

# Commissioner's Final Report

<b>Report Number:</b>	25-289-RR
<b>CanLII Citation:</b>	Departments of Education and Human Resources (Re), 2025 NUIPC 8
<b>NUIPC File Number:</b>	25-114
<b>Date:</b>	June 19, 2025

**[1]** The Complainant is an employee of the Department of Education. The Department of Human Resources asked the Complainant to undergo independent medical examinations (IMEs). The IME reports were delivered to HR and then shared with various people within Education and HR. The Complainant alleges several privacy breaches in the way the IME reports were handled. The Commissioner finds there was no unauthorized disclosure. The Commissioner also finds Education and HR did not make reasonable security arrangements to safeguard the IME reports, and recommends certain measures to improve security.

**[2]** This is a review of a privacy breach complaint. 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).

**[3]** I have jurisdiction over the Departments of Education and Human Resources: ATIPPA, section 2, definition of “public body”.

## Issues

[4] The issues in this review are:

- a. Was there an unauthorized disclosure by Education or HR of the Complainant's personal information?
- b. Did Education and HR make reasonable security arrangements to safeguard the Complainant's personal information?

## Facts

[5] The Complainant is an employee of the Department of Education. The Complainant has been on an extended leave. The human-resources elements of the file are being handled largely by the Department of Human Resources, in consultation with Education. That is normal for complex cases, which this one was.

[6] HR asked the Complainant to undergo two independent medical examinations (IMEs). The purpose of IMEs is to provide information on which HR and an employee's home department can develop a return-to-work plan and assess any necessary workplace accommodations.

[7] When asking an employee to undergo IMEs, HR has a standard-form letter that it asks the employee to sign. In the Complainant's case, the letter came from Education and was signed by an Education assistant deputy minister, but the content of the letter came from HR.

[8] The letter includes a consent agreement. The letter says (page 2):

Please confirm your ... authorization to release non-medical information relevant to the completion of the medical examinations by signing this document below.

(Underlining is in original.) This request is repeated, in slightly different words, at the top of the next page:

By signing, I ... agree to the release of the **non-medical information** obtained during the assessments to the employer in order to determine fitness for work and potential accommodation(s).

(Bolding is in original.)

**[9]** The Complainant did not immediately sign the consent agreement. HR wrote to the Complainant insisting the agreement be signed.

**[10]** The Complainant did eventually sign the agreement, but also put an asterisk after the “By signing...” sentence quoted above. The asterisk is linked to the following sentence written by the Complainant below their signature:

\*Conditionally upon mutual agreement of who, specifically, will have access to the non-medical information, the storage of the non-medical information, and the length of time the non-medical information will be stored.

Despite this written condition, there was no further discussion between HR, Education and the Complainant about the terms of such an agreement.

**[11]** To manage the IMEs, HR used the services of a private company called SOMA. HR sent to SOMA a set of questions. SOMA assigned the IMEs to doctors on its roster.

**[12]** The IMEs were duly completed by the Complainant and the SOMA doctors. The doctors’ reports were submitted to SOMA in the form of a letter that included answers to the GN’s questions. These letters are “the IME reports”.

**[13]** SOMA sent the IME reports to an Employee Relations manager on August 12, 2024. The ER manager forwarded the reports to their director, and to the Education assistant deputy minister (ADM) who was handling the Complainant’s file.

**[14]** At some point, the ER manager put the IME reports in a folder on HR’s shared network drive, and the Education ADM put them in a folder on Education’s shared network drive. Both folders have restricted access.

**[15]** On August 13, the ADM forwarded the IME reports by email to another Education ADM. The second ADM was covering for the first ADM's files while the latter was taking annual leave.

**[16]** On August 14, there was a videoconference involving the Complainant, the ER manager and the first Education ADM. During that meeting, the ER manager said to the Complainant that the only people within the GN who had seen the IME reports were the ER manager and the Education ADM.

**[17]** Also on August 14, the two Education ADMs had a very brief conversation about the Complainant's case, using the WhatsApp messaging application. The conversation took place both before and after the videoconference.

**[18]** On August 15, the Complainant wrote an email to the ER manager and the Education ADM to express (among other things) a concern about confidentiality. The email says that the condition attached by the Complainant to the consent agreement was being breached. The Complainant said that had they known the contents of the IME reports, they would not have consented to the reports being seen by the Education ADM.

**[19]** This review file was opened on February 20, 2025.

## **Law**

**[20]** The rules about collection, use and disclosure of personal information are in Part 2 of the ATIPPA, in Divisions A, B and C, respectively. In the present case, the issue raised by the Complainant is about disclosure of personal information, so it falls under Part 2, Division C, and in particular section 48.

**[21]** Section 48 of the ATIPPA is a lengthy list of circumstances in which a public body may disclose personal information. The paragraphs potentially relevant to the Complainant's case are as follows:

48. A public body may disclose personal information

(a) for the purpose for which the information was collected or compiled or for a use consistent with that purpose;

(b) where the individual the information relates to has identified the information and consented, in the prescribed manner, to its disclosure;

...

(g) for the purpose of hiring, managing or administering personnel of the Government of Nunavut or a public body;

...

(k) to an officer or employee of the public body or to a member of the Executive Council, where the information is necessary for the performance of the duties of the officer or employee or the member of the Executive Council; ....

**[22]** Section 48.1 contains guidance on how to interpret the phrase “a use consistent with that purpose” in section 48(a):

48.1. A use of personal information is consistent under section 43 or 48 with the purpose for which the information was collected or compiled where the use

(a) has a reasonable and direct connection to that purpose; and

(b) is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information.

**[23]** 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.

**[24]** This “reasonable security arrangements” standard is vague. 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 those analyses here, but I adopt them for purposes of this decision.

## Analysis

**[25]** The ATIPPA restricts how the GN can collect, use and disclose personal information. The GN collected the Complainant's personal information for a valid purpose and used it for the intended purpose. The main issue raised by the Complainant is whether the Complainant's personal information was disclosed to too many people.

**[26]** Before getting to the main issue, there is one preliminary issue that I need to address.

### *Medical information v. non-medical information*

**[27]** HR acknowledges that it is not entitled to see an employee's medical information. At the same time, HR believes that it is entitled to receive non-medical information relevant to an employee's return to work and any necessary workplace accommodations. In my view, HR is correct on both counts.

**[28]** But what exactly is "medical" and "non-medical"? The underlying premise of HR's position in this case is that IME reports do not contain medical information. In the standard-form consent agreement, for example, HR stresses (twice) that the employee is consenting only to the release of non-medical information.

**[29]** When the ER manager received the IME reports from SOMA, they took it as a given that the reports did not contain any medical information. HR relies on the fact that SOMA sends only "redacted" reports. (I will leave aside the fact that no unredacted report seems to exist, and that the so-called redacted report seems to be the only report there is.)

**[30]** I have trouble accepting HR's position. Even though the IME reports are written by medical doctors and based on medical examinations, HR says they are, somehow, not medical reports.

**[31]** It is true that the questions posed by HR and answered by the doctors are focused on return-to-work and workplace accommodations, but that does not make the reports entirely non-medical in nature. In one report, for example, the

doctor recommends a certain course of treatment from which the Complainant could benefit before returning to work. No matter how much semantic dancing one does, that is a medical opinion.

**[32]** In my view, HR needs to re-think the problematic distinction it is trying to draw between medical and non-medical information in IME reports. For the purposes of the present case, the fundamentally medical nature of IME reports underlines the privacy interests that are at stake, and why IME reports need to be handled with special care. The Complainant was sensitive about who saw the IME reports, and they had every right to be.

*Who received the reports?*

**[33]** I find as a fact that at least the following people received the Complainant's IME reports:

- a. HR Employee Relations manager.
- b. HR Employee Relations director.
- c. An Education assistant deputy minister.
- d. A second Education assistant deputy minister.

**[34]** The Complainant alleges that other people received the IME reports, but I do not see evidence of that in the file material.

*Who should have been able to see the reports?*

**[35]** The Complainant accepts that it was appropriate for the ER manager to receive the IME reports from SOMA. The Complainant does not accept that the other three people should have been able to see the reports. I will consider each in turn.

*(a) ER director*

**[36]** As soon as the ER manager received the IME reports from SOMA, they forwarded the reports by email to their director. The Complainant says this was a breach of privacy.

**[37]** GN public bodies are, by their nature, organized hierarchically. In my view, the privacy provisions of the ATIPPA should not be used in a way that prevents GN managers from exercising hierarchical supervision and support to their employees. Sharing records within a work unit for work-related purposes fits within section 48, such as section 48(a) (consistent purpose), section 48(g) (managing personnel), and section 48(k) (performance of an employee's duties).

**[38]** There are some exceptions to the hierarchical sharing of information, such as in the *Child and Family Services Act* and the *Adoption Act*, but these exceptions are expressly laid down by statute.

**[39]** In this case, the Complainant's case was complex. It is, in my view, normal and acceptable that the ER manager would want to consult their director. There could be meaningful consultation only if the director knew what was in the IME reports. I find that it was appropriate for the ER manager to share the IME reports with their director. To put it in legal terms, it was not an unauthorized disclosure of the Complainant's personal information.

**[40]** There is, however, one twist that merits further comment.

**[41]** During the videoconference call with the Complainant on August 14, the ER manager told the Complainant that the only people in the GN who had seen the IME reports were the two people on the call, i.e. the ER manager and the Education ADM. That statement was untrue, and the ER manager knew it was untrue.

**[42]** Nevertheless, I am not prepared to find that this untruth was in itself a breach of the Complainant's privacy. The ER division does not owe the Complainant an explanation of its internal functioning, nor should the privacy provisions of the ATIPPA be stretched to impose that sort of obligation. The most I



can say is that, in an environment where the Complainant's trust in the process was already low, the untruth spoken by the ER manager was unfortunate and perhaps not necessary.

*(b) First Education ADM*

**[43]** The ER manager also forwarded the IME reports by email to an assistant deputy minister at Education. The Complainant says this was a breach of privacy.

**[44]** When ER is handling a GN employee's file, they work together with the employee's home department, which in the Complainant's case was Education.

**[45]** Normally, ER's contact at Education would have been the Complainant's direct supervisor, and the ADM would not have been directly involved. In this case, however, Education had good reasons for not including the Complainant's direct supervisor in the discussion. (I am aware of the reasons, but I will not state them here because they would tend to identify the Complainant.) That is why the chosen contact was the ADM, who was the supervisor's supervisor.

**[46]** The Complainant argues that their express consent was required to share the IME reports with the ADM.

**[47]** I do not agree. As discussed in the Law section above, consent is only one of the circumstances listed in section 48 of the ATIPPA. Sharing the IME reports with the ADM comfortably fits within other parts of section 48, such as section 48(a) (consistent purpose), section 48(g) (managing personnel), and section 48(k) (performance of an employee's duties).

**[48]** The Complainant also argues that there was "clearly documented distrust" in their professional relationship with the ADM, and that if they had known the IME reports would be shared with the ADM, they would not have agreed to undergo the IMEs.

**[49]** I cannot accept this argument either. The Complainant knew the ADM was involved from early on. The consent letter, for example, was signed on Education's behalf by the ADM. The Complainant's objection to the ADM's

participation came after the IME reports had been shared, and after the meeting at which the IME reports were discussed.

[50] More importantly, the Complainant's argument shows the tangles that can be created when a privacy complaint is a sliver of a complex HR file. In my view, the privacy provisions of the ATIPPA should not be stretched to the point where I am making recommendations about which specific people in a department should be able to see which specific records, based on my assessment of interpersonal relationships within the department. That is a rabbit-hole from which this office would never emerge.

[51] I do not want to be understood as dismissing the Complainant's concerns. They may be valid, but they are better handled as questions of public service values or ethics within the context of HR management, rather than as privacy issues under the ATIPPA.

[52] Education needed to have someone work with ER on the Complainant's case. They had already decided not to involve the Complainant's direct supervisor. The ADM was as good a substitute as anyone else. I find that sharing the IME reports with the ADM was not an unauthorized disclosure of the Complainant's personal information.

*(c) Second Education ADM*

[53] The first Education ADM emailed the IME reports to a second ADM. The Complainant says this was a breach of privacy.

[54] When the IME reports were received by ER, the Education ADM was taking annual leave (i.e. on vacation). While they were taking leave, the second ADM was covering for them. This is normal practice within the GN. I accept that, in principle, someone covering for another employee should have access to any records they might need while they are covering for someone else.

[55] In hindsight, however, we know that the second ADM never needed to see the IME reports. The first ADM, even though technically on vacation, was monitoring their email and participating in some files, including the

Complainant's. The first ADM participated in the videoconference with ER manager and the Complainant. The second ADM did not participate in the Complainant's file at all.

[56] I am not prepared to find that sharing the IME reports with the second ADM was an unauthorized disclosure of the Complainant's personal information. There was always a possibility, while the first ADM was on leave, that the second ADM would have to step in with some decision or action on the Complainant's file. The situation is, however, a little closer to the line of what is acceptable, because the first ADM never let go of the file. No doubt the situation could have been handled differently.

[57] Again, though, there is a twist that merits further comment.

[58] I noted above that the ER manager, during the videoconference with the Complainant on August 14, said that only two people had seen the IME reports. That was untrue because the ER manager had sent the reports to the ER director. But it was doubly untrue because the first ADM had sent the reports to the second ADM. The ER manager says they did not know the second ADM had received the IME reports, and I accept their evidence. The first ADM says it did not really register with them during the videoconference that the ER manager's statement was untrue, so they did not step in to correct it. I accept this evidence too.

[59] The Complainant was told that only two people had seen the IME reports, when the truth was that four people had seen them. The untruth was not, however, in itself a breach of the Complainant's privacy. I can only repeat that, in an environment where the Complainant's trust in the process was already low, the untruth was unfortunate and perhaps not necessary.

#### *Conditional consent*

[60] The Complainant argues that sharing the IME reports was a violation of the condition they put on the consent agreement.

**[61]** As noted in the Facts section above, the Complainant added the following condition to the consent agreement:

\*Conditionally upon mutual agreement of who, specifically, will have access to the non-medical information, the storage of the non-medical information, and the length of time the non-medical information will be stored.

There was, however, no further discussion about the content of that condition. The Complainant went ahead with the IMEs.

**[62]** When I interviewed the ER manager and the Education ADM for this review, neither had any recollection of seeing the Complainant's condition. They were focused on whether the Complainant had signed the agreement. I accept as a fact that they did not notice it at the time.

**[63]** The Complainant referred to the condition in an email to the ER manager and Education ADM (August 15, 2024, third paragraph):

I am also writing to remind you that the release of the IME reports to my employer was contingent upon our agreement regarding who would receive this information, where it would be stored, and for how long ... . Right now, this agreement is being breached.

Again, however, the ER manager and the Education ADM have no recollection of reading that paragraph of the Complainant's email. They did not ask themselves what agreement the Complainant was referring to.

**[64]** Generally, an employee is entitled to put a condition on their consent, and a public body is bound to respect any condition it accepts. A public body can also, of course, reject any condition proposed by an employee.

**[65]** In the present case, however, I cannot find that HR or Education accepted the Complainant's condition, nor that they breached it. The condition written by the Complainant does not have substantive content. It is a proposal. No agreement was ever reached – in fact no discussion was ever held – on the items specified by the Complainant. The Complainant went ahead with the IMEs.

**[66]** In any event, the IME reports could be shared within the GN even without the Complainant's consent, as long as the sharing fit within one of the paragraphs of section 48 of the ATIPPA. As discussed above, the sharing of the reports with the ER director and the two Education ADMs was legally acceptable in the circumstances of the case.

#### *WhatsApp conversation*

**[67]** The two Education ADMs had two brief exchanges of messages about the Complainant's case, one just before the videoconference and one just after it. The exchange took place on the WhatsApp application. The Complainant says this was a breach of privacy.

**[68]** I have already found that the second ADM was covering for the first ADM while the latter was on vacation, so it was not a privacy breach for the second ADM to receive the IME reports. I apply the same analysis to the WhatsApp messages. It was not a privacy breach for the second ADM to be informed when the call was happening and the outcome.

**[69]** The messages were brief and relatively innocuous. One post-meeting comment from the first ADM was, however, more subjective in nature. Since the first ADM had decided to continue handling the file, even while on vacation, this comment was unnecessary. It was not something the second ADM needed to know. In all the circumstances, however, it did not rise to the level of being an unauthorized disclosure of the Complainant's personal information.

**[70]** In *Department of Education (Re)*, 2024 NUIPC 19 (CanLII), also known as Review Report 24-270, I recommended that Education discontinue the use of WhatsApp by senior management. The Minister's decision under section 36 of the ATIPPA neither accepted nor rejected that recommendation. I can only repeat the recommendation here. WhatsApp is outside the control of Education or the GN. It may be insecure. It should not be used to discuss human-resources issues, even in the relatively innocuous way that occurred on this file.

### *Storage of the IME reports*

**[71]** The Complainant also raises the issue of the storage of their IME reports. The Complainant wants to know where exactly the IME reports are being held, and how secure they are. Their concern is based partly on their own observations within the Department of Education, over a period of years, of less-than-careful handling of personal information.

**[72]** I have already found that it was legally acceptable for the four employees to receive the IME reports, so that is not the issue. The issue is how the IME reports were handled.

**[73]** In a recent decision, I remarked on the fact that many GN employees and work units use their email account for digital storage: *Departments of Health and Finance (Re)*, 2025 NUIPC 7 (CanLII) at paragraph 35. This case raises the same issue.

**[74]** As I pointed out in the *Health and Finance* case, I am not suggesting that GN email is insecure. It is as secure as the Information Management/Information Technology division of the Department of Transportation and Infrastructure Nunavut (TIN) can make it. But it is subject to the vulnerabilities of any email system and the vagaries of human error.

**[75]** The Complainant's IME reports were sent by email to at least the following:

- a. HR Employee Relations manager (from SOMA).
- b. HR Employee Relations director (from the ER manager).
- c. Education assistant deputy minister (from the ER manager).
- d. A second Education assistant deputy minister (from the first ADM).

**[76]** As far as I know, all four of these GN employees still hold that email (with IME reports attached) in their email Inbox folder, and at least two of them (the ER manager and the first Education ADM) hold the email in their email Sent folder. For the reasons given in the *Health and Finance* case, I find that the use of an

email program for digital storage of IME reports is not a “reasonable security arrangement” as required by section 42 of the ATIPPA.

**[77]** For the ER manager, a better method would have been to place a PDF copy of the email and IME reports in a secure shared folder on the network drive, refer their director to that folder, and delete the email from their inbox. That way access would be restricted, no copies would be made, and a digital audit trail would be created. The Education ADM could have gone through a similar process for sharing with the second ADM. If a sensitive document must be emailed, it could at least have been password-protected or encrypted.

**[78]** I understand why GN employees use email for storage the way they do. It is quick and easy. Unfortunately, in my experience over hundreds of ATIPP files, most GN employees draw no distinction between emails containing routine information and emails containing sensitive personal information. Everything stays in their inbox, and never leaves.

#### *Concluding comments*

**[79]** The best safeguard against unauthorized disclosure of personal information is a strong privacy culture: *Department of Health (Re)*, 2024 NUIPC 15 (CanLII) at paragraph 59.

**[80]** A culture of privacy, as the name implies, is not any one rule or any one practice. It is an environment. A privacy environment is reinforced every day, in ways large and small, spoken and unspoken, from top to bottom of the organization: *Department of Health (Re)*, 2023 NUIPC 5 (CanLII) at paragraph 35.

**[81]** Culture is not, by its nature, amenable to quick fixes or recommendations in a Review Report. It is a longer-term objective, but the work needs to start today.

**[82]** In this case, I have found there was no unauthorized disclosure of the Complainant’s IME reports. At almost every point, however, the reports could have been handled more carefully than they were.

## Conclusion

**[83]** There was no unauthorized disclosure of the Complainant's personal information.

**[84]** Education and HR did not make reasonable security arrangements to safeguard the Complainant's personal information.

## Recommendations

**[85]** I **recommend** that HR review and revise its email storage practices so that all IME reports are deleted from email programs after the records have been transferred to the appropriate restricted-access folder on the network drive.

**[86]** I **recommend** that HR delete the Complainant's IME reports from the email of the ER manager and the ER director (and any other HR employee who received them) after verifying that the reports are in the appropriate restricted-access folder on the network drive.

**[87]** I **recommend** that Education delete the Complainant's IME reports from the email of the two assistant deputy ministers (and any other Education employee who received them) after verifying that the reports are in the appropriate restricted-access folder on the network drive.

**[88]** I **recommend** that HR and Education review and revise their document-handling protocols so that, to the greatest extent possible, IME reports are shared via secure folders on the network drive rather than by email.

**[89]** I **recommend** that HR and Education review and revise their document-handling protocols so that, if an IME report must be emailed, the reports are password-protected and/or encrypted.

**[90]** I **recommend** that Education discontinue the use of WhatsApp by senior management.

Graham Steele

ᑲᑦᑭᑦᑭᑦ / Commissioner / Kamisina / Commissaire