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:	24-266-RR
CanLII Citation:	Department of Health (Re), 2024 NUIPC 15
NUIPC File Numbers:	24-146, 24-150
GN File Number:	1029-30-2425DH0505
Date:	July 2, 2024

Summary

[1] On numerous occasions, a Health employee accessed the electronic medical records of two patients. The first patient was a close friend. The employee had that patient's verbal permission to access their records. The second patient was the domestic partner of the first patient. The employee did not have that patient's permission to access their records. The Commissioner finds there was a privacy breach in both cases. Having a patient's verbal permission does not justify an otherwise unauthorized use and disclosure of medical records. Accessing the second patient's records was an intentional, serious, and sustained violation of that patient's privacy. The Commissioner makes recommendations to reduce the risk of similar privacy breaches in future.

Nature of Review and Jurisdiction

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

[3] I have jurisdiction over the Department of Health: ATIPPA, section 2, definition of "public body".

Issues

[4] The issues in this review are:

a. Was there an unauthorized use or disclosure of PTNT1's personal information?
b. Was there an unauthorized use or disclosure of PTNT2's personal information?
c. Did Health make reasonable security arrangements to guard against data intrusion in the Meditech system?

Facts

[5] To preserve their anonymity, the key people in this story will be referred to as follows:

a. PTNT1: Patient #1. At the relevant times, PTNT1 was PTNT2's domestic partner.

b. PTNT2: Patient #2. The Complainant. At the relevant times, PTNT2 was PTNT1's domestic partner.

c. EMP1: The Health employee who is the alleged data intruder. A close friend of PTNT1.

d. MGR1: The Health manager who is the direct supervisor of EMP1.

[6] PTNT1 and PTNT2 are residents of Nunavut. Like most Nunavummiut, their health records are stored in the electronic medical records (EMR) system used in Nunavut. Nunavut's EMR system is a proprietary system called Meditech. In this decision I will refer to a person's Meditech records as their "chart".

[7] In mid-April 2024, MGR1 became aware that EMP1 might have viewed the charts of PTNT1 and PTNT2 without a clinical reason.

[8] MGR1 did not immediately act on that information. They were not sure if the allegations were true, nor were they certain of the procedure to obtain the necessary Meditech audit report.

[9] On April 22, MGR1 met with EMP1, informed them of the allegation, and asked for an explanation. According to MGR1, EMP1 said:

a. They had looked at PTNT1's chart once, at PTNT1's request, to check an appointment time.

b. They had looked at PTNT2's chart once when PTNT2 was in the health centre. EMP1 could not offer a reason for doing so. EMP1 denied looking at PTNT2's chart at any other time.

[10] The next day, MGR1 was informed by EMP1 that EMP1 was resigning their position, effective May 10. EMP1 left Nunavut shortly after the resignation date. According to MGR1, EMP1's resignation was not surprising, nor was it necessarily connected to the previous day's meeting about the privacy breach allegation.

[11] On May 9, MGR1 received a summary analysis of the Meditech audit reports. The summary showed that, in the one-year period from April 2023 to April 2024, EMP1 had accessed PTNT1's chart on five different days, and had accessed PTNT2's chart on fourteen different days.

[12] Health then notified me of a privacy breach, as it is required to do under section 49.9(1) of the ATIPPA. Health also prepared a privacy breach report (PBR) and submitted it to me.

[13] Health's human resources division attempted to contact EMP1, but failed. Because EMP1 had resigned, Health HR did not pursue the attempt at contact. I suggested to Health that the ATIPP office should continue trying to contact EMP1 for purposes of the privacy breach investigation.

[14] On June 3, Health's ATIPP officer did speak with EMP1. EMP1 admitted that they accessed the charts of PTNT1 and PTNT2, and acknowledged they should not have done so. EMP1 apologized.

[15] Meanwhile, Health notified PTNT2 of the privacy breach, as it is required to do under section 49.10(1) of the ATIPPA. Health also tried to notify PTNT1 of the privacy breach, but failed.

[16] On June 4, shortly after receiving Health's notification letter, PTNT2 filed a privacy breach complaint with me. I concluded, under section 49.2(1), that a review was warranted in the circumstances. I then undertook my own investigation. This Review Report is the result.

[17] During my investigation, I have communicated with PTNT1, PTNT2, EMP1 and MGR1. I have spoken to a number of other witnesses, and I have obtained further analysis of the Meditech audit reports.

[18] On June 18 I sent a draft of my factual findings to EMP1 and asked for any comments or corrections they might have. I have since spoken with EMP1 by telephone but I have not received a written response.

Law

[19] Part 2 of the ATIPPA deals with the protection of privacy, and specifically with the collection, use, and disclosure of personal information.

Personal information

[20] "Personal information" is defined in section 2 of the ATIPPA to mean "information about an identifiable individual". Medical information in the Meditech system is personal information.

Unauthorized use

[21] Division B of Part 2 deals with the use of personal information. Section 43 lays down the basic rule:

> 43. A public body may use personal information only
>
> (a) for the purpose for which the information was collected or compiled, or for a use consistent with that purpose;
>
> (b) if the individual the information is about has identified the information and consented, in the prescribed manner, to the use; or
>
> (c) for a purpose for which the information may be disclosed to that public body under Division C of this Part.

[22] Section 43(b) refers to consent "in the prescribed manner". "Prescribed" means prescribed by regulation: *Legislation Act*, section 1(1). The ATIPP Regulations, section 5, specify how consent is to be given:

> 5. (1) The consent of an individual to a public body's use or disclosure of his or her personal information under paragraphs 43(b) and 48(b) of the Act
>
> (a) must be in writing or given orally; and
>
> (b) must specify to whom the personal information may be disclosed or how the personal information may be used.
>
> (2) If the consent referred to in subsection (1) is given orally, the public body shall make and maintain a written record of the consent.

[23] Section 43(c) refers to "Division C of this Part", which covers authorized disclosure. It does not apply to the present case.

[24] If neither section 43(b) nor 43(c) applies, then the public body (and its employees) must use the personal information only in accordance with section 43(a), i.e. "for the purpose for which the information was collected or compiled, or for a use consistent with that purpose".

Unauthorized disclosure

[25] Division C of Part 2 deals with the disclosure of personal information. Section 47 lays down the basic rule:

> 47. A public body may disclose personal information only
>
> (a) in accordance with Part 1; or
>
> (b) in accordance with this Division.

[26] Section 47(a) refers to Part 1 of the ATIPPA, which is the access-to-information part. It is not relevant to the present case.

[27] Section 47(b) refers to "this Division", which covers sections 48, 48.1, and 49. Nothing in those sections is relevant to the present case.

[28] If neither section 47(a) nor 47(b) applies, then the public body (and its employees) must not disclose the personal information.

Data security standard

[29] The possibility of data intrusion into the Meditech system is a "serious, permanent, and elusive threat to the privacy of Nunavummiut": *Department of Health (Re)*, 2023 NUIPC 6 (CanLII) at paragraph 63.

[30] The Department of Health has a statutory obligation to safeguard the personal information it holds. The obligation 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.

[31] In the absence of detailed, health-specific privacy legislation in Nunavut, section 42 is the only statutory standard for data security.

Previous decisions about Meditech data intrusion

[32] There have been several Nunavut decisions about data intrusion in the Meditech system: *Department of Health (Re)*, 2023 NUIPC 6 (CanLII); *Department of Health (Re)*, 2020 NUIPC 5 (CanLII); *Complainant (Re)*, 2020 NUIPC 18 (CanLII).

[33] In each of these cases, the facts were uncontested. In the first two, the data intruder looked at someone's health records for an improper purpose. In the third, the data intruder believed they were allowed to access the person's health records, but the Commissioner found they were wrong and the access was therefore improper.

[34] In *Department of Health (Re)*, 2024 NUIPC 9 (CanLII), the Complainant alleged that two Health employees viewed the Complainant's medical records without authorization. The facts were contested by the employees. I concluded, after investigation, that there had been no breach of the Complainant's privacy. To protect the Complainant's personal medical information, the facts of the case, and my analysis of the facts, were not published. This case therefore does not provide any <u>public</u> guidance, but I have taken it into account in my analysis.

[35] In *Department of Health (Re)*, 2023 NUIPC 6 (CanLII) at paragraphs 46 to 50, I quoted and adopted the analysis of the Nova Scotia Information and Privacy Commissioner in *Health (Nova Scotia) (Re)*, 2023 NSOIPC 2 (CanLII). The Nova Scotia case was a comprehensive review of medical data intrusion following the mass casualty event in March 2020 in that province. For purposes of the present case, I again adopt the analysis of the Nova Scotia Information and Privacy Commissioner.

Analysis

[36] This case is, unfortunately, another example of a Health employee misusing their access to electronic health records.

[37] EMP1 admits they accessed PTNT1's or PTNT2's charts, and acknowledges they should not have done so. Despite the admission, I believe EMP1 continues to downplay the extent and seriousness of their data intrusion.

[38] The situations of PTNT1 and PTNT2 are quite different, so I will consider them separately.

A note on terminology

[39] The act of unauthorized intrusion into someone's personal information is usually referred to as "snooping". That word and its cognates are found in almost all the literature on the subject, including decisions from privacy regulators both here in Nunavut and across Canada: see, for example, *Department of Health (Re)*, 2020 NUIPC 5 (CanLII).

[40] For the reasons given in *Department of Health (Re)*, 2023 NUIPC 6 (CanLII) at paragraphs 23 to 25, I will not use the words "snoop", "snooping" or "snooper". I will use "data intrusion" and "data intruder" instead.

PTNT1 – use and disclosure

[41] EMP1 was a close friend of PTNT1. Different people describe their relationship differently. Whatever the truth, the relationship was complex. Everything that EMP1 did appears to have been based on that relationship.

[42] The Meditech audit report shows that, during the period April 2023 to April 2024, EMP1 went into PTNT1's chart five times. At no time during this period was EMP1 involved in PTNT1's care. EMP1 admits that accessing PTNT1's chart in 2023-24 was part of a broader pattern of behaviour. EMP1 estimates that "over the years" they have accessed PTNT1's chart about 20 times for an unauthorized purpose. The number could well be higher.

[43] The purpose of going into PTNT1's chart appears to have been taking a "short cut" around the health centre's usual procedures. It was what one might call "back-door access" to health care. EMP1 and PTNT1 say, for example, that it was often difficult or impossible to get through to health centre staff by telephone. When that happened, PTNT1 would contact their friend EMP1, who would go into the Meditech chart to verify things like appointment times or a prescription.

[44] EMP1 and PTNT1 say, and I accept, that EMP1 always had PTNT1's consent to access PTNT1's chart. Nevertheless, this consent was never given or recorded in the manner prescribed by regulation, so it was never lawful consent.

[45] With or without PTNT's consent, EMP1 was acting inappropriately. Going into Meditech as a favour to a friend is not an authorized use, nor is it an authorized disclosure. It may seem harmless, but it is not. Playing around with access and consent is destructive of trust and integrity, which are essential elements of Canada's public health system; it creates risks and potential liabilities for the GN; and in the worst cases, it promotes corruption.

[46] EMP1 always had better options. EMP1 could have re-directed PTNT1 to the appropriate health-centre staff, or could have walked down the hall to have a conversation with the appropriate person (e.g. "Could you please give PTNT1 a call? They're having trouble getting through, and they're wondering about their appointment time next week"). Going into Meditech as a favour for a friend was always the wrong choice.

PTNT2 – use and disclosure

[47] EMP1 and PTNT2 knew each other through PTNT1. Except through PTNT1, they were not friends.

[48] PTNT1 and PTNT2 had a personal relationship for five years. At the times relevant to this decision, they were domestic partners. It was a troubled relationship. The relationship has since ended.

[49] In June 2023, PTNT2 was taken to the emergency room (ER) at the health centre. EMP1 did not normally work in the ER, but helped occasionally if the ER was short-staffed. EMP1 noticed that PTNT2 had been admitted and went to the ER.

[50] In the one-year period covered by the Meditech audit report, that was the first day EMP1 went into PTNT2's Meditech chart. Among other things EMP1 did that day, EMP1 printed a diagnostic image from PTNT2's chart. A Health manager informs me, and I accept, that this was "not typical" behaviour in the ER. Typically someone working in the ER would look at the image on a screen.

[51] It is not clear to me if EMP1 had any role in attending to PTNT2 in the ER. EMP1 says yes. PTNT2 says no. EMP1 did have user access to the ER module of Meditech, which reflected the fact that EMP1 was authorized to work in the ER if needed, even though their regular job was elsewhere. Because of the personal connection between EMP1 and PTNT2, EMP1 should probably have declined any involvement in PTNT2's care anyway.

[52] If that one day were the only time EMP1 went into PTNT2's chart, I would give EMP1 the benefit of the doubt. The printing of the diagnostic image is suspicious, but there might also be an innocent explanation.

[53] But it was far from the only time. Over the next three weeks, EMP1 went into PTNT2's chart almost every working day. The Meditech audit report shows EMP1 accessing PTNT2's chart in 29 separate sessions spread over 13 working days. At no time during this period was EMP1 involved in PTNT2's care.

[54] The next part of my analysis cannot be told without revealing sensitive personal information about PTNT2. For the reasons given in *Department of Health (Re)*, 2024 NUIPC 9 (CanLII) at paragraph 9, I have moved this part of my analysis to Appendix A. Appendix A will be made available only to the Department of Health. For this public part of the report, I move directly to my finding of fact.

[55] I find that EMP1's intrusion into PTNT2's chart was an intentional, serious, and sustained breach of PTNT2's personal privacy.

Reasonable security arrangements: General comments

[56] As I wrote in 2023 NUIPC 5 (CanLII) at paragraph 63, it is 100% foreseeable that there will be attempts at data intrusion in Meditech. It is likely that other data intrusions have occurred and are now occurring. Yet every time I see a data intrusion case involving Nunavut's Meditech system, I am struck by how easy it is to be a data intruder, and how hard it is for data intruders to be detected.

[57] In the present case, MGR1 became aware that EMP1 might be intruding in the charts of PTNT1 and PTNT2. I know how MGR1 discovered the intrusion, but I will not give details. I will say only that detection required some carelessness by EMP1 and some luck. It would have been easy for EMP1's data intrusion to go undetected.

[58] As noted in the Law section above, Health has a statutory duty to "protect personal information by making reasonable security arrangements": ATIPPA, section 42. The legal standard in section 42 is reasonableness, not perfection: 2023 NUIPC 6 (CanLII) at paragraph 58. No matter what safeguards are in place, there will always be some risk of data intrusion. The objective is to make data intrusion harder and detection more likely. At the same time, safeguards must be carefully designed so that they do not get in the way of necessary medical care.

Reasonable security arrangements: Privacy culture

[59] The best safeguard against data intrusion is a privacy culture within the health-care system so strong that employees would not even consider a data intrusion: 2023 NUIPC 6 (CanLII) at paragraph 60. But culture is not, by its nature, amenable to quick fixes. It is a longer-term objective. On that front, it appears that Health still has a long way to go.

Reasonable security arrangements: Anti-intrusion plan

[60] In 2023 NUIPC 6 (CanLII) at paragraphs 61 to 68, I wrote about the need for an anti-intrusion plan. "Health has bits and pieces of policy or practice in place or under consideration," I wrote, "but not all of them are written down, and they do not add up to a plan. Something more comprehensive is needed." I then outlined some elements of an anti-intrusion plan. My recommendation, in paragraph 91, was "that Health develop a comprehensive anti-intrusion plan".

[61] In his written decision in response to the Review Report, the Minister of Health rejected this recommendation. He wrote: "Health has decided not to develop an anti-intrusion plan on its own. An anti-intrusion plan is best served as a GN wide initiative".

[62] I was surprised by this portion of the Minister's decision. I believe it was based on a misunderstanding, which no doubt was due to the wording of my Review Report. My analysis of the need for an anti-intrusion plan was intended to relate only to data intrusion in Meditech. Since Health is the only department that uses Meditech, it does not make much sense to wait for "a GN wide initiative".

[63] For these reasons, I repeat the same recommendation: that Health should develop a comprehensive anti-intrusion plan for users of the Meditech system.

Reasonable security arrangements: Audit software

[64] Until very recently, Health did not have any software tools for detecting data intrusion. I discussed this gap in 2023 NUIPC 6 (CanLII) at paragraphs 71 to 74. The only tool available is an after-the-fact audit report, which can run to thousands of lines and hundreds of pages even in straightforward cases. The reports are not user-friendly and require careful interpretation.

[65] During this investigation, Health advised me that it has acquired a software tool designed to monitor for data intrusion. The roll-out, which should happen soon, will be a significant step forward in Health's efforts to combat Meditech data intrusion.

[66] With audit software almost in place, I will repeat what I wrote in 2023 NUIPC 6 (CanLII) at paragraphs 72 to 74:

> [72] The lack of a clinical connection, or looking up the records of a co-worker, are only two examples of "red flag" behaviours. There are others, such as looking up family members, neighbours, or prominent community members; or looking up records at unusual hours; or looking up records in unusual volumes. "Red flag" behaviours do not automatically mean that something is wrong, but they do mean that questions need to be asked. …
>
> [73] … Nunavut, because of its small communities and social structure, will have its own unique "red flag" behaviours.
>
> [74] Moreover, having audit software that alerts Health to unusual behaviours is pointless if it is not being used, or if nobody is reading and following up on the reports that the software generates. I therefore recommend that Health assign to a specific position the responsibility for specifying, reviewing, and following-up on "red flag" behaviours.

[67] In the present case, EMP1's high volume of chart viewings over a brief period, and for a patient with whom EMP1 had no clinical connection, is the sort of "red flag" behaviour that audit software ought to be able to catch.

Consequences for EMP1

[68] It is not my role to recommend employment discipline, except in the most serious cases: *Department of Health (Re)*, 2023 NUIPC 5 (CanLII) at paragraphs 19 to 21; *Department of Community and Government Services (Re)*, 2021 NUIPC 8 (CanLII) at paragraph 55; *Department of Health (Re)*, 2021 NUIPC 2 (CanLII) at paragraph 39. This case may be one of the exceptions.

[69] EMP1 has resigned their position with the GN and has left the territory, so the options for employment discipline are limited. Health should consider placing EMP1 on its "do not hire" list, if it has not already done so. (When I say "consider", I mean Health should at least think about it.)

[70] EMP1's actions may also be a violation of section 59(1) of the ATIPPA. For the reasons given in 2023 NUIPC 6 (CanLII) at paragraphs 39 to 41, I acknowledge that prosecution for a violation of the ATIPPA is difficult or impossible.

[71] MGR1 filed a complaint with EMP1's professional regulator. That was an appropriate step. A professional discipline complaint is often the most effective consequence for data intrusion, especially in a jurisdiction like Nunavut where there is so much turnover in the GN.

[72] A professional regulator can take an independent look at the facts of a case, gives the member an opportunity to be heard, and has a range of disciplinary measures available. If professional discipline is imposed, the disciplinary record follows the health professional wherever they go.

[73] I am concerned, however, that Health does not have an established policy or procedure for laying a professional discipline complaint in cases of data intrusion. I note that the Nova Scotia report, referred to in paragraph 35 above, finds that Nova Scotia Health sometimes moved slowly, or not at all, because it was unclear who was supposed to do what after a data intrusion was discovered.

[74] It is not clear who within Health is responsible for deciding whether to file a complaint, nor who is responsible for actually filing it. It is not clear what evidence can be submitted to support a complaint, nor who should actually submit that

evidence. It is not clear who within Health should monitor the professional disciplinary process and follow it through to its conclusion. A written policy would go a long way towards clearing up the uncertainty and making optimal use of the professional discipline process as a deterrent to data intrusion.

A final comment: Communications

[75] To counter the high risk of data intrusion, Health needs the right policies, a good plan, and effective tools. It also needs to communicate more effectively with its staff about data intrusion.

[76] Based on this case and previous cases, I believe there are too many Health employees who do not consider data intrusion to be serious, or who believe they will not be detected if they do it. I am not convinced that Health's internal communications on this topic are effective. The communications I have seen are too vague, too wordy, and too infrequent. I recommend that the roll-out of the new audit software be accompanied by a communications plan for staff. Staff need to be told, in clear and unmistakeable language, that data intrusion is wrong, that it carries consequences, and that it is now more likely to be detected.

[77] Finally, Health needs to reassure Nunavummiut that their health records are secure and will be seen only by authorized staff and used only for the intended purpose. A single case of data intrusion is one too many.

Conclusion

[78] There was unauthorized use and disclosure of PTNT1's personal information by EMP1.

[79] There was unauthorized use and disclosure of PTNT2's personal information by EMP1.

[80] Health did not make reasonable security arrangements to guard against Meditech data intrusion.

Recommendations

[81] I recommend that Health develop a comprehensive anti-intrusion plan for the Meditech system. (see paragraphs 60 to 63)

[82] I recommend that Health complete its roll-out of the recently-acquired audit software. (see paragraphs 64 to 67)

[83] I recommend that Health consider placing EMP1 on its "do not hire" list, if it has not already done so. (see paragraphs 68 and 69)

[84] I recommend that Health develop a written policy with respect to the procedure for laying a professional disciplinary complaint in cases of data intrusion. (see paragraphs 71 to 74)

[85] I recommend that Health develop a communications plan to accompany its roll-out of the audit software. (see paragraphs 75 to 77)

Graham Steele
ᑲᒥᓯᓗ / Commissioner / Kamisina / Commissaire