Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 290-2024, 007-2025

Dr. Siva Karunakaran
(Prairie Internal Medicine Specialists)

March 17, 2025

Summary: After investigating the snooping by an office manager at Prairie Internal Medicine Specialists, the A/Commissioner issued Investigation Report 108-2024. As a result of the A/Commissioner's recommendations, Dr. Siva Karunakaran (Dr. Karunakaran) determined that the office manager had continued snooping on personal health information on eHealth Saskatchewan's (eHealth) eHR Viewer by accessing their and their family members' personal health information. Dr. Karunakaran took action, including terminating the office manager's employment as well as proactively reporting the privacy breaches to the A/Commissioner. The A/Commissioner undertook another investigation into the matter. The A/Commissioner made a number of findings, including that Dr. Karunakaran has taken reasonable steps to prevent a future privacy breach. The A/Commissioner recommended that Dr. Karunakaran forward their investigation file to the Ministry of Justice and Attorney General, Public Prosecutions Division, to allow prosecutors to further consider whether an offence has occurred and if charges should be laid under *The Health Information Protection Act* and any other statute.

I BACKGROUND

[1] In Investigation Report 108-2024 (issued on September 20, 2024), I investigated a matter involving an office manager at Prairie Internal Medicine Specialists (the Clinic). The office manager had snooped upon an individual's personal health information in eHealth Saskatchewan's (eHealth) eHR Viewer over 35 times in 2021 and 2022. The unauthorized accesses resulted in the office manager having their access privileges to the eHR Viewer suspended for six months in 2022. After the six months, the office manager's access privileges were reinstated. Nevertheless, in that investigation report, I made a number of

recommendations, including that the trustee in the matter, Dr. Karunkaran, contact eHealth to establish a plan to conduct random user audits of all employees at the Clinic on an ongoing basis.

[2] Dr. Karunkaran complied with the recommendation. On or around September 23, 2024, Dr. Karunakaran received audit logs from eHealth. The audit logs revealed that the Office Manager had continued inappropriately accessing personal health information on the eHR Viewer. Specifically, from 2022 to 2024 they accessed the personal health information of family members as well as their own personal health information using the eHR Viewer. As a result, Dr. Karunakaran "permanently disabled" the office manager's access to the eHR Viewer and then terminated their employment at the Clinic.

[3] On December 20, 2024, Dr. Karunakaran's lawyer proactively reported the privacy breaches to my office. They indicated they had determined that the former office manager had accessed their own personal health information as well as that of their sister, son, stepdaughter, and husband.

[4] On January 24, 2025, my office notified both Dr. Karunakaran and the former office manager that my office would be undertaking an investigation.

[5] On February 23, 2025, the former office manager provided their submission to my office.

[6] On February 24, 2025, Dr. Karunakaran's lawyer provided Dr. Karunakaran's submission to my office.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[7] *The Health Information Protection Act* (HIPA) is engaged when three elements are present: 1) a trustee, 2) personal health information, and 3) the trustee has custody or control over the personal health information.

[8] In paragraphs [10] to [19] of Investigation Report 108-2024, I had found that Dr. Karunakaran qualified as the trustee pursuant to subsections 2(1)(t)(xii)(A) and 2(1)(t)(xv) of *The Health Information Protection Act* (HIPA) and subsection 4(b) of *The Health Information Protection Regulations* (HIPA Regulations) with custody and control of the personal health information at issue. In the submission to my office, Dr. Karunakaran's lawyer confirmed that Dr. Karunakaran is still the trustee of the personal health information viewed by the former office manager in the eHR Viewer.

[9] The personal health information that was viewed in the eHR Viewer includes name, date of birth, address, health services number, laboratory results, transcribed clinical documents, clinical encounter information and prescription profiles. Such information qualifies as personal health information as defined by subsection 2(1)(m)(i), (ii), (iii), (iv) and (v) of HIPA, which provide as follows:

> **2**(1) In this Act:
>
> …
> (m) **"personal health information"** means, with respect to an individual, whether living or deceased:
>
> (i) information with respect to the physical or mental health of the individual;
>
> (ii) information with respect to any health service provided to the individual;
>
> (iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
>
> (iv) information that is collected:
>
> (A) in the course of providing health services to the individual; or
>
> (B) incidentally to the provision of health services to the individual; or
>
> (v) registration information;

[10] As such, HIPA is engaged in this matter. Therefore, as with my finding in Investigation Report 108-2024, I find that I have jurisdiction to undertake this investigation.

2. Did privacy breaches occur?

[11] A privacy breach occurs when personal health information is collected, used, and/or disclosed without authority under HIPA.

[12] The need-to-know principle is the principle that trustees and their employees should only collect, use, or disclose personal health information that is necessary for the diagnosis, treatment or care of an individual or other purposes authorized by HIPA. The need-to-know principle is enshrined in section 23 of HIPA as follows:

> **23**(1) A trustee shall collect, use or disclose only the personal health information that is reasonably necessary for the purpose for which it is being collected, used or disclosed.
>
> (2) A trustee must establish policies and procedures to restrict access by the trustee's employees to an individual's personal health information that is not required by the employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.
>
> …
> (4) A trustee must, where practicable, use or disclose only de-identified personal health information if it will serve the purpose.

[13] Further, section 24 of HIPA restricts the collection of personal health information by trustees. It provides:

> **24**(1) A trustee shall ensure that the primary purpose for collecting personal health information is for the purposes of a program, activity or service of the trustee that can reasonably be expected to benefit the subject individual.
>
> (2) A trustee may collect personal health information for a secondary purpose if the secondary purpose is consistent with any of the purposes for which personal health information may be disclosed pursuant to section 27, 28 or 29.
>
> (3) Nothing in this Act prohibits the collection of personal health information where that collection is authorized by another Act or by a regulation made pursuant to another Act.
>
> (4) A trustee may collect personal health information for any purpose with the consent of the subject individual.

[14] Dr. Karunakaran's lawyer indicated that although one of the former office manager's family members was a patient who had "previously received care at the Clinic", none of the accesses by the former office manager were authorized by HIPA.

[15] The former office manager provided the following reasons for accessing the personal health information in the eHR Viewer. I am directly quoting from their responses as follows:

Family member	Quote of former Office Manager's submission
Sister	• this was a complete accident - there was a referral that was received in the office for one of the physicians and the patient had a similar name to my sister and not thinking I typed the name and when I realized what I had done I quickly exited the search completely.
Sons	• I am unclear of which son this might be, is it possible please for you to clarify. • my oldest son at one point had a referral to the office and in further looking into the referral it was deemed he had actually seen another physician for a similar reason and as such it was sent back to the referring physician as the rule in that department is that not to see 2 physician's [sic] for the same reason unless looking for a second opinion. • if this was for my youngest son, he is reviewed by another physician that I was working for at a different office & not having access to eHR viewer there was looking for information so that correct billing could be made.
Stepdaughter	• I don't honestly recall doing this - but looking in my personal information at home that would have been around the time that she had lab work done as she was not well and the family doctor kept saying they didn't have the results
Husband	• As for my husbands [sic] records we were having trouble setting up his Myehealth [sic] and he was going through some health issues around Sept/Oct 2023, he had a referral to the office to see one of the physicians and I was compiling records for the referral and after speaking to the physician in the office it was decided that it would be better if he saw someone else as it was more for a different issue then what the physician in the office can manage, so the referral was sent back to the GP. • As for the other dates I looked up his records with his knowledge and request, I do understand now that I should not

	have done this and rather go through his GP to have this reviewed.
Their own personal health information	• As for accessing my personal health information - first I would like to mention that I am a patient of a physician in the office and as such was getting information to put in my chart for his review. • second of all I was trying to figure out "CDM" and thought it was better to use my personal information to figure this feature out then to access someone else's.

[16] The reasons offered by the former office manager for accessing their family member's personal health information as well as their own in the eHR Viewer are not in accordance with sections 23 and 24 of HIPA. My office reviewed the audit logs and observed the following:

- The former office manager viewed family member #1 on December 1, 2022, December 5, 2022; January 1, 2023; January 3, 2023, January 9, 2023; May 11, 2023, July 6, 2023; August 23, 2023; September 13, 2023; February 12, 2024;

- The former office manager viewed the personal health information of family member #2 on January 13, 2023; April 13, 2023;

- The former office manager viewed family member #3 on January 23, 2023, August 3, 2023; August 17, 2023; August 18, 2023; August 22, 2023; August 23, 2023; August 30, 2023; August 31, 2023; September 1, 2023; September 5, 2023; October 13, 2023; October 15, 2023; October 16, 2023; October 17, 2023; October 20, 2023; October 24, 2023; October 26, 2023; October 28, 2023; October 30, 2023; October 31, 2023; November 2, 2023; November 5, 2023; November 7, 2023; November 8, 2023; November 10, 2023; November 23, 2023; December 11, 2023; December 16, 2023; December 22, 2023; December 24, 2023; December 31, 2023; January 3, 2024; January 9, 2024; May 12, 2024; May 14, 2024; May 15, 2024; May 16, 2024; May 17, 2024; May 22, 2024; May 26, 2024; June 19, 2024; June 22, 2024; June 23, 2024; June 24, 2024; June 25, 2024; June 26, 2024; June 27, 2024; June 28, 2024; June 30, 2024; September 2, 2024; September 3, 2024; September 5, 2024; September 8, 2024;

- The former office manager viewed the personal health information of family member #4 on August 14, 2023; and

- The former office manager viewed the personal health information of family member #5 on September 14, 2024.

[17] The multiple and sustained accesses by the former office manager to their family members' personal health information suggests they felt entitled to access personal health information on the eHR Viewer for personal reasons that were beyond their professional job duties.

[18] Therefore, I find that privacy breaches occurred.

3. Did Dr. Karunakaran respond to the privacy breaches appropriately?

[19] In circumstances where I have found that a privacy breach (or breaches) has occurred, my office's investigation will focus on whether the trustee (or trustees) has properly responded to the privacy breaches.

[20] As set out in section 5-4 of my office's *Rules of Procedure* and my office's *Privacy Breach Guidelines for Health Trustees*, my office determines whether the trustee properly responded to the privacy breach by analyzing the trustee's efforts to:

- Contain the breach (as soon as possible);
- Notify affected individuals (as soon as possible);
- Investigate the privacy breach; and
- Prevent future breaches.

Contain the breach (as soon as possible)

[21] Upon learning that a privacy breach has occurred, steps should be taken to immediately contain the breach. Depending on the nature of the breach, this can include:

- Stopping the unauthorized practice;
- Recovering the records;
- Shutting down the system that has been breached;
- Revoking access privileges; and

- Correcting weaknesses in physical security.

(*Privacy Breach Guidelines for Health Trustees*, p. 3)

[22] In Investigation Report 108-2024, I described how the former office manager's access privileges were revoked in 2022 by Dr. Karunakaran when it was determined that the office manager had accessed the complainant's personal health information inappropriately. Dr. Karunakaran re-instated their access privileges after six months. Dr. Karunakaran had also provided one-on-one training on the Clinic's privacy policies and procedures. In that investigation report, I had recommended that eHealth continue to audit the office manager's activities on the eHR Viewer.

[23] After learning that the former office manager had continued to access personal health information from 2022 to 2024, Dr. Karunakaran permanently revoked the former office manager's access to the eHR Viewer and terminated the office manager's employment. Therefore, I find that Dr. Karunakaran has taken appropriate steps to contain the privacy breach.

Notify affected individuals (as soon as possible)

[24] It is best practice to inform affected individuals when their personal health information has been a part of a privacy breach (*Privacy Breach Guidelines for Health Trustees*, p. 3). This is an important step so that the trustee can identify possible risks to the affected individuals and to inform them of steps they can take to protect themselves.

[25] Both eHealth and Dr. Karunakaran sent letters dated November 15, 2024, to the five family members whose personal health information the former office manager snooped upon. The letters contain the essential elements that my office recommends, such as what happened, what personal health information was snooped upon, the steps taken to prevent further breaches, an apology and the right of affected individuals to complain to my office. I find that Dr. Karunakaran (and eHealth) has provided appropriate notice to the affected individuals.

Investigate the privacy breach

[26] When considering why a privacy breach occurred, a trustee should reflect on the root causes, or what led to the breach occurring. It is an important step in mitigating the risk of a future breach of a similar nature from occurring (*Privacy Breach Guidelines for Health Trustees*, p. 5).

[27] As noted in Investigation Report 108-2024 at paragraphs [36] to [41], the former office manager was the author of the Clinic's policies in the Clinic's *The Privacy and Security Policies Manual*. These policies provided for how the Clinic was to collect personal health information "that is reasonably necessary to provide care and treatment to benefit its patients." The policies also outlined the consequences for inappropriately accessing personal health information, including further privacy training, loss of privileges, suspension without pay and dismissal. Since the former office manager was the author of such privileges, my office concluded that the former office manager would have been aware that snooping on personal health information was inappropriate.

[28] In the current case, Dr. Karunakaran's lawyer said:

> [Name of former office manager] was the Clinic's Privacy Contact Person. [They] previously worked alongside the SMA to draft and implement the Clinic's privacy policies. The Clinic's July 2016 Policy Manual indicates [Name of former office manager] was responsible for managing day-to-day compliance with the Clinic's policies and procedures. Furthermore, [they were] the point of contact for patients and staff for privacy related questions. [Name of former office manager] had significant experience working in medical clinics.
>
> There is no question [they were] familiar with the expectations of privacy and confidentiality in a healthcare setting. Accordingly, Dr. Karunakaran is confident[Name of former office manager] was aware of [their] obligations under HIPA and the Clinic's policies. Unfortunately, [Name of former office manager] failed to respect and follow provincial privacy legislation and/or the Clinic's privacy policies notwithstanding [their] own knowledge and experience, Dr. Karunakaran's strict warnings, and [their] additional training.

[29] In their submission, the former office manager said:

> …the only training that I received was reviewing the privacy videos on the SMA website and that of the Privacy Commission's website, I had taken what I learned in those videos and updated the office's policies.

[30] While it is not clear which privacy videos the former office manager is referring to, they admit they "updated" the Clinic's privacy policies. As such, they were well-aware that snooping on personal health information was inappropriate.

[31] Given that the office manager had authored the Clinic's privacy policies and had their access privileges to the eHR Viewer revoked in 2022 for a period of six months, the former office manager was aware that accessing personal health information on the eHR Viewer for reasons beyond fulfilling their job duties was inappropriate. I find that it was the willful decision of the former office manager to inappropriately access personal health information to be the root cause of these privacy breaches.

[32] Subsections 64(1) and (2) of HIPA provides:

> **64**(1) No person shall:
>
> (a) knowingly contravene any provision of this Act or the regulations;
>
> …
>
> (2) Every person who contravenes subsection (1) or (1.1) is guilty of an offence and is liable on summary conviction:
>
> (a) in the case of an individual, to a fine of not more than $50,000, to imprisonment for not more than one year or to both; and
>
> (b) in the case of a corporation, to a fine of not more than $500,000.

[33] I recommend that Dr. Karunakaran forward their investigation file to the Ministry of Justice and Attorney General, Public Prosecutions Division to allow prosecutors to further consider whether an offence has occurred and if charges should be laid under HIPA or any other statute. I also strongly encourage eHealth to do the same – that is, forward its investigation file to the Ministry of Justice and Attorney General, Public Prosecutions Division.

[34] Finally, I strongly encourage eHealth to never grant the former office manager access privileges to the eHR Viewer again.

Prevent future breaches

[35] The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring (*Privacy Breach Guidelines for Health Trustees*, p. 6). Prevention steps include strategies such as adding/enhancing safeguards, providing additional training, monitoring or auditing systems and users, and providing additional training.

[36] Dr. Karunakaran's lawyer outlined the following actions that their client will take to prevent similar privacy breaches:

- Implement a system of random audits with eHealth;
- Review the Clinic's privacy policies and procedures with the Saskatchewan Medical Association (SMA);
- Implement a policy that clarifies and confirm its employees are prohibited from viewing their own or family members' personal health information;
- Implement a zero-tolerance policy for privacy breaches going forward such that inappropriate conduct such as the former office manager will result in immediate termination of employment for cause;
- Conduct semi-annual reviews of all privacy policies and procedures to ensure staff members under the Clinic's privacy policies and procedures and allow for staff to ask questions if needed;
- Require all staff to review pertinent policy and training materials every six months and require staff to sign and date a spreadsheet confirming they have reviewed the materials;
- Arrange for the SMA to attend the Clinic to speak to staff about the importance of privacy and confidentiality policies;

- Require all new staff members to review all relevant privacy policies and procedures and require them to confirm they have reviewed the materials and to sign a confidentiality agreement on their first day of work;

- Training a new office manager on the Clinic's privacy and confidentiality policies and procedures;

- Appoint a new privacy officer who will be trained on the Clinic's privacy and confidentiality policies and procedures.

[37] Dr. Karunakaran's lawyer also outlined Dr. Karunakaran's plan with regard to suspected snooping by employees as follows:

> In future circumstances where employee snooping is suspected, Dr. Karunakaran intends to ensure the Clinic records details regarding how the breach occurred; suspends the employee's access to PHI; retrieves log information (if available); interviews the employee in question; identifies and interviews any pertinent witnesses; considers who needs to be notified regarding such breaches; determines whether the name of the employee will be disclosed to affected patients; reviews the privacy training that the employee in question has received in addition to any relevant contracts; and proactively reports to the OPIC [sic] to seek further advice. In accordance with Dr. Karunakaran's proposed zero-tolerance policy, incidents of confirmed employee snooping will also result in immediate termination of employment.

[38] I find that Dr. Karunakaran is taking reasonable steps to prevent a future privacy breach. However, with regard to whether the name of the employee will be disclosed to affected individuals, my office has taken the position that the snooper has a diminished expectation of privacy and that aggrieved individuals have a right to a complete account of what has occurred. In Investigation Report 203-2019 et al, I said at paragraph [68]:

> [68] My office's position is that an individual who has snooped should have a diminished expectation of privacy. Their identities and the disciplinary action taken against them should be revealed to affected individuals. The impact of a privacy breach is not standard and flat. Learning that a best friend, business partner, estranged spouse, co-worker, boss, neighbour, or a stranger snooped upon one's personal health information has different implications for individuals. Affected individuals are in the best position to understand the impacts of a privacy breach upon themselves. Knowing the identity of the snooper provides affected individuals with information to assess the harm that may result from having their privacy invaded. In my Investigation Report 100-2015, I cited the former Ontario Information and Privacy Commissioner's Investigation Report HO-010 that provided that aggrieved individuals have a right to a complete accounting of what has occurred. Aggrieved individuals will not find closure

> regarding the incident unless all the details of the investigation have been disclosed. Receiving general assurances that "the incident has been dealt with appropriately" falls far short of the level of disclosure that is required. Further, publicly identifying the snooper and the disciplinary action taken against the snooper would be a strong deterrent for other employees and contractors.

[39] Therefore, I recommend that if, in the future, Dr. Karunakaran determines any of their employees have inappropriately accessed personal health information, that they reveal the identity of the employee to the affected individuals so that the affected individual have a complete accounting of what has occurred.

III FINDINGS

[40] I find that I have jurisdiction to undertake this investigation.

[41] I find that privacy breaches occurred.

[42] I find that Dr. Karunakaran has taken steps to contain the privacy breach.

[43] I find that Dr. Karunakaran (and eHealth) has provided appropriate notice to the affected individuals.

[44] I find that it was the willful decision of the former office manager to inappropriately access personal health information to be the root cause of these privacy breaches.

[45] I find that Dr. Karunakaran is taking reasonable steps to prevent a future privacy breach.

IV RECOMMENDATIONS

[46] I recommend that Dr. Karunakaran forward their investigation files to the Ministry of Justice and Attorney General, Public Prosecutions Division to allow prosecutors to further consider whether an offence has occurred and if charges should be laid under HIPA or any other statute.

[47] I recommend that if, in the future, Dr. Karunakaran determines any of their employees have inappropriately accessed personal health information, that they reveal the identity of the employee to the affected individuals so that the affected individual have a complete accounting of what has occurred.

Dated at Regina, in the Province of Saskatchewan, this 17th day of March, 2025.

Ronald J. Kruzeniski, K.C.
A/Saskatchewan Information and Privacy Commissioner