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:	23-239-RR
CanLII Citation:	Department of Health (Re), 2023 NUIPC 6
NUIPC File Numbers:	22-177, 22-179
GN File Number:	1029-30-DH1849
Date:	March 27, 2023

Summary

[1] Over a period of eighteen months, and without any clinical purpose, a doctor viewed the Complainant's electronic medical records. The doctor's contract was terminated. The Complainant filed a privacy breach complaint and asks that the doctor be named and prosecuted. The Commissioner finds there was a breach of privacy, and that Health did not make reasonable security arrangements against the risk of data intrusion. The Commissioner makes certain recommendations to reduce the risk of data intrusion and to increase the likelihood that similar kinds of data intrusion will be detected. The Commissioner declines to name the doctor. The Commissioner recommends that Health, in consultation with Justice, consider prosecution.

Nature of Review and Jurisdiction

[2] This is a privacy breach review. The request for review was filed under section 49.1(1) of the *Access to information and Protection of Privacy Act* (ATIPPA). I conducted my review under section 49.1(2).

[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 a privacy breach?
b. Should the data intruder be named?
c. Should the data intruder be prosecuted?
d. Did Health make adequate security arrangements against the risk of data intrusion?

Facts

[5] The Complainant was a worker in Nunavut's health-care system. The position they held, and the community in which they worked, are not relevant to this decision and are omitted because they would tend to identify the Complainant.

[6] In May 2020 there was a workplace incident involving the Complainant and a medical doctor. The other details of the workplace incident are not relevant to this decision. It is enough to say that the incident was stressful for the Complainant, and that the doctor later acknowledged that their conduct was inappropriate and apologized for it.

[7] Shortly after the workplace incident, the doctor started looking at the Complainant's electronic medical records (EMRs). The doctor did so through Nunavut's EMR system, which is called "Meditech". The doctor had no clinical relationship with the Complainant and had no clinical reason to look at the Complainant's records.

[8] We know when the doctor started looking at the Complainant's medical records because Meditech keeps track of who looks at which records. This audit trail also confirms that the doctor looked at the Complainant's records on numerous occasions over the next eighteen months.

[9] Although there was an audit trail, Meditech had no built-in alert system. The doctor's actions came to light only because the Complainant asked, through ATIPP, to see the Meditech audit trail.

[10] When confronted with the audit evidence, the doctor admitted that they looked at the Complainant's medical records without any clinical reason. Health terminated the doctor's contract and referred the matter to the doctor's professional regulator.

[11] The doctor's admission was in a letter to the territorial medical chief of staff. The Complainant says that, in the course of this letter, the doctor committed another privacy breach: the doctor was using information obtained from the privacy breach to explain their conduct. In this way, the Complainant's personal information was disclosed to the medical chief of staff and anyone else within Health who read the doctor's letter.

[12] On December 28, 2022, the Complainant filed a privacy breach complaint with this office.

Law

[13] "Personal information" is defined in section 2 of the ATIPPA to mean "information about an identifiable individual".

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

[15] 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.

Paragraph (b) refers to consent. Paragraph (c) refers to "Division C of this Part", which covers authorized disclosure. Neither applies to the present case.

[16] If neither section 43(b) nor 43(c) applies, then the public body (and its employees and contractors) must use the personal information only for the purpose for which it was collected, or a consistent purpose.

[17] 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.

Paragraph (a) refers to Part 1 of the ATIPPA, which is the access-to-information part. It is not relevant to the present case. Paragraph (b) refers to "this Division", which covers sections 48, 48.1, and 49. Nothing in those sections is relevant to the present case.

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

Analysis

[19] The doctor's actions were a profound violation of the Complainant's personal privacy. In the lengthy discussion that follows, that simple fact should always be kept in mind.

[20] The doctor admits the privacy breach. They hardly had a choice, because the audit trail showed conclusively that the doctor viewed the Complainant's records on numerous occasions over eighteen months. To put it in legal terms, I find there was unauthorized use of the records by the doctor, and unauthorized disclosure of the records to the doctor, contrary to sections 43 and 47 of the ATIPPA.

[21] In their letter to the medical chief of staff, the doctor offered a rationale for the data intrusion, but it is self-serving and scarcely believable. I find the letter

constitutes a further privacy breach, because it uses information obtained from the privacy breach to try to justify the privacy breach. The Complainant's personal information was thus further used and disclosed for an unauthorized purpose.

[22] The only remaining questions for me to consider are the consequences under the ATIPPA for the doctor, and what Health can do to reduce the risk of similar breaches in future.

A note on terminology

[23] 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).

[24] The Complainant objects that "snooping" is an inappropriate word. It has a connotation of innocent curiosity. There was nothing innocent about what the doctor did in this case and the word "snooping" downplays the violation, says the Complainant.

[25] I agree. It is unfortunate that "snooping" has become so widespread in the decisions and literature on the subject. In this decision, I will not use "snooping" or its cognates. I considered using "data voyeurism" or "data invasion" but instead settled on "data intrusion". The doctor was a data intruder.

Naming the doctor

[26] The Complainant requests that I name the doctor in this Review Report, which is a public document.

[27] One argument put forward by the Complainant in favour of publicly naming a data intruder is that deterrence is more likely if data intruders know they will be "named and shamed". Another argument is that data intruders should not benefit from the very privacy protections they have violated.

[28] Against these arguments must be weighed the words of the ATIPP Act:

a. A privacy breach review under the ATIPPA must be conducted in private: section 49.3(1).

b. I am required not to disclose information that comes to my knowledge while doing my job: section 56(1).

c. I may nevertheless disclose in a Review Report anything that I consider "necessary" to establish grounds for the findings and recommendations in the Review Report: section 56(3)(b).

[29] In the 24 years since Nunavut was created, this office has issued close to 240 Review Reports. In none of them have the people involved been identified by name, probably because the former Commissioner and I never considered naming to be "necessary".

[30] To the contrary, the former Commissioner and I have gone to some lengths to make it difficult to identify those involved. We leave out identifying details such as job title, community, gender, and age unless those details are relevant to the findings and recommendations. In a jurisdiction like Nunavut with such a small population, it is inevitable that sometimes a knowledgeable reader can accurately guess who was involved in one of our cases, but we do what we can to make it difficult.

[31] The closest I have come to identifying a wrongdoer is *Department of Community and Government Services (Re)*, 2021 NUIPC 8 (CanLII) at paragraphs 15 to 20. In that case, a GN employee had deliberately leaked to a third party the name of an ATIPP applicant. Even in that case, I did not identify the leaker, though I did not rule out the possibility of doing so in an appropriate future case.

[32] In the end, I am bound by the ATIPPA. The legal test for revealing a data intruder's name is whether it is "necessary" to explain my findings and recommendations. I understand the Complainant's arguments that it may be <u>desirable</u> to name this data intruder, but I find it is not <u>necessary</u>. I therefore will not do it.

Prosecuting the doctor

[33] The Complainant also asks if the doctor can be prosecuted.

[34] Section 59 of the ATIPPA lays out two punishable offences:

> 59. (1) Every person who knowingly collects, uses or discloses personal information in contravention of this Act or the regulations is guilty of an offence punishable on summary conviction and is liable to a fine not exceeding $5,000.
>
> (2) Every person who wilfully
>
> (a) obstructs the Information and Privacy Commissioner or any other person in the exercise of the powers or performance of the duties or functions of the Information and Privacy Commissioner or other person under this Act,
>
> (b) fails to comply with any lawful requirement of the Information and Privacy Commissioner or any other person under this Act, or
>
> (c) makes any false statement to, or misleads or attempts to mislead, the Information and Privacy Commissioner or any other person in the exercise of the powers or performance of the duties or functions of the Information and Privacy Commissioner or other person under this Act,
>
> is guilty of an offence punishable on summary conviction and is liable to a fine not exceeding $5,000.

There has not, to my knowledge, ever been a prosecution under this section in Nunavut. There have been successful prosecutions for data intrusion in other Canadian jurisdictions. If there were a prosecution in the present case, it would be under section 59(1).

[35] There were at least two occasions on which the former Commissioner recommended that the GN consider prosecution under section 59: *Complainant (Re)*, 2020 NUIPC 17 (CanLII); and *Review Report 19-154 (Re)*, 2019 NUIPC 7 (CanLII).

[36] In the first case, the Health minister rejected the Commissioner's findings of fact, and therefore did not address the recommendation of prosecution. In the second case, the Justice minister explicitly rejected the Commissioner's

recommendation to prosecute, for the following reasons (from the minister's letter to the Commissioner, dated December 10, 2019):

> …the Department of Justice is declining to pursue prosecution of the complainant. Currently, the lack of legal resources in this territory has put undue pressure on our court system, resulting in a need to prioritize immediate cases.
>
> Since the complainant resides outside of Nunavut, prosecution would require significant legal resources due to the complexity of layering [sic] charges outside the territory.
>
> Furthermore, the six-month limitation period for summary conviction offences makes prosecution of this case unlikely given that this review was requested in July of 2018.
>
> As a final point, the benefit of sending a message to other Government of Nunavut contractors by prosecuting the complainant, is outweighed by the improbability of this type of incident recurring within the Government of Nunavut.

[37] There are three other cases in which the former Commissioner raises the possibility of prosecution:

a. The former Commissioner writes "I came very close … to having a charge laid" against an individual: *Review Report 17-122 (Re)*, 2017 NUIPC 9 (CanLII).

b. The former Commissioner writes that she would have recommended prosecution, but accepted that workplace discipline had already been issued and would have to suffice: *Review Report 17-117 (Re)*, 2017 NUIPC 4 (CanLII).

c. The former Commissioner writes that she threatened prosecution under section 59 to spark a response from a public body: *Review Report 07-26 (Re)*, 2007 NUIPC 2 (CanLII).

[38] In none of these cases did the former Commissioner discuss the process by which a prosecution might actually occur. And therein lies the rub.

[39] I have been in touch with the Public Prosecution Service of Canada (PPSC), which is Nunavut's only prosecutorial service, and the RCMP, which is Nunavut's only police service. My communications were about section 59 cases in general, and not this specific case. Neither was able to commit to investigating (in the case of the RCMP) or prosecuting (in the case of the PPSC) an offence under section 59 of the ATIPPA. They are not sure it is within their respective mandates.

[40] I have also been in touch with the GN Department of Justice, which is ultimately responsible for the investigation and prosecution of territorial offences (as opposed to *Criminal Code* offences or offences under other federal statutes). That discussion, which is also about section 59 in general and not this specific case, is not yet concluded. In any event, I am doubtful that GN Justice is the appropriate entity to deal with ATIPPA offences. The ATIPPA applies only to a "public body" under the GN umbrella. An alleged offender will almost always be someone employed by or otherwise associated with the GN.

[41] I do recommend that Health, in consultation with GN Justice, consider prosecuting the doctor, but I am aware of the difficulties: the doctor is no longer in Nunavut, there is a six-month limitation period for a summary conviction offence, the maximum fine hardly merits the required cost and effort, and GN Justice may first have to negotiate a prosecution protocol for ATIPP offences with the PPSC.

Reducing the risk of data intrusion

[42] I now turn to the real heart of this Review Report, which is whether the Department of Health had adequate safeguards against data intrusion.

[43] Nunavut is one of a very few jurisdictions in Canada that does not have health-specific privacy legislation. If it did, the legislation would almost certainly contain detailed rules about the protection of personal health information.

[44] In the absence of detailed, health-specific privacy legislation, the only statutory standard for public bodies in Nunavut is 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.

[45] The test I will apply, then, is whether Health made "reasonable security arrangements" against the risk of data intrusion. Did Health meet that test? For the reasons that follow, I conclude it did not.

The Nova Scotia case

[46] The risk of data intrusion is well-known, and has been for as long as there have been medical records. The advent of electronic medical records has merely increased the speed and volume at which data intrusion can occur.

[47] Fortunately there is a very recent report from my counterpart in Nova Scotia that comprehensively reviews the issue of data intrusion: *Health (Nova Scotia) (Re)*, 2023 NSOIPC 2 (CanLII), which was issued in February of this year. The Nova Scotia report results from an investigation spanning two and a half years, covering a series of data intrusions linked to the Nova Scotia mass casualty event of March 2020.

[48] The Nova Scotia report reminds us how widespread data intrusion can be, the variety of ways in which data intruders self-justify their actions, and how inventive data intruders can be in getting around safeguards.

[49] The Nova Scotia report also reviews the major Canadian precedents. The report then provides, based on the precedents, the following synthesis of what "reasonable security arrangements" look like (at paragraph 158, footnotes omitted):

> 1. Contextual: Reasonable security is contextual. Overwhelmingly, what is clear in the case law is that reasonable security is intended to be an objective standard measured against the circumstances of each case.
> 2. Sensitivity: The more sensitive the information, the higher the security standard required. Personal health information is frequently among the most sensitive and can require a higher level of rigor to achieve reasonable security.
> 3. Not technically prescriptive: Reasonable security is not technically or operationally prescriptive. It does not specify particular technologies or

procedures that must be used to protect personal information. The reasonableness standard recognizes that, because situations vary, the measures needed to protect privacy vary. It also accommodates technological changes and the challenges and solutions that they bring to bear on, and offer for, personal information security.

4. Foreseeability: Reasonable security must take into account the foreseeability of the breach and the harm that would result if the breach occurred. The higher the risk of a breach, the higher the security standard will be.

5. Trust: For public sector custodians such as [Nova Scotia Health], reasonable security also includes reasonable assurances to the public that the custodian is taking privacy protections seriously. Where custodians hold personal information, the public has an increased level of trust that their personal information is being protected. This creates a high standard for custodians to ensure security measures are in place.

6. Industry standards: Industry standards, codes of practice or established user agreements can illuminate security requirements provided that following those practices reaches the contextual standards of reasonableness. If the industry standard is less than the contextual evidence demonstrates reasonable security requires, the industry standard is not sufficient. Simply accepting that a third party or contractor will follow industry standards or established user agreements does not demonstrate reasonable security.

7. Cost: The cost of implementing a new security measure may be a factor but it is on an extreme scale – reasonable security does not require a custodian to ensure against a minute risk at great cost. A custodian cannot dilute security by insisting on a cost efficiency in one area and refusing to pay for reasonable security in another.

8. Life cycle: Reasonable security applies to the entire life cycle of the records.

9. Format: The medium and format of the records will dictate the nature of the physical, technical and administrative safeguards.

10. Timing: Reasonableness requires a proactive and speedy response to known or likely risks. Time is of the essence in any privacy breach. The safeguards must ensure that should a privacy breach occur, the custodian and the affected individual will learn of the breach and have response measures in place quickly and efficiently.

11. Documentation: Procedures for establishing reasonable security must be documented, and custodians must be prepared to respond to the idea that employees won't always follow the documented procedures.

> 12. User logs: Cases dealing with intentional unauthorized access and use of personal health information by authorized users highlight the need for technical infrastructure to log user access of electronic systems and the need for an ongoing program of proactive auditing to address the general risk of intentional abuse of access by authorized users.

[50] I adopt this analysis. My recommendations flow from the application of the foregoing factors to the facts of this case.

Review Report 20-168

[51] The Nova Scotia report is very useful, but there is also a recent precedent from Nunavut: *Department of Health (Re)*, 2020 NUIPC 5 (CanLII); see also *Complainant (Re)*, 2020 NUIPC 18 (CanLII). I will refer to this case as "Review Report 20-168". It is a data intrusion case concerning Meditech. It was issued on April 4, 2020, so it is only three years old.

[52] In Review Report 20-168, a health employee looked at the complainant's Meditech records because "his spouse was having an affair with the complainant and he was concerned about the possibility that [the complainant] had tested positive for a sexually transmitted infection". The complainant had previously asked Health not to permit the employee to have any access to their records. The employee had been warned, both verbally and in writing, that they were not to look at the complainant's records. Despite the warnings, the audit trail showed the employee did look at the complainant's records once, for three minutes.

[53] Based on this scenario, the former Commissioner made several recommendations to bolster security against data intrusion. I summarize them as follows:

a. Every new Health employee should sign an oath of privacy protection. The oath must be explained to them as part of their "on-boarding". The oath must be renewed at least every two years. An employee who has not signed the oath must be denied access to health records.

b. The GN Code of Values and Ethics should include a section on privacy protection.

c. A policy should be developed that recognizes an individual's right to limit access to their health records, and there should be a procedure about how to limit access. When such a directive is given, there should be "regular and frequent" audits to ensure it is being complied with.

d. Privacy training, commensurate with the level of access to personal health information, should be mandatory for all Health employees. This training should be repeated at least every two years. The training should be offered on-line. The training modules should be kept up-to-date.

e. There should be a system of periodic audits of Meditech access, both targeted and random.

f. There should be a warning for any user who attempts to access the medical records of a person with whom they are not associated. The warning should also go to the user's supervisor. These warnings should be monitored and investigated as soon as possible.

[54] By letter dated May 26, 2020, the Minister of Health issued his written decision under section 49.6 of the ATIPPA, in response to the Commissioner's recommendations. The minister wrote "…the Department of Health welcomes your report and accepts your recommendations. Health staff will be following on your recommendations, including implementing online privacy training modules".

[55] As part of this review, I asked Health to report on the status of the recommendations from Review Report 20-168. They did so.

[56] Despite the minister's statement in 2020 that all recommendations had been accepted and would be implemented, the recommendation about targeted and random audits was in fact rejected ("Periodic targeted and random audits are neither practical nor able to detect privacy breaches."). The rest of the

recommendations, says Health, are currently (three years after Review Report 20-168) at various stages of being implemented or explored.

[57] I conclude that, at the time of the doctor's data intrusion in the present case, the recommendations in Review Report 20-168 had not been implemented.

General comments about reasonable security arrangements

[58] The legal standard in section 42 of the ATIPPA is reasonableness, not perfection. 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 cannot get in the way of urgent medical care.

[59] Meditech is a proprietary product, used under license. It is widely deployed across Canada. There is a limit to changes that Nunavut can make on its own. I therefore will not be too prescriptive in my recommendations. I prefer instead to recommend objectives, leaving it to Health, in consultation with its IT staff and the Meditech vendor, to determine how best to achieve those objectives.

[60] The best safeguard against data intrusion is a privacy culture within the health-care system so strong that staff would not even consider a data intrusion. In two previous decisions, I have alluded to this notion of a "privacy culture" or "privacy environment": *Department of Health (Re)*, 2021 NUIPC 2 (CanLII) at paragraph 37; *Department of Health (Re)*, 2023 NUIPC 5 (CanLII) at paragraphs 35 and 36. But culture is not, by its nature, amenable to quick fixes. It is a longer-term objective.

Reasonable security arrangements: an anti-intrusion plan

[61] Health needs an overall plan to counter data intrusion. It currently has bits and pieces of policy or practice in place or under consideration, but not all of them are written down, and they do not add up to a plan. Something more comprehensive is needed.

[62] EMRs contain some of our most sensitive personal information (Item 2 in the list of relevant factors, paragraph 49 above). Nunavummiut trust Health to

keep that sensitive data secure (Item 5). A comprehensive anti-intrusion plan is the minimum starting point for “reasonable security arrangements”.

[63] The plan must start with an acknowledgement that data intrusion into medical records is a serious, permanent, and elusive threat to the privacy of Nunavummiut. It is 100% foreseeable that there will be attempts at data intrusion into medical records (Item 4). It is, in fact, likely that other data intrusions have occurred and are now occurring. The only reason we do not know about them is because Health currently lacks any systematic means of detecting them.

[64] To counter this foreseeable risk, the plan must consider the three kinds of safeguards against data intrusion:

a. Physical safeguards include measures like locked rooms and locked filing cabinets. They are most applicable to hard-copy records. (Despite the use of Meditech, there are still many hard-copy medical records in Nunavut.)

b. Administrative safeguards include measures like hiring, training, oaths, supervision, access management, contracts, and employment discipline.

c. Technical safeguards include measures like password management, different levels of access for different providers, system warnings, and audit trails.

[65] A key administrative safeguard is to assign responsibilities in the anti-intrusion plan and establish accountabilities. It is one thing to create a plan; it is another thing to implement it and sustain it. The GN has a chronic issue with vacancies, turnover, and short-staffing. The anti-intrusion plan must take these factors into account. The plan must not fall victim to “capacity issues”.

[66] The plan must be documented (Item 11). The documentation should include both policies and procedures. With clear accountabilities and a documented plan, there is a greater chance of a timely, efficient response to known or likely risks of data intrusion (Item 10). That includes prompt notification

to affected individuals. I note that the Nova Scotia report 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.

[67] Health needs to introduce privacy concepts at an early stage of the employment or contracting process, and then regularly reinforce them. The reinforcement can happen in a variety of ways, including oaths, training, and ethical codes. However the reinforcement is done, the point is to avoid a situation in which an employee or contractor can plausibly say "I didn't know that what I did was wrong".

[68] The plan also needs to take frank account of the power relationships and personal relationships within the health-care system. It is a known risk that health staff with more power may use others to do their data intrusion for them. It is also a known risk that one person may become a data intruder as a "favour" to someone else.

[69] The plan should be public, and Health should report publicly, at regular intervals, on whether the plan's objectives are being met. The report should include the number of data intrusions since the last report, and the number of Nunavummiut affected by each data intrusion.

Reasonable security arrangements: other recommendations

[70] The key fact in the present case is that the doctor was able to breach the Complainant's privacy repeatedly, over a period of eighteen months, without anyone noticing. There was an audit trail, but nobody within Health was looking at it because there were no alerts to suggest anything amiss. The only reason the data intrusion was detected was because the Complainant was familiar with Meditech and knew what to look for when they filed an ATIPP request.

a. Audit software

[71] At the time of the data intrusion, Health did not have in place software that would alert it to unusual activity, such as a clinician repeatedly viewing records of a co-worker with whom they had no clinical relationship.

[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. In Nova Scotia, the use of audit software was a critical tool for identifying and then drilling down into data intrusion.

[73] I recommend that Health acquire software that will alert it to "red flag" behaviours. I believe Health is already moving down this path. I will not be prescriptive about which software that should be or what behaviours it should look for. 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.

b. Access warning

[75] There was no warning to the doctor when they accessed the Complainant's records.

[76] A warning notice is available in Meditech, but my understanding is that it is currently used only in the training/test environment. During this review, I pointed out to Health that the warning is not well written. I will not be prescriptive about what the warning should say, but it needs to be short and simple and unmistakably clear.

[77] A warning will not deter a determined data intruder, but it may give pause to a casual intruder. The effect of a warning may be diluted if there are too many "false positives" for users engaged in unproblematic behaviour. Health needs to listen to its users and be ready to modify the parameters for the warning.

[78] I recommend that Health modify the Meditech system so that, at a minimum, users receive a warning each time they attempt to access the records of a patient with whom they have no clinical connection.

c. Restricting access to records of a given patient

[79] One of the Complainant's fears was that the doctor could continue to access the Complainant's records, even after the data intrusion had been exposed.

[80] Health explains that Meditech access is linked to a person's GN credentials. When the GN credentials are cancelled, there is no way for that person to enter Meditech. In this case, we know when the doctor's GN credentials, and therefore their access to Meditech, were cancelled. That should provide some reassurance to the Complainant.

[81] Nevertheless, a slight change in the facts might have produced a different result. For example, what if the Complainant had asked Health, immediately after the workplace incident, to block the doctor from accessing the Complainant's records? What if the doctor's contract, and therefore their access to Meditech, had not been terminated? There appears to be no procedure by which a specific person with Meditech access can be blocked from another specific person's records. In my view, this is a significant gap. It is, in fact, one of the key issues identified in Review Report 20-168, which was issued three years ago.

[82] I therefore recommend that Health modify the Meditech system so that a given user can be blocked from accessing a given patient's records. There should, at the very least, be a means by which the file access is flagged to a supervisor or privacy officer.

d. Progress report

[83] Finally, I recommend that Health provide to this office, before the end of December 2023, a progress report on its EMR anti-intrusion plan.

[84] I have not made a recommendation of this kind before. I have generally considered this office's role to end when a Review Report is issued. The final step

in the review process is usually the minister's written decision in response to my recommendations: ATIPPA, section 49.6. It is generally undesirable for this office, an independent office of the Legislative Assembly, to maintain an ongoing supervisory role over executive administration.

[85] In this case, however, I believe a different approach is called for. Because of the seriousness of the data-intrusion risk, and because previous recommendations about Meditech were "accepted" but not implemented, a progress report is needed. Without a public progress report, we cannot be sure that Health is meeting its mandatory obligations under section 42 of the ATIPPA.

Conclusion

[86] There was an unauthorized use and an unauthorized disclosure of the Complainant's personal information.

[87] I will not name the data intruder.

[88] A decision about whether to prosecute the data intruder should be made by Health, in consultation with the GN Department of Justice.

[89] Health did not make reasonable security arrangements against the risk of data intrusion.

Recommendations

[90] **I recommend** that Health, in collaboration with the GN Department of Justice, consider prosecution of the doctor under section 59(1) of the ATIPPA (see paragraphs 33 to 41).

[91] **I recommend** that Health develop a comprehensive anti-intrusion plan (see paragraphs 61 to 69).

[92] **I recommend** that Health acquire software that will alert it to "red flag" behaviours by users of the Meditech system (see paragraphs 71 to 73).

[93] **I recommend** that Health assign to a specific position the responsibility for specifying, reviewing, and following-up on “red flag” behaviours by users of the Meditech system (see paragraph 74).

[94] **I recommend** that Health modify the Meditech system so that users who access the records of a person with whom they have no clinical relationship receive a clear warning (see paragraphs 75 to 78).

[95] **I recommend** that Health modify the Meditech system so that a given user can be blocked from accessing a given patient’s records (see paragraphs 79 to 82).

[96] **I recommend** that Health provide to this office, before the end of December 2023, a progress report on its medical records anti-intrusion plan (see paragraphs 83 to 85).

Graham Steele
ᑲᒥᓴᓇ / Commissioner / Kamisina / Commissaire