ᓄᓇᕗᒻᒥ ᑐᓴᐅᒪᔪᓕᕆᓂᕐᒧᑦ ᑲᙳᓇᖅᑐᓕᕆᓂᕐᒧᓪᓗ ᑲᒥᓯᓇ
Nunavut Information and Privacy Commissioner
Nunavunmi Tuhaqtauyukhaliqinirmun Kanngunaqtuliqinirmun Kamisina
Commissaire à l’information et à la protection de la vie privée du Nunavut

Commissioner’s Final Report

Report Number:	25-288-RR
CanLII Citation:	Departments of Health and Finance (Re), 2025 NUIPC 7
NUIPC File Number:	25-114
Date:	June 13, 2025

Summary

[1] The Commissioner received a complaint that the Department of Health required someone submitting a claim for medical-expense reimbursement to provide their Social Insurance Number. The Health unit asked for the SIN because the Department of Finance said it was mandatory. The Commissioner finds there was an unauthorized collection of personal information. Collection of the SIN was convenient for Finance but it was not “necessary” as required by section 40(c). The Commissioner recommends Health and Finance take certain steps to safeguard the security of the SINs they hold.

Nature of Review and Jurisdiction

[2] This is a review of a privacy breach complaint against the Department of Health. The complaint was filed under section 49.1(1) of the *Access to Information and Protection of Privacy Act* (ATIPPA). I conducted my review under section 49.2(1). My review also covers the Department of Finance, for reasons that will be explained.

[3] I have jurisdiction over the Departments of Health and Finance: ATIPPA, section 2, definition of “public body”.

Issues

[4] The issues in this review are:

a. Was there an unauthorized collection of Social Insurance Numbers?
b. Have Health and Finance made reasonable security arrangements against the risk of disclosure of Social Insurance Numbers?

Facts

[5] The Complainant is a resident of Nunavut. They were entitled to reimbursement by the Department of Health for some medical-travel expenses.

[6] The claim form provided by Health contained a box for the claimant's Social Insurance Number (SIN). The form said that providing the SIN was mandatory. The Complainant did not want to provide their SIN, because they considered it to be sensitive personal information and irrelevant to expense reimbursement. They completed the form anyway, fearing that reimbursement would otherwise be denied.

[7] After submitting the form to Health, the Complainant contacted me and asked me to review the collection of the SIN. I agreed, and proceeded under section 49.2(1). The issue raised by the Complainant applies to all claimants. This review is therefore about the GN's systems, rather than the facts of the Complainant's individual case.

[8] When a medical-travel expenses form is submitted to Health, adjudication is done by a processing unit in Rankin Inlet. If reimbursement is approved, the processing unit sends an authorization to Finance in Iqaluit. It is Finance that processes the actual reimbursement. Ultimately, it is Finance that required a claimant to provide their SIN. Health collected SINs because Finance told them to.

[9] During this review, Finance transitioned to a new enterprise resource management (ERM) system called Oracle Fusion Cloud. (Transition to the new system had been in the works for a long time. It is only coincidence that the transition occurred during this review.) The new system does not require collection of SINs for medical expense reimbursements. I am advised by Finance

that the transition of data from the old system to Oracle Fusion Cloud did not include transfer of SINs.

Law

[10] A Social Insurance Number (SIN) is issued by the federal government to Canadians for certain administrative purposes. The federal government has a detailed *Social Insurance Number (SIN) Code of Practice* that, among other things, lists permissible uses of the SIN by the federal government.

[11] It is common for the question to arise whether someone outside the federal government can ask for the SIN, and whether a citizen is required to provide it. That is a big topic. In this Review Report, I will restrict myself to the collection of SINs by Health and Finance for purposes of medical-expense reimbursement.

[12] In Nunavut, the collection of information by a public body is governed by section 40 of the ATIPPA. The relevant parts of that section read as follows:

> 40. No personal information may be collected by or for a public body unless
>
> (a) the collection of the information is expressly authorized by an enactment;
> …
> (c) the information relates directly to and is necessary for
> (i) an existing program or activity of the public body, or
> …
> ….

[13] With respect to section 40(a), Nunavut law contains several provisions expressly authorizing a public body to collect someone's SIN. For example:

a. *Family Support Orders Enforcement Act* and its regulations

b. *Vital Statistics Form Regulations*

c. *Payroll Tax Regulations*

d. *Income Assistance Regulations*

e. Student Financial Assistance Regulations

None of these provisions is relevant to medical-expense reimbursement, so section 40(a) cannot apply.

[14] That leaves section 40(c) as the only possible justification for the collection of SINs by Health and Finance. Collection of personal information is authorized only if it "relates directly to and is necessary for" medical-expense reimbursement.

[15] There are not many cases in Nunavut dealing with the meaning of the words "relates directly to and is necessary for" in section 40(c): see, for example, *Review Report 16-109 (Re)*, 2016 NUIPC 13 (CanLII); *Workers' Safety and Compensation Commission (Re)*, 2024 NUIPC 1 (CanLII) at paragraph 46. Those cases deal with medical records and are not helpful in the present context.

[16] There is only one Nunavut case dealing in a substantive way with someone's SIN: *Review Report 05-16 (Re)*, 2005 NUIPC 1 (CanLII). That case, however, deals with the disclosure of someone's SIN. It is not helpful in the present case, which is about collection of someone's SIN.

Analysis

[17] The SIN is a sensitive piece of personal information. It is a unique identifier that follows a Canadian citizen from birth to death. If a malicious actor obtains someone's name and SIN, there is an increased risk of identity theft.

[18] In the absence of express statutory authorization, a public body in the GN should not be collecting someone's SIN unless it relates directly to a program and is demonstrably necessary for the administration of the program.

[19] In this case, I have no doubt that having a claimant's SIN is convenient for Finance. They need to be able to distinguish between people with similar names, and the SIN is a convenient way to make that distinction. But section 40(c) of the ATIPPA requires more than convenience. For the reasons that follow, I find that the collection of the Complainant's SIN for medical expense reimbursement did not comply with section 40(c).

[20] Collection of SINs may comply with section 40(c) if there is an element of a program that requires verification with the Canada Revenue Agency. For example, there are several GN programs that are income-tested. Typically, the GN verifies an applicant's income by exchanging information with CRA. For that purpose, collection of the SIN goes beyond convenience. It is necessary.

[21] In this case, however, the program involves medical-expense reimbursement. There was no income-tested element. There was no need for Health or Finance to verify the information with CRA.

[22] Finance wants the SIN to ensure that payment is made to the correct recipient. The SIN, as a unique identifier, helps Finance to distinguish between recipients with similar names. That is obviously a valid objective.

[23] Finance points out, and I accept, that Inuit names can sometimes pose challenges. Inuit naming traditions are unique and important: see, for example, Pelagie Owlijoot and Louise Flaherty (eds.), *Inuit Kinship and Naming Customs* (2014). These traditions can, for example, result in people in the same household having the same or similar names.

[24] The problem, from a privacy perspective, is that sensitive personal information (the SIN) was being collected from <u>everyone</u> who applied for medical-expense reimbursement, even if there was little or no risk of confusion.

[25] Finance acknowledges that alternatives are available. A person's date of birth (DOB), in combination with their name, is a reasonably unique identifier. The Health claim form also requires the claimant's address. (There is also space for email address and phone number, but they are not mandatory.) The combination of name, DOB, and address should be enough to distinguish almost all claimants.

[26] Unfortunately, the accounts-payable portion of Finance's new ERM system is not configured as well as it could be to capture alternatives to the SIN. There is space in the system for the SIN, but, surprisingly, not for the DOB. Finance has established some workarounds, but they are not perfect. Finance tells me that some identification issues have cropped up with the new system that did not

occur when Finance was using SINs in the old system. Nevertheless, Finance is not proposing, at least for now, that it go back to collecting SINs.

Storage of SINs

[27] The Complainant also raises the issue of the storage of their SIN. From the Complainant's perspective, the GN unnecessarily collected a sensitive piece of personal information. The Complainant wants to know where it is being held, and how secure it is.

[28] The Complainant's question about security is, of course, entirely legitimate, and not just because Health and Finance collected the SIN unnecessarily.

[29] Personal information held by the GN is all too often subject to unauthorized access and use by GN employees, often referred to as "snooping": see, for example, *Department of Health (Re)*, 2024 NUIPC 15 (CanLII); *Department of Health (Re)*, 2023 NUIPC 6 (CanLII); *Department of Health (Re)*, 2020 NUIPC 5 (CanLII). Snooping is most prominent in the health context but is, unfortunately, not limited to that context.

[30] Personal information held by the GN, especially when it is not destroyed in accordance with GN records-retention schedules, may be disclosed in error: see, for example, *Department of Finance (Re)*, 2022 NUIPC 10 (CanLII).

[31] Personal information held by the GN may also be stolen during a cyberattack. The GN was subject to a widespread cyberattack in 2019, though in that case personal information does not appear to have been stolen. The same happened at Qulliq Energy Corporation in 2023. GN contractors holding the personal information of Nunavummiut have also suffered from cyberattacks. A recent attack on Nova Scotia Power may have resulted in the loss of up to 140,000 SINs: see, for example, "Thieves gain access to about 140,000 social insurance numbers in NS Power database" (CTVnews.ca, May 29, 2025). Like the GN, Nova Scotia Power used the SINs for authentication purposes, but collection of the SINs was not necessary and other, less risky methods could have been used.

[32] In Nunavut, the legal obligation of a public body regarding the storage of personal information is in section 42 of the ATIPPA:

> 42. The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

[33] This "reasonable security arrangements" standard is vague, but it is all we have. I reviewed what "reasonable security arrangements" means in two Special Reports: *Department of Finance and three other public bodies (Re)*, 2024 NUIPC 7 (CanLII) and *Department of Executive and Intergovernmental Affairs and twelve other public bodies (Re)*, 2023 NUIPC 12 (CanLII). I will not repeat that analysis here, but I adopt it for purposes of this decision.

[34] After discussions with Health and Finance, I conclude that the SINs of medical expense claimants, including the Complainant, may be currently stored in the following places:

a. Health: The email inbox of the "generic" email address used by the processing unit in Rankin Inlet. According to Health, access to this inbox is restricted according to position.

b. Health: The claimant's electronic file. Any paper copies of the form are shredded, but the electronic file is kept indefinitely. I do not have information on where precisely these electronic files are held. I assume it is on the GN network drive, which was the subject of my Special Report in *Department of Executive and Intergovernmental Affairs and twelve other public bodies (Re)*, 2023 NUIPC 12 (CanLII). Security of the Y: drive varies widely from department to department, from unit to unit, and even from folder to folder.

c. Finance: The mail inbox of the email address used by Finance to receive reimbursement authorizations from the Health processing unit in Rankin Inlet. According to Finance, access to this inbox is restricted according to position.

d. Finance: The old ERM system. Although Finance has transitioned to Oracle Fusion Cloud, the old system will be maintained for at least a couple of years for audit and verification purposes. According to Finance, access is restricted to a handful of Finance employees. Finance plans eventually to decommission the old system.

e. Finance: Hard copies. Some accounts-payable files are kept in hard copy, in locked filing cabinets (which were shown to me). According to Finance, access to this filing cabinets is restricted to a handful of Finance employees. The files are destroyed in accordance with Finance's records-retention policy. In accordance with the policy, all hard-copy files will in time be destroyed.

[35] I have been aware for some time, anecdotally and from numerous files, that many GN employees and work units use their email inbox as digital storage. This is the first Review Report in which I address the question directly.

[36] Use of an email inbox as digital storage is not, in my view, a "reasonable security arrangement", as required by section 42 of the ATIPPA. That does not mean it is completely insecure – an email inbox is as secure as the GN's overall email system. But individual email accounts are prone to all the common errors associated with email – auto-complete errors, reply-all errors, chain errors, unintended attachments, and so on. Scams of all kinds target email users and may result in a compromised email account. Users may retain access to their old emails after changing jobs. In my experience, GN users rarely use passwords or encryption for email attachments. I doubt that many GN employees or work units systematically purge their email inboxes in accordance with GN records-retention schedules. And of course GN email may fall victim to cyberattack.

[37] For all these reasons, the use of an email inbox for storage is problematic.

[38] A better method, at least in theory, is for file documentation to be extracted from emails and placed in restricted-access folders on the network drive (in the GN, the Y: drive) or equivalent. The email would then be securely deleted. If file documentation must be consulted or shared, it would be done via

the network drive. That way access would be restricted, no copies would be made, and an audit trail would be created.

[39] Unfortunately, the GN's network drive is itself rife with security issues and does not meet the "reasonable security arrangements" standard in section 42 of the ATIPPA. That was my primary finding in *Department of Executive and Intergovernmental Affairs and twelve other public bodies (Re)*, 2023 NUIPC 12 (CanLII). The GN is working towards replacement of the Y: drive with a more modern, more secure solution, but they are not there yet. I understand and accept that transitioning to the new system will take time.

[40] I am not naïve enough to believe that everyone in the GN will stop using their email inbox as their digital storage. It is so easy to do, which is why so many individuals and work units do it. All I can do is point out the privacy issues thereby created, and recommend that public bodies think about the privacy implications and tighten their controls.

A concluding comment

[41] This review is about a specific program – the Department of Health's medical expense reimbursement program. The principle, however, applies to any GN program for which SINs are collected.

[42] All GN units that collect SINs need to take a hard look at whether collection of the SIN is really necessary, as required by section 40(c) of the ATIPPA. The best way to keep safe the SINs of Nunavummiut is not to collect them at all. If GN units do need to collect SINs – and some do – they have a corresponding responsibility to develop and follow strict policies about access, use, storage, and disposal.

Conclusion

[43] The collection of Social Insurance Numbers by Health (at the behest of Finance) for purposes of medical-expense reimbursement did not comply with section 40(c) of the ATIPPA. It was an unauthorized collection of personal information.

[44] Health and Finance have made some reasonable security arrangements to safeguard the Social Insurance Numbers they hold, but there are additional steps they should take or additional checks they should perform.

Recommendations

[45] I recommend that Health stop collecting Social Insurance Numbers from claimants for medical-expense reimbursement, and that Finance formally confirm to the Health processing unit in Rankin Inlet that collection of a claimant's SIN is not mandatory.

[46] I recommend that Health review the use of the email inbox used by the processing unit in Rankin Inlet to (a) confirm that access is restricted by position to those who need to see it, and (b) delete emails from which the relevant information has been transferred to the claimant's electronic file. See paragraph 34(a).

[47] I recommend that Health set up and enforce an automatic deletion rule for medical-expense claimants' electronic files that is consistent with (a) the relevant records-retention schedule, and (b) audit requirements. See paragraph 34(b).

[48] I recommend that Finance review the use of the generic email inbox used by the Accounts Payable unit in Iqaluit to (a) confirm that access is restricted by position to those who need to see it, and (b) delete emails from which the relevant information has been transferred to Oracle Fusion Cloud. See paragraph 34(c).

[49] I recommend that Finance set a firm date for the decommissioning of the accounts-payable portion of the old ERM system and ensure that personal information contained therein is, on that date, permanently and securely deleted. See paragraph 34(d).

Graham Steele
ᑲᒥᓯᓗ / Commissioner / Kamisina / Commissaire