sufficient knowledge, expertise and authority to correct the record. OIPC examined this section of the Act in Report AH-2020-001.
2. the information which is the subject of the request consists of a professional opinion or observation that a custodian has made in good faith about the individual. The custodian must meet two conditions for this to apply: the record must be a professional opinion or observation, and it must be made in good faith. OIPC examined this section of the Act in Report AH-2104-001. OIPC Saskatchewan poses the question "is this correction a substitution of opinion" in Review Report 023-2025.
3. the custodian believes on reasonable grounds that the request is frivolous, vexatious or made in bad faith.

When a custodian refuses a request to correct PHI, the custodian still has an obligation to document the request by annotating the personal health information with the correction that was requested and not made. Where practical, the custodian shall notify any person the custodian had disclosed the information within the 12-month period immediately preceding the request for correction of the annotation, unless the custodian reasonably believes that the correction will not impact the ongoing provision of health care or other benefits.

When a request to correct PHI is refused, the custodian must provide the requestor with a written notice outlining the correction that the custodian refused to make, the reasons for the refusal and the right of the individual to appeal the refusal to the courts or request a review by the Information and Privacy Commissioner.

Key Takeaways

- Custodians should have policies and procedures on the processing of correction requests.
- If granting the correction, the custodian must inform anyone they disclosed the inaccurate information to within a 12-month timeframe.
- If denying the correction, the custodian must explain why, make an annotation to the record, and must inform anyone to whom they disclosed the information within a 12-month timeframe of the request and subsequent denial.

Snooping – Identification of Snoopers

This is the second in a series of articles about snooping; the first article was featured in the May edition of Safeguard. Future articles will focus on containing and detecting snooping incidents and investigating potential snooping incidents.

Privacy legislation, including ATIPPA, 2015 and PHIA, require that public bodies and custodians protect the information in its custody or control, which includes ensuring safeguards are in place to protect information from insider threats.

When impacted individuals are notified of a snooping incident, one of the first questions asked is usually who snooped. It has traditionally been considered that release of such information would be an unreasonable invasion of personal privacy.

OIPC examined a number of snooping reports across Canada and noted that the trend is changing. In some reports, Commissioners have recommended that notification letters be re-issued with the name of the snooper, while others recommended that notification letters include information about requesting audit reports or that audit reports of all accesses be attached to the notification. Some have even recommended that employment status or disciplinary action taken as a result of the incident be released. Following are some summaries of select reports, along with links to complete reports for fuller reading.

In December 2018, OIPC PEI released Breach Report HI-18-005. This Report details the discovery of inappropriate access on the Clinical Information System database (the CIS) during a regular audit process by Health PEI. The CIS is Health PEI's electronic medical records system that digitally stores personal health information of patients.

In the summary section, the Report states, in part:

> In most circumstances individuals who interact with a health care provider should know who is accessing their personal health information. In cases of CIS snooping, affected individuals have a heightened need to know the identity of the snooper, for various reasons, but primarily to identify whether the snooper is someone with malicious intentions. The Commissioner recommended that, for any future cases of CIS snooping, Health PEI should proactively provide a copy of an excerpt of the log of accesses to an affected party's electronic personal health information on the CIS, highlighting the dates(s) and the name of the snooper.

In March, 2019, OIPC PEI released Breach Report HI-19-001. This report examined a custodian who, during an investigation about use of an employee's business email for personal use, discovered that the employee had disclosed to a family member, by email, personal health information of the Custodian's clients. Unlike the 2018 report, the Commissioner did not determine that the identity of the snooper should be disclosed, however outlines considerations from paragraphs 38-45, including:

- HIA neither requires nor prohibits custodian's from identifying the snooper;
- concerns that the snooper will obtain another position in which they will have access to personal health information;
- both the custodian and law enforcement were satisfied that the purpose of the snooper's disclosure and the Recipient's collection, was unrelated to the content of the personal health information; and
- a declaration by the Recipient and the Recipient's employer confirming the destruction of personal health information, and that the personal health information was not used or disclosed and will not be used or disclosed.

In October, 2020, OIPC Saskatchewan released Investigation Report 203-2019, 214-2019, 257-2019, which examined a physician that snooped in a clinic's EMR. The Rosetown Primary Care Centre (RPCC) is located in a building that was made available by the Town of Rosetown (the Town) and the Rural Municipality of St. Andrews No. 287. Clinic staff, such as the medical office assistants, are employed by the Town; the Saskatchewan Health Authority (SHA) provides the clinic's equipment including the electronic medical record (EMR) and contracts the physicians that work at the clinic. The physicians are billed for a portion of the cost associated with the operation of the EMR on a monthly basis and all staff and physicians at the Clinic have SHA email addresses and accounts.

An SHA investigation revealed that a physician at RPCC accessed personal health information without a professional need-to-know; the Commissioner's report concluded that **The Health Information Protection Act** did not authorize the physician's accesses to the EMR and that the SHA's notification of the privacy breaches to the affected individuals did not provide a complete accounting of what occurred.

At paragraph 68, the Commissioner states:

> My office's position is that an individual who has snooped should have a diminished expectation of privacy. Their identities and the disciplinary action taken against them should be revealed to affected individuals. The impact of a privacy breach is not standard and flat. Learning that a best friend, business partner, estranged spouse, co-worker, boss, neighbour, or a stranger snooped upon one's personal health information has different implications for individuals. Affected individuals are in the best position to understand the impacts of a privacy breach upon themselves. Knowing the identity of the snooper provides affected individuals with information to assess the harm that may result from having their privacy invaded. In my Investigation Report 100-2015, I cited the former Ontario Information and Privacy Commissioner's Investigation Report HO-010 that provided that aggrieved individuals have a right to a complete accounting of what has occurred. Aggrieved individuals will not find closure regarding the incident unless all the details of the investigation have been disclosed. Receiving general assurances that "the incident has been dealt with appropriately" falls far short of the level of disclosure that is required. Further, publicly identifying the snooper and the disciplinary action taken against the snooper would be a strong deterrent for other employees and contractors.

And at paragraph 71, the Commissioner details expectations for notification letters, stating:

> I recommend that the SHA send another letter to the affected individuals that identifies Dr. Narang as the snooper. The letter should also identify the disciplinary actions, if any, taken against Dr. Narang. Further, it should identify concrete actions taken by the SHA to prevent future incidents of snooping. For example, it should provide details of whether Dr. Narang's access to personal health information was restricted, what training Dr. Narang has undertaken so that they understand the requirements of HIPA, and how often Dr. Narang is audited. The letter should also include instructions to individuals on how they can submit a formal access to information request under HIPA for access to their personal health information in the EMR, including the audit logs of who may have accessed their personal health information. The letter should include the contact information of an SHA employee who can answer questions about this matter. Since some time has elapsed since it

> was discovered that Dr. Narang has snooped into the EMR, I recognize that the RPCC may not have the current contact information of affected individuals. As such, if the SHA does not have the current contact information for any of the affected individuals, then I recommend that the SHA post its notification of this privacy breach to its website for a period of at least 30 days. To ensure the greatest chance of affected individuals receiving the notification via the SHA's website, I recommend that the SHA post the notification to a webpage of the SHA's website that receives a lot of traffic. This can include its "News Releases" page at https://www.saskhealthauthority.ca/news/releases.

In February, 2023, OIPC NS issued Investigation Report IR23-01. This Report details breaches that occurred in the weeks following Nova Scotia's tragic mass casualty event on April 18-19, 2020. Nova Scotia Health (NSH) proactively monitored employees who were accessing the electronic health records of individuals associated with the events to ensure they had a valid reason to be viewing those records. Eight employees accessed the electronic health records of individuals without a valid purpose; follow-up investigations identified more instances of unauthorized access of additional electronic health records by six of those eight employees. Two were confirmed as 'serial snoopers' that had repeatedly abused their access to look up hundreds of individuals' sensitive personal health information without a legitimate need to do so. These employees looked up information on family, friends, children's friends, acquaintances from community organizations and sports, co-workers, neighbours, the other party in an automobile collision, former patients and persons receiving public attention or notoriety.

While the NSH notification letter did not include the name of the snooper, it did provide a phone number for individuals with outstanding questions. Individuals who called were told the identity of the snooper, as well as whether that person was actively employed by NSH at the time of the notification. The content of the letter is analyzed in paragraph 142 and the Commissioner states, in part,

> NSH's letter could have been more specific and precise in its notification, particularly where the employee viewed detailed electronic health records. The letter possibly obscured the nature and severity of the breaches because it did not name the employee. Sometimes custodians worry about causing additional privacy breaches by naming employees in letters to affected individuals in case letters are sent to the wrong individual or are intercepted. While I think that possibility is fairly remote, if that is a real concern for custodians, they need to ensure that information is supplied in some way to the affected individual. This task should not be delegated to an affected individual to call the custodian. Rather, the custodian must take the onus of informing the affected individual, either in written format or verbally.

At paragraph 144, as part of recommendation #5, the Commissioner recommends that future notifications, " …identify the name of the employee who engaged in the unauthorized access;…"

Key Takeaways

- Custodians should have a policy or procedure that addresses snooping incidents, including content of notification letters and expectations regarding the naming of the snooper.
- In case of snooping incidents, custodians should consider if notification letters should include the name of the snooper, details of how to request an audit report, or include a copy of an audit report.
- Considerations
  - Is the snooper someone with malicious intentions?
  - Is the snooper's identity necessary for impacted individuals to determine the nature and severity of the breaches?
  - Has the impacted individual asked about the identity of the snooper or raised specific concerns?
  - Does the custodian have the authority to disclose the name of the snooper, and the discipline or employment status?

The November edition of Safeguard will include a legislative analysis of audit records and the disclosure of the identity of a snooper, as well as any discipline taken, as we continue our series on snooping!

PHIA Privacy Breach Statistics: May 1 – July 31, 2025

Between May 1 – July 31, OIPC received five privacy breach notifications; this remains steady with last quarter's five breaches. The five breach reports came from two custodians.

The five breaches were:

- mis-directed correspondence by email;
- mis-directed correspondence by fax;
- an issue with verification of identity, which resulted in the overwriting of an MCP number;
- a system issue that provided a payment statement to the incorrect end user; and
- a snooping incident which impacted 29 individuals.

Want Training?

We would like to remind custodians that OIPC offers PHIA training that can be customized to their needs!

We are also available to speak at annual general meetings and other events!

Interested custodians should email OIPC at commissioner@oipc.nl.ca.

There are also a number of PHIA resources available on OIPC's website.