Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 155-2025[1]

Saskatchewan Health Authority and Marianne Mann

January 23, 2026

Summary: The Saskatchewan Health Authority (SHA) proactively reported a privacy breach to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC). This was after a discovery that an employee (Snooper), working at the Dr. F.H. Wigmore Regional Hospital in Moose Jaw (Moose Jaw Hospital), accessed their own personal health information and the personal health information of 98 individuals (affected individuals) in the Sunrise Clinical Manager (SCM) without legal authority. OIPC investigated the incident under *The Health Information Protection Act* (*HIPA*) and found that the Snooper did not have the lawful authority to access (use) their own personal health information and the personal health information of the affected individuals. The situation was aggravated by the fact that the Snooper used inappropriately accessed information from SCM to engage a colleague in a conversation with respect to their personal health information. The Snooper also inappropriately disclosed information about a family member's hospital admission. The privacy breach involved 102 inappropriate accesses in SCM over the course of 11.5 months prior to its discovery.

The Commissioner made the following findings: (1) SHA did not adequately contain the privacy breach as soon as it could have; (2) SHA provided appropriate and timely notice to the affected individuals upon discovery of the privacy breach; (3) SHA had insufficient administrative safeguards related to proactive auditing in place at the time of the privacy breach; (4) SHA took reasonable steps in auditing the Snooper's accesses in SCM once the privacy breach was discovered and that SHA took reasonable steps to investigate the privacy breach; (5) SHA had appropriate administrative safeguards for privacy training in place at the time the privacy breach occurred; (6) the root cause of the privacy breach was failure

[1] This office opened OIPC file 155-2025 on June 19, 2025, when SHA proactively reported the privacy breach. On the same day, this office opened a second investigation file, OIPC file 156-2025, with respect to the Snooper. This Investigation Report explains the investigation with respect to both parties and involves both files.

on the part of the Snooper to adhere to the administrative safeguards that were in place at the material time; and (7) the Snooper willfully and knowingly violated *HIPA* in this matter. The Commissioner made recommendations from the above findings.

TABLE OF CONTENTS

I BACKGROUND

[1] On June 19, 2025, the Saskatchewan Health Authority (SHA) proactively reported a privacy breach to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC) under *The Health Information Protection Act* (*HIPA*).[2]

[2] The privacy breach involved allegations of snooping by an employee of SHA. The employee (Snooper) was a Unit Clerk in the Emergency department at the Dr. F.H. Wigmore Regional Hospital in Moose Jaw (Moose Jaw Hospital). In their role as a Unit Clerk, the Snooper had access to the Sunrise Clinical Manager (SCM) database. SHA noted that the employee's access to SCM was appropriate for their role in a limited capacity only.[3]

[3] SCM is the electronic acute care record database that is used in the hospital for each admitted patient. SHA outlined that the SCM database collects the following information: patient's name, date of birth, health services number, and the details of a patient's acute care visit.

[4] On August 6, 2025, SHA provided OIPC with its *Report of Personal Information/Personal Health Information Privacy Breach* (internal privacy breach report) dated June 24, 2025. SHA also provided this office with the contact information for the Snooper. SHA stated that it became aware of a potential privacy breach when the Snooper approached another employee of the Moose Jaw Hospital (the Witness) and asked about their personal health information with respect to a recent hospital stay that the employee had heretofore kept strictly private.[4] The Witness reported the conversation to their manager on April 23, 2025.

---

[2] *The Health Information Protection Act*, S.S. 1999, c. H-0.021, as amended.

[3] The "Unit Clerk" job description included the following key activities: the booking of patient appointments, the arranging of patient transfers to other units/facilities, the assembling of patient discharge and special needs packages, and other such clerical duties.

[4] This individual will be referred to as "the Witness".

The Witness was upset and correctly believed that only a breach of privacy could account for the Snooper's knowledge.

[5] SHA commissioned a total of six audits of the Snooper's accesses to SCM over the timeline from July 1, 2024 to June 16, 2025. SHA also prepared a breach spreadsheet based on the audit results. The spreadsheet lists 102 inappropriate accesses.[5] The audits and the Snooper's inappropriate accesses listed in the spreadsheet can be summarized as follows:

Audit Timeframe	**Number of Inappropriate Accesses**
February 1, 2025 to May 15, 2025 (Conducted on May 15, 2025)	73 inappropriate accesses
January 1, 2025 to February 1, 2025 (Conducted on June 10, 2025)	9 inappropriate accesses
November 1, 2024 to December 31, 2024 (Conducted on June 11, 2025)	11 inappropriate accesses
September 1, 2024 to October 31, 2024 (Conducted on June 11, 2025)	No inappropriate access
July 1, 2024 to August 31, 2024 (Conducted on June 11, 2025)	9 inappropriate accesses
May 15, 2025 to June 16, 2025 (Conducted on June 16, 2025)	No inappropriate access

[5] SHA confirmed that a representative from Labour Relations and the Manager reviewed the audit reports to ensure that the spreadsheet reflected the unauthorized views. The spreadsheet contains the following columns: Patient Name, Date of Event, Type of Event, Employee Response, and Other/Correlation to Employee. Based on a review of this spreadsheet, there were 102 inappropriate accesses by the Snooper into SCM over the course of 11.5 months – this includes the access of one individual's record on three separate dates and two separate dates where the Snooper accessed their own record. The 102 inappropriate accesses in SCM includes the Snooper's access into their own record twice and accesses into the records of 98 other individuals.

[6] SHA concluded that the Snooper accessed their own personal health information and the personal health information of 98 other individuals in SCM without legal authority between July 1, 2024 and June 16, 2025.

[7] SHA suspended the Snooper's employment on June 16, 2025 and terminated the Snooper on July 2, 2025. As previously noted, SHA proactively reported to this office on June 19, 2025.

[8] On August 12, 2025, OIPC notified SHA that an investigation would be commenced. On September 11, 2025, SHA provided this office with its internal privacy breach report, dated August 13, 2025.

[9] On August 12, 2025, OIPC notified the Snooper of its investigation into the privacy breach. Among other things, the notice informed that this office would be investigating whether there was a willful violation of the legislation and that the investigation could lead to a public report and possible naming and referral to the Attorney General. The Snooper was invited to provide a submission if they wished, and legal counsel was welcome to respond on their behalf. On September 12, 2025, OIPC received a submission from the Snooper.

II DISCUSSION OF THE ISSUES

1. Jurisdiction

[10] *HIPA* is engaged when three elements are present: 1) personal health information; 2) a trustee; and 3) the trustee has custody or control over the personal health information. Below is an analysis to see if HIPA is engaged.

i. First element – personal health information

[11] As noted above, the Snooper worked as a Unit Clerk in the Moose Jaw Hospital during the material time. The Snooper had limited access to SCM in the capacity of their clerical duties. Altogether, the Snooper accessed their own personal health information and the

personal health information of 98 individuals. Based on the details provided by SHA, this included the Snooper inappropriately accessing the records of co-workers and family members who had been admitted as patients at the hospital. In some instances, the Snooper's access to a patients' record occurred after discharge.

[12] The information in SCM constitutes "personal health information" pursuant to sections 2(1)(m)(i), (ii) and (v) of *HIPA* which provides:[6]

> **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;
>
> …
> (v) registration information;

[13] Section 2(1)(q) of *HIPA* defines "registration information" as follows:

> **2** In this Act:
>
> …
> (q) **"registration information"** means information about an individual that is collected for the purpose of registering the individual for the provision of health services, and includes the individual's health services number and any other number assigned to the individual as part of a system of unique identifying numbers that is prescribed in the regulations;

[14] Based on the above analysis, personal health information was accessed such that the first element is present for *HIPA* to be engaged.

[6] OIPC Investigation Report 103-2025, 104-2025 at paragraphs [11] and [12]. In this case it was found that the information in two other SHA electronic medical record databases (MedAccess and OR Manager), contained information that qualifies as personal health information pursuant to sections 2(1)(m)(i), (ii) and (v) of *HIPA*.

ii. Second element – a trustee

[15] SHA qualifies as a "trustee" pursuant to section 2(1)(t)(ii) of *HIPA*. In an email dated October 17, 2025, SHA confirmed that the Moose Jaw Hospital is an SHA facility.

[16] *The Health Information Protection Regulations, 2023* (*HIPA Regulations*) provides the following definition of an employee:[7]

> **2**(1) In these regulations:
>
> …
> **"employee"** means:
>
> (a) an individual:
>
> (i) who is employed by a trustee, including an individual retained under a contract to perform health services for the trustee; and
>
> (ii) who has access to personal health information; or
>
> …
> but does not include a health professional who is retained under a contract that is not an employment agreement, to perform services for the provincial health authority.

[17] In this mater, SHA advised that the Snooper commenced employment with SHA in 2016. The Snooper had access to SCM to carry out their clerical duties for SHA while employed at the hospital. Therefore, the section 2 definition of "employee" pursuant to *HIPA Regulations* applies to the Snooper at the time of the privacy breach.

[18] The Snooper was employed by a trustee such that the second element is present for *HIPA* to be engaged.

[7] *The Health Information Protection Regulations, 2023*, c. H-0.021 Reg 2 (August 1, 2023), as amended by Saskatchewan Regulations 68/2023.

iii. Third element – the trustee must have custody or control over the personal health information

[19] "Custody" is the physical possession of a record by a trustee combined with a measure of control. "Control" connotes authority. Personal health information is under the control of a trustee when the trustee has the authority to manage the information, including restricting, regulating and administering its use, disclosure or disposition. Custody is not a requirement for control to be present.[8]

[20] All the personal health information in the SCM database is stored within the Moose Jaw Hospital, a recognized SHA facility. Therefore, SHA has custody and control of the personal health information in question and the third element is present for *HIPA* to be engaged.

[21] SHA advised that SCM was the only program to which the Snooper had access that contained personal health information.

[22] OIPC finds that the three elements are present for *HIPA* to be engaged and OIPC has jurisdiction to undertake this investigation under the jurisdiction afforded by *HIPA*.

2. Did a privacy breach occur?

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

[24] "Use" is defined at section 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.

[8] OIPC Investigation Report 306-2019 at paragraphs [15] and [16].

[25] *HIPA* does not define the term "disclosure." This office defines "disclosure" as the sharing of personal health information with a separate entity, not a division or branch of the trustee in custody or control of that information.[9]

[26] In the case at hand, the Snooper accessed their own personal health information and that of 98 other individuals in SCM. Employees working within the health system in Saskatchewan cannot access their own personal health information without the requisite "need to know" precondition as supplied by the normal course of employment duties. User privileges are granted to allow employees access to patient information in electronic databases/systems so they may perform their tasks. Prurient interest cannot factor as a viable requirement to access others' personal health information, or even one's own. In this case, the Snooper conceded the impropriety of their actions in viewing their own records on SCM. The Snooper's access to others' records or their own personal health information in SCM was never prefaced with the required "need to know" as part of their employment and therefore cannot constitute authorized use.

[27] In another instance, the Snooper used the personal health information accessed in SCM to engage in a discussion with the Witness about their pregnancy which the Witness was keeping secret. When asked about this incident at an internal meeting, the Snooper claimed a lack of memory but also conceded the information came from a SCM viewing.

[28] In another instance, the Snooper admitted to disclosing personal health information gleaned from SCM to inform someone in their family that an estranged family member had been admitted to the Moose Jaw Hospital.

[29] This office provided the Snooper with notice of this investigation. The Snooper was offered an opportunity to file a submission and on September 12, 2025, OIPC received the Snooper's submission. The Snooper outlined their reasons for accessing personal health information in SCM while performing the role of Unit Clerk. The Snooper acknowledged the impropriety of their actions with the following concessions:

[9] OIPC Investigation Report 293-2024; 009-2025 at paragraph [20].

- I was totally in the wrong for checking my co-workers record but I did it out of compassion as I genuinely care about my co-workers. Honestly after I spoke to [them], I realized that I had been a fool and that I should have kept my mouth shut. It was not my intent to upset [them]. I should have apologized immediately but I did not and I feel bad for that. I am very sorry for my actions and never meant to cause that [person] more heart ache and grief.

- I should not have accessed my [family member's] records and I knew it was wrong and that I could get a into trouble for it. I truly care about my [family member's] and what happens to [them] although through a series of unfortunate events [they] want nothing to do with me.

- I also knew that it was wrong to check my own results and that I should have looked on my phone. I just felt so lousy and wanted to know what was wrong with me and go home…

[30] The "use" of personal health information occurs when personal health information is accessed/viewed on SCM by an employee of SHA. The SHA investigation revealed that: 1) the Snooper accessed their own personal health information; and 2) the Snooper accessed the personal health information of other patients, and in one instance, spoke to the Witness about their personal health information. The Snooper's access to personal health information records in SCM and the discussion with the Witness constituted a "use" within section 2(1)(u) of *HIPA*.

[31] The Snooper conceded that they disclosed personal health information via text message to a family member to inform that another family member had been admitted to the Moose Jaw Hospital. This constitutes a "disclosure" of personal health information.

[32] The authority to collect, use and disclose personal health information is set out in *HIPA*. This authority is subject to the overarching rule that trustees and their employees should only collect, use or disclose personal health information where reasonably necessary for the authorized purpose in connection with the valid fulfillment of their employment duties. These rules or principles are commonly referred to as the "need-to-know" and "data minimization" principles and are set out in section 23 of *HIPA* which states, in part, 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.

[33] Section 26 of *HIPA* is also relevant because it further restricts the *use* of personal health information by trustees in absence of the consent of the subject individual. Obviously, consent is not an issue in this analysis because consent for any of the uses/disclosures on the part of the Snooper was never obtained from any of the violated parties. Section 26 of *HIPA* provides:

> **26**(1) A trustee shall not use personal health information in the custody or control of the trustee except with the consent of the subject individual or in accordance with this section.
>
> (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.

[34] Section 27 of *HIPA* restricts the *disclosure* of personal health information by trustees in absence of the consent of the subject individual, unless it is for a specific enumerated authorized purpose. Once again, consent is clearly not an issue in this analysis for the reason that consent was never sought or given in this case.

[35] SHA confirmed that the Snooper intentionally accessed health records in SCM without a need to know. SHA provided this office with the relevant audit reports from SCM that confirmed the unauthorized accesses on multiple occasions, as well as a spreadsheet prepared from a compilation of the audits. There were six audits completed in total as

explained in paragraph [5] of this Investigation Report. The audits and subsequent interviews conducted with the Snooper confirmed the inappropriate accesses of personal health information on SCM between July 1, 2024 and June 16, 2025.

[36] This office has previously defined "snooping" as the "unauthorized access to personal information or personal health information by employees without a need-to-know."[10] Based on the audits and investigation undertaken by SHA of the Snooper's accesses, these accesses were not for a program, activity or in the service of the trustee, they were not in the course of providing patient care, and consent was never obtained from the affected individuals[11]. The Snooper's accesses in SCM is correctly identified as snooping.

[37] There is a finding that the Snooper did not have lawful authority to access SCM to: (1) view their own personal health information absent the requisite "need to know"; (2) access the personal health information of the 98 affected individuals without the requisite "need to know"; (3) speak to the Witness about their personal health information; and (4) disclose the personal health information of one family member to another family member.

3. Did SHA respond to the privacy breach appropriately?

[38] There are four main determinants of whether a trustee's response to a privacy breach is appropriate. Section 7-7 of OIPC *Rules of Procedure* sets out the considerations. Did the trustee:

a) Contain the breach (as soon as possible);
b) Notify affected individuals (as soon as possible);
c) Investigate the breach;
d) Take steps to prevent future breaches.

[10] OIPC Investigation Report 193-2024, 043-2025 at paragraph [35].

[11] SHA provided OIPC with its interview notes with the Snooper. In one of the instances, the Snooper explained that an individual asked them to look up their record in SCM while the individual was "standing over my shoulder." Even if this could be construed as consent, access to patient records should not be provided in this fashion. Further, this type of access was not part of the Snooper's employment contractual duties.

[39] What follows is an analysis of the response by SHA to the privacy breach.

a) Containment of the Breach

[40] The following is a detailed timeline of key events based on information provided to this office from SHA. This timeline is crucial in understanding the actions on the part of both the Snooper and SHA during the material time and to fully understand the background to containment:

- **April 28, 2016** – Snooper signed a *Confidentiality Pledge* with the former Five Hills Health Region. SHA indicated that all employees receive privacy training during orientation. SHA explained that that the Snooper would have received privacy training on the same day the *Confidentiality Pledge* was signed.

- **July 14, 2024** – First inappropriate Snooper access in SCM.

- **January 14, 2025** – Snooper completed online privacy training (*Privacy Training 2023*) and acknowledged having read, understood and agreed to the terms of the *Pledge of Confidentiality* (*Pledge*).

- **February 13, 2025** – Snooper completed online privacy training (*Privacy Training 2024: Need to Know*) and acknowledged having read, understood and agree to the terms of the *Pledge*.

- **April 18, 2025** – Snooper approached the Witness while at work and asked specific questions regarding Witness' personal health information that was not public.

- **April 23, 2025** – Witness reported the conversation to a hospital Manager.

- **April 29, 2025** – HR contacted the SHA Privacy Office requesting an audit. The Privacy Office requested a Privacy Incident Report Form (PIR) be completed to allow the Privacy Office to determine the parameters of the audit.

- **May 1, 2025** – The PIR was submitted to the SHA Privacy Office.

- **May 11, 2025** – Snooper's last inappropriate access in SCM.

- **May 15, 2025** – First SHA audit of the Snooper's accesses in SCM from February 1, 2025 to May 15, 2025.

- **May 16, 2025 –** Manager reviewed the first audit of the Snooper's accesses in SCM and identified several suspicious accesses.
- **May 30, 2025** – SHA meeting with Snooper to discuss complaint from the Witness and suspicious accesses in SCM.
- **June 10 and 11, 2025** – SHA conducted four additional audits of the Snooper's accesses in SCM.
- **June 16, 2025** – SHA second meeting with Snooper to discuss accesses in SCM that were now identified as unauthorized. Snooper's employment with SHA was suspended.
- **June 16, 2025** – Manager requested a sixth and final audit of the Snooper's accesses in SCM from May 15, 2025 to June 16, 2025. SHA indicated that no further inappropriate accesses were identified in this timeframe.
- **June 19, 2025** – SHA removed the Snooper's access privileges to SCM and network access.
- **July 2, 2025** – Termination of Snooper's employment with SHA.

[41] A trustee should immediately take steps to contain a breach once it is clear that a breach has occurred. These steps will depend entirely on the nature of the breach, but they may include:

- Stopping the unauthorized practice;
- Recovering the records;
- Shutting down the system that has been breached;
- *Revoking or suspending access privilege*; and
- Correcting any weaknesses in physical security.

[42] OIPC applies a standard of reasonableness to assess the containment of a breach. The trustee must demonstrate that it has reduced the magnitude of the breach and the resulting risk to affected individuals.[12]

[12] OIPC Investigation Report 253-2024, 033-2025 at paragraph [23].

[43] In this case, the SHA investigation was triggered by a complaint from the Witness to a Manager on April 23, 2025. SHA met with the Snooper on May 30, 2025 to discuss the results of the initial May 15, 2025 audit that revealed several suspicious accesses to SCM. The results of that interview resulted in the Snooper claiming a general lack of memory for most of the interview. However, the last two matters below involved concrete admissions on the part of the Snooper to having violated *HIPA*:

- The Snooper was asked about an access to a record with an individual that had the same last name as the Snooper. The Snooper claimed a lack of memory.

- The Snooper was asked about an access to the personal health information of the Snooper's family member. The Snooper first conceded this access without the requisite need to know principle but later the Snooper claimed to be the Unit Clerk at the time of the family member's admission.

- When asked about the Snooper's suspicious access to the Witness' personal health information, the Snooper claimed a lack of memory.

- When asked about a suspicious access to the personal health information of fellow employees and patients, the Snooper claimed a lack of memory.

- The Snooper admitted to accessing their own personal health information without the requisite need to know;

- The Snooper admitted to sharing text messages on their phone confirming that they had disclosed personal health information of a family member to another family member and conceded that this was wrong;

[44] Clearly on May 30, 2025 there were, in our opinion, grounds to suspend, if not revoke, the Snooper's access to SCM. The Snooper claimed a lack of memory for many of the suspicious accesses but the last two bullet points above constitute violations of *HIPA*. Despite SHA identifying suspicious accesses in the initial audit conducted on May 15, 2025, and the Snooper's two admissions on May 30, 2025, SHA did not immediately suspend/revoke the Snooper's access to SCM .

[45] This office has recommended that when there are grounds to believe an individual is inappropriately accessing personal health information, SHA should immediately suspend

the individual's access to the electronic medical record.[13] Granted, there were no further inappropriate accesses after May 11, 2025 in this case. The point is that this breach could have been contained much earlier than June 19, 2025.

[46] There is a finding that SHA did not adequately contain the privacy breach as soon as it could have. There will be a recommendation that SHA immediately suspend user accounts when there are grounds to believe that the individual is inappropriately accessing personal health information.

b) Notification to Affected Individuals

[47] OIPC has developed *Privacy Breach Guidelines for Trustees* that provides trustees should notify affected individuals of a privacy breach as soon as possible. This document is based on the findings and recommendations gathered from the collective wisdom of previous investigations and recommended best practices of this office. *Privacy Breach Guidelines for Trustees* outlines the information that should be included in every notice to an affected individual, such as:[14]

- A description of what happened (a general description of what happened).
- A detailed description of the personal health information involved (e.g., name, medical record, etc.).
- A description of the types of harm that may possibly come to them because of the privacy breach.
- Steps taken and planned to mitigate the harm and to prevent future breaches.
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g., how to change a health services number).
- Contact information of an individual within the organization who can answer questions and provide information.

[13] *Supra*, footnote 6 at paragraph [38].

[14] OIPC resource *Privacy Breach Guidelines for Trustees* at pages 3 and 4.

- A notice that individuals have a right to complain to the OIPC.
- Recognition of the impacts of the breach on affected individuals and an apology

[48] On June 27, 2025, SHA provided written notification via letter to all the affected individuals, except the Witness. On July 3, 2025, the Witness received a hand delivered letter from the Manager and SHA. This timeline for notification was reasonable. As of the date of this Investigation Report, no affected individuals have submitted a formal complaint to this office.

[49] SHA provided OIPC with a copy the notification letter sent to the affected individuals. The notification letter is sufficient in that it referenced the most vital elements of the breach. The letter included instructions for affected individuals to request a full report of the inappropriate accesses to their SCM record and included contact information for an SHA employee. OIPC applauds SHA for its transparency to the affected individuals. There will be a finding that SHA provided appropriate and timely notice to the affected individuals upon discovery of the privacy breach.

c) Investigation of the Breach

[50] Once containment has been addressed and appropriate notification of affected individuals, the trustee must investigate the privacy breach. The investigation must address the incident on a systemic basis and include a root cause analysis and conclusion. This office has previously outlined the following recommended steps for trustees when investigating an allegation of snooping:[15]

- Record the details of how the breach came to light.
- Confirm that the employee's access to the electronic database has been suspended/revoked.
- Retrieve the information log, if available.

[15] *Supra*, footnote 6 at paragraph [45].

- Interview the employee in question (establish if the employee may have shared their user account and identification and/or if they routinely logged out of account).
- Identify and interview witnesses.
- Review and record the privacy training provided to the employee in question.
- Review any relevant employment contracts.
- Outline the parties that must be notified if a breach is found(e.g., supervisor, union, police, eHealth Saskatchewan, affected individuals, etc.)
- Decide if the identity of the employee in question will be disclosed to the affected individual when providing notification.
- Proactively report to OIPC.

[51] The trustee must also consider its duty to protect personal health information as set out in section 16 of *HIPA*. Specifically, section 16 of *HIPA* requires that a trustee establish policies and procedures to maintain administrative, technical and physical safeguards:

> **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:
>
> (a) protect the integrity, accuracy and confidentiality of the information;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the information;
>
> (ii) loss of the information; or
>
> (iii) unauthorized access to or use, disclosure or modification of the information; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[52] In assessing the root cause of a privacy breach, the local authority must formulate safeguards that would prevent future similar breaches from occurring. Safeguards can be administrative (e.g., policies, procedures, confidentiality statements on contracts),

technical (e.g., access controls on electronic storage) or physical safeguards (e.g., locked cabinets or bins, locked doors, security cameras).[16]

i. Auditing (Technical Safeguard) & Auditing Policies (Administrative Safeguard)

[53] SHA initiated its investigation of this matter because of a complaint from a colleague of the Snooper who suspected a privacy breach. The investigation commenced with a short audit of the Snooper's accesses in SCM: February 1 to May 15, 2025.

[54] This office, in conjunction with eHealth Saskatchewan, has produced a helpful resource that outlines the role and timing of audits in a possible privacy breach investigation: *Audit and Monitoring Guidelines for Trustees*.[17] Events that could trigger an audit include:

- An accessor has viewed their own record;
- An accessor views a record or information outside the scope of their practice or employment;
- An accessor views a record of an individual who has the same last name as the user;
- An accessor views a record that belongs to a fellow employee;
- The accessor repeatedly views one record;
- The accessor views records outside of scheduled working hours;
- A record has been viewed that does not have an appropriate service event to match (e.g., a record from 5 years ago was viewed recently, yet there are no recent visits made by the patient);
- A record has been viewed that is associated with a media event (e.g., records relating to a suspected bioterrorism attack);
- A record has been accessed that is associated with a VIP (e.g., celebrities, board members, politicians); and

[16] OIPC Investigation Report 065-2025 at paragraph [31].

[17] OIPC resource *Audit and Monitoring Guidelines for Trustees* at page 4.

- Break-the-glass events (e.g., a user overrides a mask put on an individual's record).

[55] The audits easily retrieved the following inappropriate accesses, but we note that this list is not exhaustive of the infractions in this matter:

1) The Snooper accessed personal health information of patients *after* they were discharged from the unit/hospital;

2) The Snooper accessed personal health information of fellow SHA employees;

3) The Snooper accessed a health record of an individual with the same last name as the Snooper; and

4) The Snooper accessed their own record in SCM.

[56] OIPC has previously commented that auditing is a technical safeguard and is necessary to assess compliance with, and to measure the effectiveness of, policies and procedures. Audits also provide an opportunity to assess compliance with legislation and determine whether appropriate measures are firmly in place to monitor access.[18] There are benefits to conducting regular monitoring/auditing of electronic health records databases to ensure compliance with privacy and security policies. Auditing can also act as a deterrent to unauthorized access. Further, regular proactive audits provide an early opportunity to identify inappropriate access on the part of snoopers.[19]

[57] Through regular proactive auditing of SCM, SHA may have caught the Snooper's inappropriate accesses sooner. Had the Witness not reported the suspected privacy breach that initiated the investigation by SHA, the Snooper may have continued indefinitely.

[18] OIPC Investigation Report 260-2017 at paragraph [33] and Investigation Report 108-2018 at paragraph [38].

[19] *Supra*, footnote 6 at paragraph [57].

[58] In a recent investigation report, SHA acknowledged that it was developing a proactive audit policy.[20] We understand a policy of this nature involves a great deal of work and commitment, still such a policy would have assisted SHA detecting the inappropriate accesses in this case earlier.

[59] There is a finding that there were insufficient administrative safeguards related to proactive auditing in place at the time of the privacy breach. We will not make a recommendation with respect to this finding because SHA has previously committed to the completion of this goal.

[60] In determining the appropriate timeframe for an audit, trustees should also consider what a reasonable timeframe would be to ensure that any unauthorized access are detected, so far as is reasonably possible. OIPC recognizes that conducting audits can be more complicated in cases such as this where the profession of the Snooper requires that they have access to sensitive information regularly and a stress on resources. In this case, SHA conducted a total of six responsive audits of the Snooper's accesses in SCM for the timeframe of July 1, 2024 to June 16, 2025. There is a finding that SHA took reasonable steps in auditing the Snooper's accesses in SCM once the privacy breach was discovered and that SHA took reasonable steps to investigate the privacy breach.

ii. Privacy Training & Pledge of Confidentiality (Administrative Safeguard)

[61] Users of personal health information databases should complete privacy and security training and sign a confidentiality pledge or agreement as a condition of gaining access to systems that contain personal health information. Since August 2023, section 5 of *HIPA Regulations* provides the following, including specific requirements regarding training and pledges of confidentiality:

> **5** To ensure compliance with the Act by its employees, a trustee that has custody or control of personal health information must:

[20] *Ibid*, at paragraph [59], SHA indicated on September 12, 2025 that there was a three to six month timeline for completion of the proactive audit policy.

> (a) provide orientation and ongoing training for its employees about the trustee's policies and procedures respecting the protection of personal health information; and
>
> (b) ensure that each of its employees signs a pledge of confidentiality that includes an acknowledgement that the employee:
>
> (i) is bound by the trustee's policies and procedures mentioned in clause (a); and
>
> (ii) is aware of the consequences of breaching those policies and procedures.

[62] SHA provides online privacy training to its employees, which includes a review of the SHA *Pledge*. The *Pledge* includes a statement that employees complete all mandatory privacy training on an ongoing basis, including the completion of privacy training and a review of the *Pledge* annually.[21] In a recent investigation report involving SHA, this office commended SHA for its excellent privacy training and outlined the topics covered by SHA in its *Privacy Training 2024: Privacy and the Need-to-Know*:[22]

- The access to information and privacy legislation in Saskatchewan, specifically *The Local Authority Freedom of Information and Protection of Privacy Act* (*LA FOIP*) and *HIPA* is discussed.
- The "need-to-know" principle is emphasized.
- Snooping, gossiping, and the public discussion of personal health information is specifically condemned. There is a warning that the names of snoopers may be released to affected individuals.
- A warning is given with respect to management audits and the digital traces evident in SHA electronic systems.
- Privacy breaches in the form of unauthorized collections and uses are condemned and discussed at length.

[21] SHA *Pledge of Confidentiality (Staff and Practitioner Staff)* (August 29, 2024), statement number 5.

[22] *Supra*, footnote 6 at paragraph [48].

[63] SHA explained that all employees receive privacy training during orientation - for the Snooper, this would have occurred in 2016. In addition, SHA provided records demonstrating that the Snooper completed online privacy training on January 14, 2025 and February 13, 2025.

[64] SHA also provided a copy of the former Five Hills Health Region *Confidentiality Pledge* that the Snooper signed on April 28, 2016 which stated, in part, as follows:

> …I the undersigned agree as follows:
>
> (a) That I will only access personal health information on a need-to-know basis for performing services on behalf of the Organization;
>
> (b) That I will keep all personal health information in my possession in the strictest of confidence and only use such information for the purposes of performing services on behalf of the Organization.
>
> …
> (d) That I will follow all applicable Organization security and confidentiality policies, procedures and practices, which include electronic records;
>
> (e) I acknowledge that I have read this Confidentiality Pledge and understand that a breach of it may be in contravention of the *Health Information and Protection Act* or other applicable laws.

[65] SHA indicated that employees accept the *Pledge* at the completion of each online privacy training. The Snooper completed online privacy training on January 14, 2025 and February 13, 2025, and therefore, would have acknowledged they had read, understood and agreed to the terms of the *Pledge* after completing training on those dates. The SHA website includes a copy of the *Pledge* that provides comprehensive training and warranties to cover all aspects of privacy legislation in the health care system in Saskatchewan.[23]

> a) I will only view, use or disclose confidential information legitimate need-to-know;
>
> b) I will keep all confidential information in the strictest of confidence;

[23] *Supra*, footnote 21 at statement number 1.

c) I will only view and use such information for the purpose(s) for which I am granted user rights, and will only disclose that information as permitted by HIPA, LA FOIP, other applicable privacy law, and/or SHA policy;

e) I will not access my own personal information (PI) or personal health information (PHI), unless I make an approved request as per SHA policy;

f) I will not look up any information on my spouse, family members, friends, acquaintances, co-workers etc. without a professional need-to-know. I will not look up birth dates, phone numbers and addresses for personal use;

g) I will not look up patient, client and/or resident's PHI out of curiosity/general interest. It is prohibited;

I acknowledge that I have received and reviewed the Privacy and Confidentiality Policy.

I agree that I am bound by the Privacy and Confidentiality Policy and the statements within this document.

I am aware of the consequences of breaching the Privacy and Confidentiality Policy and the statements within this document.

[66] In their submission to this office, the Snooper confirmed that in spite of the privacy training and the warranties they gave in the *Pledge* during their employment with SHA, they did not understand the "need to know" principle and they never sought clarification.

[67] The Snooper also claimed that they left their computer open and available for others to see while signed on with their own access criteria. In so doing, the Snooper contravened the *Pledge* by abandoning all responsibility for their own computer and online access when leaving it unattended. This issue was clearly explained and confirmed in the *Pledge* accepted by the Snooper on January 14, 2025 and February 13, 2025.

[68] Despite completing the privacy training and acknowledging the *Pledge*, the Snooper continued to snoop in patient records in SCM. It is abundantly clear that the Snooper disregarded their training, contravened the *Pledge* and should have known their actions violated *HIPA*.

[69] There is a finding that SHA had appropriate administrative safeguards for privacy training in place at the time the privacy breach occurred. The root cause of this privacy breach is a Snooper who failed to adhere to these administrative safeguards. There is also a finding to this effect.

d) Prevention of Future Breaches

[70] Proactive prevention is one of the most important steps in the process of reviewing a privacy breach.[24] Measures for the prevention of future breaches can include: adding/enhancing safeguards, providing additional training, and the regular monitoring/auditing of systems and system users with the following considerations being relevant:[25]

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

[71] Prevention is key in assisting a restoration of lost public trust. We specifically address some obvious methods of prevention below.

[72] SHA provided the following regarding the long-term strategies that would be implemented as result of this privacy breach:

- The SHA implemented a series of weekly messaging to all staff reminding them of the importance of accessing personal health information only within the need to know. Regular privacy reminders will be published on a bi-weekly basis starting this fall.

[24] *Supra*, footnote 10 at paragraph [137].

[25] OIPC Investigation Report 290-2024, 007-2025 at paragraph [35]; OIPC Investigation Report 083-2023 at paragraph [35].

- The SHA Privacy Office will push training uptake rates and lists of employees who have yet to complete the training to executive directors on a bi-weekly basis, prompting them to work with their teams to get training rates up.

[73] These are positive steps for SHA towards the prevention of future privacy breaches.

[74] As addressed earlier in this Investigation Report, SHA confirmed that there is no SCM proactive auditing in Moose Jaw at this time. Proactive monitoring and auditing of employee accesses can determine if users are complying with privacy and security policies of the organization, act as a deterrent to unauthorized access and identify snoopers earlier on and potentially those who would ordinarily not be caught.[26]

[75] The *Audit and Monitoring Guidelines for Trustees* provides that auditing practices are necessary to safeguard personal health information. To ensure compliance with *HIPA*, trustees should regularly monitor employee access to the personal health information of its patients:[27]

> **Random Auditing**
>
> Random audits should be used by the trustee to ensure user compliance with provincial and federal legislation, joint services and access policies (JSAP) and with the trustee's internal privacy and security policies. It is the trustee's responsibility to establish a process for conducting random audits of user activity…
>
> Monitoring On the contrary to auditing, monitoring utilizes a less structured process, and involves continuous checks to verify the effectiveness of the process. Monitoring is often done by creating business rules that trigger alerts which identify suspicious patterns of activity or system use, in turn revealing the need for a more focused audit.

[76] SHA did not share any plans to implement proactive monitoring and auditing as a result of this privacy breach at the hospital in Moose Jaw. There will be a recommendation that SHA

[26] *Supra*, footnote 6 at paragraph [57].

[27] *Supra*, footnote 17 at pages 2 and 3.

implement proactive monitoring and auditing of SCM to assist in monitoring employees' compliance with *HIPA* and its privacy and security policies.

4. Section 64 of *HIPA*

[77] With the personal health information of 98 affected individuals inappropriately accessed in this privacy breach, it is necessary to consider the merit of a referral of this matter to the Attorney General of Saskatchewan. It is crucial to ensure justice for the vulnerable citizens of Saskatchewan whose personal health information is subjected unauthorized access. It is also crucial to maintain trust and ensure the inviolability of health services of this province.

[78] In a publication entitled, *Detecting and Deterring Unauthorized Access to Personal Health Information* (January 2015), the former Information and Privacy Commissioner of Ontario, Brian Beamish, advocated for an increase in prosecutions of those who access personal health information without the requisite "need to know" principle. The public naming of those who commit a privacy breach and the referral of the matter to the Attorney General of Saskatchewan for consent to prosecute represents our community's zero tolerance for violations of *HIPA*. We affirm that the unauthorized access and use of personal health information in Saskatchewan is unacceptable.[28]

[79] In Saskatchewan, individuals that are responsible for a violation under *HIPA* could be subject to the offence provisions in section 64 of *HIPA*. In this present case, section 64 of *HIPA* requires 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 willfully 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

[28] *Supra*, footnote 6 at paragraph [77].

> not more than one year or to both, whether or not the trustee has been prosecuted or convicted.
>
> …
> (4) No prosecution shall be commenced pursuant to this section except with the express consent of the Attorney General of Saskatchewan.
>
> (5) No prosecution shall be commenced pursuant to this section after the expiration of two years after the date of the discovery of the alleged offence.

[80] In the *Pledge*, as formally acknowledged by the Snooper twice in early 2025, the following is included:

> 9. I understand my name may be released by the SHA as part of full disclosure in a proven case of a breach of confidentiality.
>
> 10. I understand that failure to comply with this document may result in action being taken against me which may include but is not limited to the following:
>
> a) disciplinary action by the SHA that may result in the suspension or revocation of the team members' appointment and privileges, or the termination of their employment;
> b) a legal action against the team member by the SHA or the patient, client or resident affected by the breach of confidential information;
>
> c) a complaint or report about the team member to their professional licensing body by the SHA, the individual affected by the breach of confidential information or another individual;
>
> d) a report to the Saskatchewan Office of the Information and Privacy Commissioner (OIPC) by the SHA;
>
> e) a complaint to the OIPC by the individual affected by the breach of confidential information; and/or
>
> f) a complaint to the Ministry of Justice by the SHA that may result in a fine of up to $50,000.
>
> [Emphasis added]

[81] For sections 64(1)(a) and (3.2) of *HIPA* to apply, the contravention would have to be proven as being willful and committed with full knowledge. This office defines these terms as follows:[29]

> - A person who acts *knowingly* understands that the social harm will almost certainly be a consequence of the action but acts with other motives and does not care about whether the social harm occurs.
>
> - A voluntary act becomes *willful*, in law, only when it involves conscious wrong or evil purpose on the part of the actor, or at least inexcusable carelessness, whether the act is right or wrong.
>
> [Emphasis added]

[82] Based on the findings as made in the body of this Investigation Report, there is a finding that the Snooper willfully and knowingly violated *HIPA* in this matter.

[83] This office has identified several factors that must be considered when consent is sought from the Attorney General for a prosecution of a matter of this nature. We list those factors here: (1) overall strength of the case; (2) public interest in a prosecution; (3) harm to the community; (4) number of complaints from community; and (5) available litigation resources.[30]

[84] In this case, counsel would have to produce documentary evidence and call SHA witnesses to testify and be subjected to cross-examination. While this office is of the opinion that this case is one where the chances of meeting the threshold of proof is high, there are other issues to consider. We have noted that SHA did not contain the breach as soon as it could have but thankfully, no further inappropriate accesses occurred after May 11th, 2025. Adequate notice was given to the affected individuals identified, including the right to complain to OIPC. To date, this office has not received any formal complaints from the affected individuals. The Snooper's employment was terminated. This was an appropriate

[29] *Supra*, footnote 10 at paragraph [154], which considered these definitions from *Black's Law Dictionary* (12th Ed., 2024).

[30] *Supra*, footnote 6 at paragraph [80].

remedy in this matter. In light of the fact that the Snooper's employment was terminated, the fact that litigation of this nature would be costly to the people of Saskatchewan and the fact that the harm caused was minimal – based on the lack of complaints from the affected individuals - this office concludes that the public interest in a prosecution is low.

[85] We stop short of seeking consent from the Attorney General of Saskatchewan in this matter but we do choose to name the Snooper: Marianne Mann.[31] As a result, there will not be a recommendation that this matter be referred to the office of the Attorney General of Saskatchewan for consent to prosecute pursuant to section 64(4) of HIPA.

III FINDINGS

[86] The three elements are present for *HIPA* to be engaged.

[87] OIPC has jurisdiction to undertake this investigation under the jurisdiction afforded by *HIPA*.

[88] The Snooper did not have lawful authority to access SCM to: (1) view their own personal health information absent the requisite "need to know"; (2) access the personal health information of the 98 affected individuals without the requisite "need to know"; (3) speak to the Witness about their personal health information; and (4) disclose the personal health information of one family member to another family member.

[89] SHA did not adequately contain the privacy breach as soon as it could have.

[90] SHA provided appropriate and timely notice to the affected individuals upon discovery of the privacy breach.

[31] *Stebner v Canadian Broadcasting Corporation*, 2019 SKQB 91 on the inherent right of this office to publish a snooper's name. In that case Danyluk J. of the Saskatchewan Queen's Bench (as it then was) dismissed an application for injunctive relief and further dismissed an application for a publication ban at paragraphs [164] to [167] of that decision.

[91] SHA had insufficient administrative safeguards related to proactive auditing in place at the time of the privacy breach.

[92] SHA took reasonable steps auditing the Snooper's accesses in SCM once the privacy breach was discovered and took reasonable steps to investigate the privacy breach.

[93] SHA had appropriate administrative safeguards for privacy training in place at the time the privacy breach occurred.

[94] The root cause of this privacy breach is that the Snooper failed to adhere to the administrative safeguards that were in place at the material time.

[95] The Snooper willfully and knowingly violated *HIPA* in this matter.

IV RECOMMENDATIONS

[96] I recommend that SHA immediately suspend user accounts when there are grounds to believe that the individual is inappropriately accessing personal health information.

[97] I recommend that SHA implement proactive monitoring and auditing of SCM to assist in monitoring employees' compliance with *HIPA* and its privacy and security policies.

Dated at Regina, in the Province of Saskatchewan, this 23rd day of January, 2026.

Grace Hession David
Saskatchewan Information and Privacy Commissioner