Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 266-2024, 031-2025

Saskatchewan Health Authority

March 31, 2025

Summary: The Saskatchewan Health Authority (SHA) proactively reported that an SHA employee (Snooper) inappropriately accessed personal health information in its Sunrise Clinical Manager (SCM) electronic health record while working at the Yorkton Regional Health Centre between 2023 and 2024. Upon investigation, the A/Commissioner noted that the SHA claimed that 70 individuals were affected by privacy breaches. The A/Commissioner found that the SHA did not properly contain the privacy breaches. He recommended that, within 30 days of issuance of this Investigation Report, the SHA amend its policies and procedures to revoke or restrict an employee's access to personal health information in electronic health records at the outset of any internal privacy breach investigation and provide his office with a copy of its amended policies and procedures. The A/Commissioner also found that the SHA did not take appropriate steps to notify the 70 individuals affected by the privacy breaches and his office. He recommended that the SHA re-issue notification letters that include copies of excerpts from the SCM records which apply to each affected individual, highlighting the access(es) which reflect the breach(es), including dates of unauthorized accesses and the name of the Snooper. He also recommended that the SHA ensure, going forward, this information is provided alongside notification in subsequent cases where snooping is identified. He recommended that the SHA amend its policies to proactively notify his office of privacy breaches within ten calendar days of initiating its containment of a breach, and to provide his office with a copy of its amended policies and procedures. The A/Commissioner found that the SHA appropriately investigated the privacy breach, but that the SHA has not taken appropriate steps to mitigate or prevent breaches of a similar nature from occurring in the future. He recommended that the SHA ensure, within 30 days of issuance of this Investigation Report, that it has finalized its audit policy and provides a copy of it to his office. He recommended that the SHA share with SHA staff the name of the Snooper and the disciplinary actions taken. Finally, the A/Commissioner recommended that the SHA forward their investigation files to the Ministry of Justice and Attorney General,

Public Prosecution Division, to allow prosecutors to further consider whether an offence has occurred and if charges should be laid under *The Health Information Protection Act* or any other statute.

I BACKGROUND

[1] On November 18, 2024, the Saskatchewan Health Authority (SHA) contacted my office to proactively report that, from November 1, 2023 to May 3, 2024, an SHA employee of the Yorkton Regional Health Centre (one of its facilities) inappropriately accessed the personal health information of 70 individuals, with 210 distinct accesses of their PHI via the Sunrise Clinical Manager (SCM) system. SCM is an electronic health record used by the Yorkton Regional Health Centre.

[2] On December 13, 2024, my office sent notification to the SHA that I would be investigating the matter. My office requested that the SHA provide my office with a completed *Privacy Breach Questionnaire* provided by my office and other documentation by January 13, 2025.

[3] On January 13, 2025, the SHA provided its internal investigation report, in lieu of my office's *Privacy Breach Questionnaire*, as well as copies of the SHA's *Privacy and Confidentiality* policy, *Pledge of Confidentiality* for staff, and *Acceptable Use of Information Technology (IT) Assets* policy.

[4] After a review of the SHA's internal investigation report, it was apparent that it lacked sufficient detail for my office to fully investigate the matter. As a result, on January 16, 2025, my office asked the SHA to provide, by January 21, 2025, additional information and materials, including SCM audit logs and notes from interviews with the employee at issue. On January 21, 2025, the SHA responded to my office and, instead of providing all of the information requested, the SHA asked for the rationale or purpose of requiring the audit log and interview notes. After several emails back and forth between January 22, 2025, and January 30, 2025, the SHA finally provided the audit report and interview notes to my office.

[5] Also, on January 30, 2025, my office requested additional clarification and information, including the contact information for the employee at issue. Again, the SHA asked for the purpose for making contact with the employee at issue. On January 31, 2025, the SHA indicated it needed to complete an internal review before it could respond. On February 4, 2025, after not receiving the information requested, my office contacted the SHA, informing it that I required the contact information for the employee at issue by end of day. The SHA responded indicating it had not conducted its internal review and would not be providing the materials as required. Finally, after another week of resistance, the SHA provided my office with the contact information for the employee at issue on February 6, 2025.

[6] By way of registered mail dated February 12, 2025, my office notified the employee at issue of my office's investigation.

[7] On February 28, 2025, a legal representative for the employee at issue emailed my office to indicate that they had chosen to not make representations.

[8] Throughout February and early March, my office requested additional information and materials from the SHA, which were provided without issue.

[9] On March 6, 2025, my office informed the SHA and the legal representative for the employee at issue that it would be issuing this Investigation Report on the matter.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[10] *The Health Information Protection Act* (HIPA) applies when three elements are present:

1. Personal health information,
2. A trustee, and

3. The personal health information is in the custody or control of the trustee.

[11] First, I must consider the presence of personal health information. In the SHA's internal investigation report, the SHA indicated that, "information in SCM includes lab results, radiology reports, immunization records, prescriptions, and clinical documents." However, the SHA later confirmed that the employee in question had access to patients' addresses, telephone numbers, birthdates, genders, and health services numbers through the electronic health record. These are examples of personal health information pursuant to subsections 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;

[12] As there is personal health information involved, I find that the first element is present.

[13] Next, I must consider the presence of a trustee. This second element is present, given that the SHA qualifies as "the provincial health authority" pursuant to subsection 2(1)(t)(ii) of HIPA, which provides:

> **2**(1) In this Act:

> ...
> (t) **"trustee"** means any of the following that have custody or control of personal health information:
>
> ...
> (ii) the provincial health authority or a health care organization;

[14] Finally, I must consider whether the SHA is *the* trustee with custody or control over the personal health information at issue. According to my office's Review Report 333-2019 at paragraph [13], to have "custody" means that a trustee has physical possession of records with a measure of control over them; whereas, to have "control" means having the authority to manage the records including storing, restricting, and regulating their use. In Investigation Report 320-2017 at paragraph [8], I found that the SHA had custody and control of personal health information in the SCM, which is the same system at issue in this investigation. Therefore, I find that the SHA had custody and control of the personal health information at issue in this investigation, and that the third element is present.

[15] As all three elements are present, HIPA is engaged, and I find that I have jurisdiction to investigate this matter.

2. Did privacy breaches occur?

[16] Personal health information must be collected, used and/or disclosed in accordance with HIPA. To do otherwise may be a breach of privacy.

[17] A privacy breach occurs when personal health information is collected, used or disclosed in a way that is not authorized by HIPA.

[18] "Use" is defined at subsection 2(1)(u) of HIPA as follows:

> **2**(1) In this Act:
>
> …
> (u) "use" includes reference to or manipulation of personal health information by the trustee that has custody or control of the information, but does not include disclosure to another person or trustee.

[19] In its internal investigation report, the SHA acknowledged that, "the employee, an RN, accessed 70 electronic patient records in Sunrise Clinical Manager (SCM) at the Yorkton Regional Health Centre." These accesses of SCM qualify as "uses" because the employee at issue accessed patient records (personal health information) via SCM at the Yorkton Regional Health Centre, which makes that information in the custody and control of the SHA.

[20] To collect, use, or disclose personal health information in accordance with HIPA means to have duly considered the "need-to-know principle;" that is, the principle that trustees (and their staff) should only collect, use, and/or disclose what is necessary for the diagnosis, treatment, or care of an individual or other purposes authorized by HIPA. This definition is echoed at paragraph [21] of Investigation Report 108-2024 and at section 23 of HIPA, which provides for circumstances in which a trustee may "use" personal health information:

> **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.
>
> [Emphasis added]

[21] To assess if privacy breaches occurred, I must evaluate whether the personal health information was accessed without a need-to-know, which is without authority. To have a need-to-know, the reason why the patient's personal health information is accessed is important. In particular, subsections 26(1) and (2) of HIPA provide as follows:

> **26**(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 may use personal health information:
>
> (a) for a purpose for which the information may be disclosed by the trustee pursuant to section 27, 28 or 29;
>
> (b) for the purposes of de-identifying the personal health information;
>
> (c) for a purpose that will primarily benefit the subject individual; or
>
> (d) for a prescribed purpose.

[22] I now turn to examine the statements provided by the SHA.

[23] In its internal investigation report, the SHA acknowledged that, "the employee, an RN, accessed 70 electronic patient records in SCM at the Yorkton Regional Health Centre without a need-to-know" under HIPA. In other words, it was not "reasonably necessary" for the employee at issue to collect, use, or disclose the personal health information.

[24] In the course of its internal investigation, the SHA consulted audit logs and conducted interviews with the employee at issue. As a result, the SHA determined that the employee at issue was not able to reasonably substantiate a need-to-know (pursuant to subsection 23 of HIPA) for any of the accesses. Some examples of how the SHA arrived at this conclusion are as follows:

- Initially, the employee at issue had alleged that other employees may have accessed their account. The SHA found that no other employee worked all of the hours that matched the times of unauthorized accesses.

- Further, the employee at issue had alleged that, in some instances, they had accessed patients' historical information as part of clinic processes for registering them as new patients. The SHA found that the clinic does not engage in processes as described by the employee at issue, and that there is no need to view a patient's history in the electronic medical record, as all information is listed on an order.

- In addition, the employee at issue had alleged that, in some instances, they viewed the personal health information of patients in their care for the purposes of

providing care. The SHA found that several of those patients were no longer in the care of the employee at issue, had recently died, or were not patients relevant to the type of care provided by the employee at issue.

- Moreover, the employee at issue acknowledged that, in some instances, they viewed the personal health information of individuals out of curiosity.

- When asked why they would access patient files without a need-to-know on the same day they had completed the SHA's required privacy and confidentiality training, the employee at issue stated they, "skimmed through it and didn't take it as seriously as [they did] now."

- Ultimately, the SHA found that the employee at issue had recollections of details for 14 of the patients whose personal health information was accessed. Of the 14 patients, only 10 of the recollections were plausible. The employee at issue had no explanation or recollection for the remaining affected individuals whose personal health information was accessed.

[25] In other words, the accesses were not for the purposes of diagnosis, treatment, or care of the patients in question or for any other purpose authorized by subsections 26(1) and (2) of HIPA.

[26] With reference to an audit report provided by the SHA, my office verified that the employee at issue accessed electronic health records of 70 patients. It appears their personal health information was accessed 210 times by the employee at issue, without a requisite need-to-know.

[27] My office defines "snooping" as the unauthorized access of personal information or personal health information by employees without a need-to-know" (*Guide to LA FOIP*, Chapter 6 on "Protection of Privacy" [*Guide to LA FOIP*, Ch. 6], p. 334). It appears that "snooping" captures the actions of the employee at issue, described by the SHA. Hereinafter, the employee at issue will, therefore, be referred to as the "Snooper."

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

3. Were the privacy breaches appropriately handled by the SHA?

[29] In circumstances where a trustee proactively reports a privacy breach to my office, my office will consider whether the trustee appropriately handled the privacy breach. In order to be satisfied, my office would need to be confident that the trustee took the privacy breach seriously and appropriately addressed it. My office recommends four best practice steps be taken when a trustee discovers a breach of privacy has occurred. A trustee should have:

- Contained the breach (as soon as possible);
- Notified affected individuals (as soon as possible);
- Investigated the breach; and
- Taken steps to prevent future breaches.

(*Rules of Procedure*, updated January 7, 2025, p. 34)

[30] I will consider these four steps in the SHA's response to the privacy breaches.

Contained the breach (as soon as possible)

[31] Upon learning that a privacy breach occurred, a trustee should immediately take steps to contain the breach or reduce the risks. Depending on the nature of the breach, this may include:

- Stopping the unauthorized practice.
- Recovering the records.
- Shutting down the system that has been breached.
- Revoking access to personal health information.
- Correcting weaknesses in physical security.

(*Privacy Breach Guidelines for Trustees*, updated August 2022, p. 3).

[32] Effective and prompt containment reduces the magnitude of a breach, and the risks involved, with personal health information being inappropriately accessed. I now turn to evaluate the SHA's containment of the privacy breaches.

[33] The SHA's internal investigation report provided to my office asserted that it contained the Snooper's access to SCM by terminating their employment. While termination of employment certainly is a definitive response to a snooping issue, I must review the SHA's efforts to manage and restrict the Snooper's access at the time it learned there were potential inappropriate accesses occurring in SCM.

[34] Based on a review of the SHA's internal investigation report, email correspondence, and additional materials, the following facts emerge as relevant:

- In March 2024, initial suspicions of privacy breaches surfaced as a result of a routine audit.
- On April 12, 2024, the SHA initiated an internal investigation into the Snooper's unauthorized accesses to personal health information.
- Throughout the month of April, the Snooper was on leave from the SHA. As a result of their leave, the Snooper's access to SCM was suspended.
- In May 2024, the Snooper began a new position within the SHA and their access to SCM was fully reinstated. At the time, the SHA had a new manager in place who did not know about the employee's privacy concerns and, as such, was not auditing her access.
- On May 3, 2024, it was reported that the Snooper had 27 additional unauthorized accesses to the personal health information of seven additional affected individuals. An audit was run on May 17, 2024, and provided to the original manager. As of March 21, 2025, the SHA was not able to confirm when the manager confirmed that there were additional accesses.
- The Snooper retained access to SCM from May until the termination of their employment on October 18, 2024.

[35] My office has previously urged the SHA to revoke employee's access to electronic medical records at the outset of any investigation into their potential snooping. In Investigation Report 203-2019, 214-2019, 257-2019 at paragraph [65], I recommended that, "**when the**

SHA has grounds to believe an individual is inappropriately accessing personal health information, that the SHA immediately suspend the individual's access to the [electronic medical record] …" [Emphasis added]. Notably, the SHA did not heed my recommendation in this case or at the time following the issuance of the aforementioned investigation report, when, in its response to my office's recommendation, the SHA asserted: "Removing a clinician's access to the [electronic medical record] means that they would not be able to provide safe patient care and therefore puts the patient at risk." I question how allowing a Snooper's access to an electronic medical record assures patient safety. In fact, it can also be argued that allowing access puts patient safety at risk. My office has investigated malicious cases of snooping where medical records have been modified or edited by snoopers. For example, in Investigation Report H-2013-001, I commented on privacy breaches wherein snoopers used their employee user privileges to modify information such as name, sex, and infectious disease information in the electronic information systems, while including vulgarities and the acronym "RIP" in patient files.

[36] The impact of the SHA's failure to revoke the Snooper's access to SCM is magnified by the fact that the SHA itself documented 27 additional unauthorized accesses to personal health information in SCM *after* the investigation was initiated. Had SHA effectively contained the Snooper's access to SCM, there would have been fewer individuals affected by the privacy breaches.

[37] A trustee's duty to protect personal health information is established at section 16 of HIPA. Specifically, subsections 16(b)(iii) and (c) of HIPA provide:

> **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> …
>
> (b) protect against any **reasonably anticipated**:
>
> …
>
> (iii) unauthorized access to or use, disclosure or modification of the information; and

> (c) otherwise ensure compliance with this Act by its employees.
>
> [Emphasis added]

[38] Given the Snooper's pattern of behaviour, it is unclear how the SHA could not have "reasonably anticipated" the additional 27 unauthorized accesses made by the Snooper while it conducted its internal investigation. By failing to revoke the Snooper's access to the electronic medical record, it failed to meet its duty to protect the patients' personal health information and did not ensure compliance with HIPA by the Snooper.

[39] Therefore, I find that the SHA did not appropriately contain the privacy breaches.

[40] I recommend that, within 30 days of issuance of this Investigation Report, the SHA amend its policies and procedures to revoke or restrict an employee's access to personal health information in electronic health records at the outset of any internal privacy breach investigation and provide my office with a copy of its amended policies and procedures.

Notified affected individuals (as soon as possible)

[41] As soon as possible following containment, a trustee must endeavor to notify affected individuals that their personal health information was inappropriately disclosed. Not only do individuals have a right to know, but they also need to know to protect themselves from any potential harm that may result from a privacy breach. Unless there is a compelling reason not to, a trustee should always notify affected individuals. An effective notification should include:

- A description of the breach (a general description of what happened).
- A detailed description of the personal health information involved (e.g., name, medical records, etc.).
- A description of possible types of harm that may come to the affected individual because of the breach of privacy.
- Steps taken and planned to mitigate the harm and prevent future breaches.

- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves.
- Recognition of the impacts of the breach on affected individuals and an apology.
- Contact information of an individual within the organization who can answer questions and provide further information.
- A notice that individuals have a right to complain to the IPC (provide contact information).
- Recognition of the impacts of the breach on affected individuals and an apology.

(*Privacy Breach Guidelines for Trustees*, p. 4)

[42] In addition to notifying individuals, trustees may want to notify other organizations, such as my office, law enforcement or other regulatory bodies that oversee professions.

[43] I will now consider whether the SHA appropriately provided these notifications.

[44] The SHA provided notification of the unauthorized accesses to affected individuals by way of letters and telephone conversations between December 5, 2024, and December 19, 2024. In its internal investigation report provided to my office, the SHA asserted:

> Due to the postal strike, we were unable to mail out the notification letters to the affected individuals when we originally intended (November 20, 2024). However, the letters were sent via courier to the individuals who have a civic address on December 5. Individuals that have a P.O. Box or General Delivery address were called between December 5 and 12. For individuals that we were not able to reach, letters were mailed out on December 19, as the strike was over.

[45] The SHA provided my office with copies of its notification letters to the affected individuals. The letters include several of the best practices outlined at paragraph [41] of this Investigation Report, insofar as the SHA provided the following to affected individuals:

- Both a general and more detailed description of what happened.
- A recognition of the impacts of the breach and an apology.

- The contact information of the manager prepared to answer questions and provide further information.

[46] However, the SHA's notification letter to affected individuals failed to embody some other critical best practices outlined at paragraph [41] of this Investigation Report, upon which I will comment next.

[47] For one, the SHA failed to provide to affected individuals a description of the possible types of harm that may come to them as a result of the breach of privacy. Similarly, the SHA failed to provide advice on actions the affected individuals could take to further mitigate the risk of harm and protect themselves.

[48] I recognize that, in its internal investigation report, the SHA stated, "the SHA does not believe there is any risk to the patients." However, as has been previously communicated to the SHA in my office's Investigation Report 065-2021, 068-2021, 069-2021, 073-2021:

> [42] **The SHA is not in a position to evaluate whether a snooper's motives were 'malicious' or not. Only affected individuals are in the position to determine how snooping impacts them.** Snooping is serious and jeopardizes patients' trust in the SHA.
>
> [Emphasis added]

[49] In other words, it is the SHA's responsibility to provide objective information to the affected individuals and allow those affected individuals to interpret the ramifications of the privacy breaches.

[50] This is of particular concern given that the notification letter provided to affected individuals only documented that, "information in SCM includes lab results, radiology reports, immunization records, prescriptions, and clinical documents." However, this statement does not appear to capture the scope of the personal health information breached. On February 20, 2025, my office asked the SHA to clarify if SCM provided the Snooper with access to any patients' addresses, telephone numbers, birthdates, genders, and health

services numbers. In response via email on February 26, 2025, the SHA confirmed, "this information is available in SCM."

[51] For this reason, the notification letters should have included a warning about the risk of identity theft and set out the actions that individuals could take to mitigate the risks.

[52] Most critically, however, in its notification letter, the SHA failed to convey to affected individuals the steps taken by the SHA to mitigate harm and prevent future breaches. In this case, it would have been reasonable to provide affected individuals with:

- The Snooper's name.
- An indication of how many breaches occurred and when.
- A summary of how the investigation was conducted.
- The consequences for the Snooper imposed by the SHA or other authorities.

[53] To this end, I draw the SHA's attention to my previous Investigation Report 203-2019, 214-2019, 257-2019, wherein at paragraph [68], I stated:

> … 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. … 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.
>
> [Emphasis added]

[54] Similarly, regarding disclosing employee discipline, my office communicated the following to the former Saskatoon Regional Health Authority in Investigation Report 100-2015 at paragraphs [23] and [27]:

> [23] … given the seriousness of employee snooping and how it undermines patient trust, … there is a public interest disclosure of such personal information … **The disclosure would help to provide closure to affected individuals ... It could also help to restore Saskatchewan residents' trust that the health [authority] is protecting personal health information appropriately.**

> …
>
> [27] … I strongly recommend that SRHA disclose the disciplinary action taken against employees who snoop.
>
> [Emphasis added]

[55] Other jurisdictions throughout Canada have arrived at the same conclusion: that is, the identities of (and disciplinary actions taken regarding) snoopers *should be disclosed*. For example, the former Ontario Information and Privacy Commissioner emphasized the following in Order HO-010 at page 32:

> Accessing a patient's personal health information in an unauthorized manner is a serious violation of an individual's privacy and security of the person. In such a situation, the aggrieved individual has a right to a complete accounting of what has occurred. **In many cases, the aggrieved parties 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.**
>
> [Emphasis added]

[56] Moreover, the former Prince Edward Island Information and Privacy Commissioner stated in Breach Report HI-18-005 at paragraph [72]:

> … In most circumstances individuals who interact with a health care provider should know who is accessing their personal health information. In the case of a snooper, citizens have a heightened need to know the identity of the snooper, for various reasons, but primarily to identify whether the snooper is someone with malicious intentions.

[57] Therefore, I find that the SHA did not take appropriate action in terms of providing notice of the privacy breaches to the 70 affected individuals.

[58] According to Breach Report HI-18-005, the health authority involved in the case offered an electronic log to those affected individuals who sought the name of the snooper and/or the dates of each unauthorized access to their personal health information. However, the former Commissioner recommended at paragraph [73] of the report that:

> … in future, [the health authority should] reference the electronic log in their notification letter, and enclose a copy of an excerpt from the electronic log which applies to the affected individual, highlighting the access(es) which reflect the breach, including the date(s) and the name of the snooper.

[59] The above presents a practical strategy that could have been employed in the privacy breaches at issue here.

[60] To that end, I recommend that SHA re-issue notification letters that include copies of excerpts from the SCM records which apply to each affected individual, highlighting the access(es) which reflect the breach(es), including dates of unauthorized accesses and the name of the snooper.

[61] In tandem with that re-issuance, I recommend that the SHA ensure, going forward, privacy breach notifications to affected individuals include the elements detailed at paragraph [41] of this Investigation Report.

[62] Further, I recommend that the SHA ensure, going forward, when snooping is identified, notification letters include copies of excerpts from electronic logs which apply to the affected individual, highlighting the access(es) which reflect the breach(es), including the dates of unauthorized accesses and the name of the snooper.

[63] Next, I must consider how the SHA notified other relevant organizations. The SHA notified its privacy officer of the privacy breaches within a reasonable amount of time. In addition, the SHA provided notice to the College of Registered Nurses of Saskatchewan at the conclusion of its investigation into what it considered the Snooper's professional misconduct, by way of letter dated October 23, 2024. I commend the SHA for ensuring this notification was provided. However, the SHA proactively reported the privacy breaches to my office more than 30 calendar days after the investigation concluded and more than eight months after it first learned of the possible breaches. The purpose of my office's proactively reported breach process is so my office can provide support and assistance throughout the trustee's navigation of the four best practice steps. This ensures the trustee can advise

affected individuals in its notification letters (and inform the public, when necessary) that it is working with my office.

[64] I recommend that, within 30 days of issuance of this Investigation Report, the SHA amend its policies and procedures to proactively notify my office of the breaches of privacy within ten calendar days of initiating its "containment" of a breach, and to provide my office with a copy of its amended policies and procedures.

Investigated the breach

[65] Once the breach has been contained and appropriate notification has occurred, the trustee must conduct an internal investigation. My office outlines specific questions to be considered as part of an effective investigation, which should address the incident on a systemic basis and include a root cause analysis, with a consideration of section 16 of HIPA, which sets out a trustee's duty to protect personal health information. At the conclusion of its investigation, the trustee should have a solid grasp on what occurred which helps inform how to prevent future breaches.

[66] Questions to ask during an investigation include:

- When and how did your organization learn of the privacy breach?
    - Has the privacy breach been contained?
    - What efforts has your organization made to contain the breach?
- What occurred?
    - What type of breach occurred (e.g., collection, use, disclosure, accuracy, etc.)?
    - What personal health information was involved in the privacy breach?
    - When did the privacy breach occur? What are the timelines?
    - Where did the privacy breach occur?
- How did the privacy breach occur?
    - Who was involved?
    - What employees, if any, were involved with the privacy breach?

  - What privacy training have they received?
  - Who witnessed the privacy breach?
  - What factors or circumstances contributed to the privacy breach?
  - What is the root cause of the breach?

- What is the applicable legislation and what specific sections are engaged?

- What safeguards, including policies and procedures, were in place at the time of the privacy breach?

- Was the duty to protect met?

  - Were the safeguards followed?
  - If no safeguards were in place, why not?
  - Were the individuals involved aware of the safeguards?

- Who are the affected individuals?

  - How many are there?
  - What are the risks associated to a privacy breach involving this information (e.g., is the affected individual at risk for identity theft, health insurance fraud, etc.)?
  - Have affected individuals been notified of the privacy breach?

(*Privacy Breach Guidelines for Trustees*, p. 5)

[67] My office has established that, when employee snooping is suspected, the following elements warrant extensive consideration as part of the investigation:

- Record details of how the breach came to light.

- Suspend employee's access to the personal health information.

- Retrieve log information if available.

- Interview the employee in question (establish if the employee may have shared their user account and identification and routinely logged out of account).

- Identify and interview any witnesses.

- Review the privacy training the employee in question has received (have warnings of routine audits been given?).

- Review any relevant contracts.

- Consider who needs to be notified (e.g., supervisor, union, police, e-Health Saskatchewan, etc.).

- Decide if the identity of the employee in question will be disclosed to the affected individual when providing notification.

- Proactively report to the IPC for further advice.

(*Privacy Breach Guidelines for Trustees*, p. 6)

[68] I will now consider these critical factors in relation to the SHA's handling of its internal investigation into the Snooper's actions.

[69] Based on a review of materials provided by the SHA, it appears the SHA took the following steps in its investigation:

- The SHA retrieved and reviewed audit reports.
    - These audit reports focused on the unauthorized accesses of the Snooper and captured whose personal health information was breached, what page(s) within SCM were viewed, when each access occurred, and where.

- The SHA conducted an interview.
    - The SHA began its interview on May 27, 2024, then continued and concluded the interview on August 13, 2024. The Snooper, as well as two Saskatchewan Union of Nurses (SUN) representatives and an SHA labour relations specialist, were present for the interview.
    - No additional witnesses were identified in relation to these unauthorized accesses to warrant interviews.

- The SHA evaluated some of the safeguards it had in place.
    - The SHA required the Snooper to complete its *Privacy Training 2023* module on November 6, 2023.
    - As part of its *Privacy Training 2023* module, the SHA provided the Snooper with the opportunity to review its *Pledge of Confidentiality* and, thereby, facilitated the opportunity to ponder and probe the obligations communicated in the trustee's document.

[70] Further, in its internal investigation report, the SHA determined from its investigation that, "Administrative Safeguards were not followed. Although [the Snooper] had completed the privacy training on November 6, 2023, [they] stated that [they] didn't understand the seriousness of it."

[71] Based on the actions taken, I find that the SHA appropriately investigated the privacy breach.

Taken steps to prevent future breaches

[72] The most important part of responding to a privacy breach is the implementation of measures to prevent similar future breaches from occurring. To do so, my office recommends that a trustee address the following questions:

- What steps can be taken to prevent a similar privacy breach?
  - Can your organization create or make changes to policies and procedures relevant to this breach of privacy?
  - Are additional safeguards needed?
  - Is additional training needed?
  - Should a practice be stopped?

(*Privacy Breach Guidelines for Trustees*, p. 6)

[73] Clearly, the SHA's primary response to preventing future privacy breaches was to terminate the Snooper's employment. However, the SHA also outlined what it referred to as, "long-term strategies the SHA would take to correct the situation," replicated below:

- The SHA now requires all staff to take [a] Privacy Training [module] annually. A new training module will be developed each year. Staff will also read and virtually re-sign the confidentiality pledge.
- Routine auditing of SHA electronic systems.

- Monthly messages in 'Rounds' (email sent to all SHA staff) that speak to a specific privacy subject.

[74] I will now comment on each of the preventative measures identified above by the SHA.

[75] The importance of meaningful training is highlighted by the Nova Scotia Information and Privacy Commissioner in Investigation Report IR23-01 at paragraph [197]:

> Proper onboarding of users to electronic information systems is not the only relevant information practice to protect against unauthorized access to personal health information. Employees also need proper training about what they can look up within the access granted to them. Just because a user has system access does not mean that they are authorized to look at everything they have access to. This is where the role of training becomes important. …

[76] The SHA facilitated access to its training modules for my office. I will comment here on its newest training module, *Privacy Training 2024: Privacy and the Need-to-Know*, available since spring of 2024, which is more comprehensive than its predecessor in the following ways:

- It describes access to information and privacy legislation in Saskatchewan, specifically *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) and HIPA.
- It provides a definition of what constitutes personal health information.
- It emphasises the "need-to-know" principle, including a direct emphasis on the SHA's rejection of the "Circle of Care" model and inclusion of its Need to Know versus Circle of Care directive.
- It imparts warnings about audits and the digital traces evident in the SHA's electronic systems.
- It comments on snooping, gossiping, and the public discussion of PHI, overtly stating that the names of snoopers may be released to affected individuals.
- It discusses privacy breaches in the forms of unauthorized collections and uses, notably drawing upon a wide array of examples of privacy breaches relevant to a health-care environment.
- It addresses how to respond to privacy breaches, with a focus on containment, notification, and prevention.

- It highlights high-profile cases wherein snoopers working in healthcare environments have been prosecuted.

[77] As of March 21, 2025, a new training module for the year is not yet available.

[78] As an extension of its 2024 training module, the SHA has stated that it requires employees to sign its *Pledge of Confidentiality* annually. The active version of the document (signed electronically within the *Privacy Training 2024: Privacy and the Need-to-Know* module) was updated on August 29, 2024. The SHA's requirement for employees to sign its *Pledge of Confidentiality* annually is a reasonable preventative measure. However, I encourage the SHA to place greater emphasis on educating its staff about the potential for prosecutions borne from privacy breaches within this pledge, as it is silent on this possibility. To this end, I, again, look to the Nova Scotia Information and Privacy Commissioner's emphasis in Investigation Report IR23-01 at paragraph [204]:

> In terms of the training and confidentiality pledge content, one glaring topic missing from training and the confidentiality pledge is the issue of prosecutions for privacy breaches. When the OIPC investigator asked an employee found to have breached privacy whether they were aware that prosecution was a potential consequence of employee snooping, they indicated they were not. The employee explained that this knowledge would have influenced their decision to snoop. **It should be plain in any training going forward that prosecution could be a direct consequence of employee snooping, including adding it to the list of actions that may be taken for violations contained in [the trustee's] confidentiality pledge**.
>
> [Emphasis added]

[79] I will now consider the role of routine auditing as a preventative measure. As noted earlier in this Investigation Report, the SHA was alerted to the unauthorized accesses as a result of a review of audit logs. However, this did not appear to be part of an existing audit policy. In its internal investigation report provided to my office, the SHA indicated that it was, "… in the process of standardizing our proactive auditing in SCM." After further inquiry by my office, it stated, "The SHA does not have an Audit Policy. We re [sic] working on building standard auditing processes." However, in its correspondence with my office, the SHA did not explain its timelines for drafting, implementing, and assessing a pending audit policy, nor did it convey what information it would be looking to trace in its audits.

[80] I am concerned that the SHA has not achieved the development of an auditing work standard for SCM, or, more importantly, all of its electronic information systems, in 2025. The idea of proactive or routine auditing is not a new concept. In jointly issued resource *Audit and Monitoring Guidelines for Trustees*, developed with eHealth Saskatchewan, my office emphasized, "it is mandatory for trustees to monitor the access of this information by staff within their organization" (p.2). In 2014, the former Ontario Information and Privacy Commissioner noted the dual detection and deterrence functions of audits in Order HO-013:

> Audits are essential technical safeguards to protect personal health information. They can be used to deter and detect collections, uses and disclosures of personal health information that contravene [Ontario's *Personal Health Information Protection Act*]. In this way, they help maintain the integrity and confidentiality of personal health information stored in electronic information systems. … (p. 1).

[81] Similarly, the Nova Scotia Information and Privacy Commissioner established in Investigation Report IR23-01:

> [209] … an important information practice to prevent unauthorized user access to electronic information systems is to monitor user access. **Even when custodians have reasonable role-based access onboarding procedures and implement training to teach employees what access is unauthorized, it is possible that some employees may still snoop. That is why access still needs to be continually monitored.** With electronic information systems, this monitoring is typically done by way of system auditing.
>
> …
>
> [212] For audits to work as a technical safeguard, electronic information systems must first be able to log all instances where users have viewed personal health information. Then, **the audit reports must be monitored proactively for high-risk behaviors on a regular basis**, as well as in response to complaints. …
>
> [Emphasis added]

[82] I recommend that, within 30 days of issuance of this Investigation Report, the SHA finalizes its proactive or routine audit policy for SCM and provides it to my office.

[83] I will now consider the role of the SHA's monthly "Rounds" messages as a preventative method. My office asked the SHA to provide examples of messages in "Rounds." Here is a summary of the content conveyed in these messages, some deployed and some pending:

- "Meet the Privacy Unit" (November 26, 2024) explained the role of privacy and access department.
- "Faxing Tips" (December 17, 2024) outlined reminders for sending fax communications.
- "Need to Know" (January 14, 2025) defined the titular principle and directs readers to ensure that they have completed the training module about it.
- "Securing Information" (February 11, 2025) provided suggestions for how to keep records and documents from being subject to a privacy breach.
- "Patients and families [sic] recordings at SHA" (March 11, 2025) addressed whether SHA staff can be recorded while providing care.
- "Social media" (April 15, 2025) advises staff to never reference work in personal social media accounts and it directs readers to complete a training module about it.

[84] In addition, each of these messages provides an invitation to contact the area privacy officer for guidance on privacy-related issues.

[85] While establishing ongoing communication between the privacy office and staff of the SHA can be of value, I am curious how the SHA will measure the impact of these messages. Given that there is no action item associated with these messages, it is entirely possible that these messages remain unread in the inboxes of busy health professionals. I urge the SHA to consider incorporating a "read receipt" and an action item to be associated with each "Rounds" message to gauge who is reading the messages and how effective they might be.

[86] I will now consider additional factors relevant to preventative measures.

[87] While the SHA did employ reasonable safeguards in the form of its privacy training module and *Pledge of Confidentiality*, a relevant safeguard would have been the presence of a policy wherein the SHA restricts or revokes access to the electronic health record at the

outset of an internal investigation into snooping. As previously discussed at paragraph [34], the SHA did not employ this safeguard. The Snooper had access throughout most of the SHA's investigation. I believe that the SHA has greater responsibility in protecting personal health information, pursuant to section 16 of HIPA.

[88] Moreover, my office has previously established the preventative value of identifying a snooper by name. In considering the SHA's response to snooping in Investigation Report 203-2019, 214-2019, 257-2019, at paragraph [68], I asserted: "… publicly identifying the snooper and the disciplinary action taken against the snooper would be a strong deterrent for other employees and contractors." This is echoed in Investigation Report 100-2015, which emphasized at paragraph [23]:

> The disclosure would … also act as a deterrent to snooping by other employees. It could also help to restore Saskatchewan residents' trust that the health region is protecting personal health information appropriately.

[89] In a previous investigation about a similar type of privacy breach by a health care professional, the former Ontario Information and Privacy Commissioner emphasized in Order HO-010 at page 32:

> For other staff members of the hospital involved, **knowing that all of the details of the disciplinary action imposed will be publicly disclosed, should serve as a strong deterrent.** This is especially true if those details also become known to other employees, either through the actions of the aggrieved individual, the custodian, or both.
>
> [Emphasis added]

[90] By contrast, in its notification letter to affected individuals, the SHA did not identify the Snooper by name, nor did it directly state that the Snooper's employment was terminated as a result of its investigation into their snooping. Further, the SHA did not notify staff as to the circumstances of the Snooper's termination of employment. In other words, the SHA did not employ identification of the Snooper by name (and the disciplinary actions taken against them) as preventative measures.

[91] As a result of all of the above, I find that the SHA has not taken appropriate steps to mitigate or prevent breaches of a similar nature from occurring again in the future.

[92] I recommend, as a deterrent to future snooping, the SHA notify its staff of the name of this Snooper and of the disciplinary actions taken in relation to this Snooper's privacy breaches.

5. Should my office recommend prosecution of the Snooper under section 64 of HIPA?

[93] At this time, I must consider if the privacy breaches at issue warrant consideration of prosecution of the Snooper pursuant to section 64 of HIPA.

[94] There is a precedent in Canada to prosecute snoopers who violate privacy. In his publication entitled, *Detecting and Deterring Unauthorized Access to Personal Health Information* (January 2015), the former Commissioner in Ontario advocated for an increase in the number of prosecutions of those who snoop. He emphasized:

> The fact that charges may be laid will be an effective deterrent only to the extent that custodians and their agents believe that such measures are going to be used in appropriate circumstances. Given the current pervasiveness of the problem of unauthorized access, it may be necessary to increase the number of prosecutions to warn custodians and their agents that unauthorized access is not acceptable and will not be tolerated.

[95] By its nature, snooping is harmful and intrusive, and it erodes the public's trust in an institution. With the personal health information of 70 patients involved in these privacy breaches, it is necessary to consider the merit of a prosecution in this case: not only to ensure justice for the individuals made vulnerable by the unauthorized accesses, but also to definitively impart that trustees and employees will be held accountable for these violations under HIPA.

[96] In Saskatchewan, snoopers of personal health information could be subject to the offence provisions in section 64 of HIPA. In the present case, subsections 64(1)(a) and (3.2) of HIPA deserve consideration:

> **64**(1) No person shall:
>
> (a) knowingly contravene any provision of this Act or the regulations;
> …
>
> (3.2) An individual who is an employee of or in the service of a trustee and who wilfully accesses or uses or directs another person to access or use personal health information that is not reasonably required by that individual to carry out a purpose authorized pursuant to this Act is guilty of an offence and is liable on summary conviction to a fine of not more than $50,000, to imprisonment for not more than one year or to both, whether or not the trustee has been prosecuted or convicted.

[97] To induce employees' compliance with HIPA, the SHA has instituted some policies and procedures pursuant to sections 16 and 23. For example, the SHA's *Privacy and Confidentiality* policy clearly defines the term "need-to-know" and emphasizes that team members are to access and review only information they need-to-know for their job duties. Similarly, the SHA's *Acceptable Use of Information Technology (IT) Assets* policy clearly establishes that employees are subject to LA FOIP, HIPA, and other applicable legislation. Further, the SHA confirmed that the Snooper signed the *Pledge of Confidentiality* in 2023. That document required the Snooper to acknowledge and agree that they would only view, use, or disclose confidential information with a legitimate need-to-know.

[98] Based on information provided by the SHA, I find that the Snooper should have known that their actions would be in contravention of the training they received (and policies and procedures of which they were made aware), and subsequently, be in violation of HIPA. Although the Snooper claims to not have understood the seriousness of the offence, this is not an excuse for violating the law.

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

IV FINDINGS

[100] I find that I have jurisdiction to investigate this matter.

[101] I find that privacy breaches occurred.

[102] I find that the SHA did not appropriately contain the privacy breaches.

[103] I find that the SHA did not take appropriate action in terms of providing notice to the 70 affected individuals or my office of the privacy breaches.

[104] I find that the SHA appropriately investigated the privacy breach.

[105] I find that the SHA has not taken appropriate steps to mitigate or prevent breaches of a similar nature from occurring in the future.

[106] I find that, based on information provided by the SHA, the Snooper should have known that their actions would be in contravention of the training they received (as well as policies and procedures of which they were made aware), and subsequently, would be in violation of HIPA.

V RECOMMENDATIONS

[107] I recommend that, within 30 days of issuance of this Investigation Report, the SHA amend its policies and procedures to revoke or restrict an employee's access to personal health information in electronic health records at the outset of any internal privacy breach investigation and provide my office with a copy of its amended policies and procedures.

[108] I recommend that SHA re-issue notification letters that include copies of excerpts from the SCM records which apply to each affected individual, highlighting the access(es) which reflect the breach(es), including dates of unauthorized accesses and the name of the snooper.

[109] I recommend that the SHA ensure, going forward, privacy breach notifications to affected individuals include the elements detailed at paragraph [41] of this Investigation Report.

[110] I recommend that the SHA ensure, going forward, when snooping is identified, notification letters include copies of excerpts from electronic logs which apply to the affected individual, highlighting the access(es) which reflect the breach(es), including the dates of unauthorized accesses and the name of the Snooper.

[111] I recommend that, within 30 days of issuance of this Investigation Report, the SHA amend its policies and procedures to proactively notify my office of the breaches of privacy within ten calendar days of initiating its "containment" of a breach, and to provide my office with a copy of its amended policies and procedures.

[112] I recommend that, within 30 days of issuance of this Investigation Report, the SHA finalizes its proactive or routine audit policy for SCM and provides it to my office.

[113] I recommend, as a deterrent to future snooping, the SHA notify its staff of the name of this Snooper and of the disciplinary actions taken in relation to this Snooper's privacy breaches.

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

Dated at Regina, in the Province of Saskatchewan, this 31st day of March, 2025.

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