Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 103-2025, 104-2025

Saskatchewan Health Authority and Fahmida Shipa

October 6, 2025

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 the discovery that an employee (Snooper), working at the Battlefords Union Hospital and Don Ross Primary Health Care in North Battleford, had accessed the personal health information of 323 patients without legal authority. OIPC investigated the incident under *The Health Information Protection Act* (*HIPA*) and found the snooper did not have the lawful authority to access/use the personal health information of the affected individual in question. OIPC also found that multiple (323) privacy breaches occurred involving personal health information.

The Commissioner found that SHA did not adequately contain the privacy breaches as soon as it could have but that SHA provided appropriate notice to the affected individuals upon discovery of the privacy breaches and sufficiently investigated them. The Commissioner also found that SHA took appropriate steps to prevent a future breach from occurring.

Finally, the Commissioner found that the Snooper willfully and knowingly violated section 23 (collection, use and disclosure on a need-to-know basis) of *HIPA* in this matter. The Commissioner made recommendations, all arising from the above findings.

The Commissioner did not recommend consent be obtained from the Attorney General of Saskatchewan to prosecute pursuant to section 64 (the offence section) of *HIPA*. The Commissioner discussed several factors that must be considered when recommending a prosecution of a matter of this nature. In this case, while the instances of snooping were egregious and self-admitted, it was concluded that the public interest in a prosecution is low.

I BACKGROUND

[1] On May 8, 2025, the Saskatchewan Health Authority (SHA) proactively reported privacy breaches to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC) under *The Health Information Protection Act* (*HIPA*).[1]

[2] The breaches involved an allegation of snooping by an employee who held multiple roles with the SHA. In essence, the former employee in question worked as a medical office assistant (MOA) at Don Ross Primary Health Care (Primary Care) and as an operating room scheduler (OR Scheduler), at Battlefords Union Hospital (BUH) in North Battleford. In this dual capacity, the individual had access to two electronic medical records (EMR) databases: **MedAccess** for Primary Care and the **OR Manager** system for BUH. What follows is a brief timeline of the employee's work history. The employee held other short-term, casual positions before becoming a full-time employee, but we focus on the following work placements for this Report:

- **August 16, 2023 -** the employee was employed in the Pediatric Therapy Services department as a casual MOA at Primary Care in North Battleford.
- **December 11, 2023 -** the employee began to work in a casual capacity as an MOA with the Food Services department at Primary Care in North Battleford. The employee worked these two positions interchangeably due to a casual status.
- **August 27, 2024** - the employee also worked in a casual capacity as a medical imaging scheduler at BUH in North Battleford.
- **November 18, 2024 -** the employee moved to a full-time medical imaging scheduler at BUH in North Battleford.
- **January 6, 2025** - the employee moved to a full-time position as an OR Scheduler with BUH in North Battleford.[2]

[1] *The Health Information Protection Act*, SS 1990-91, c. H-0.021, as amended.

[2] On January 6, 2025 the employee accepted full time employment as an OR Scheduler and no longer worked as a casual worker therefore their ability to access MedAccess should have been terminated on this date but as we will see, it was not.

- **May 1, 2025 -** the employee voluntarily resigned from all positions with SHA.

[3] SHA provided its breach report to OIPC on August 6, 2025. SHA stated that an employee who worked as an MOA and OR Scheduler in North Battleford had accessed an estimated 323 patient records without legal authority between October 1, 2024, and April 17, 2025. It is relevant at this point to explain that SHA commissioned a total of three audits in relation to this matter. There were two audits of MedAccess. The first audit of MedAccess that first flagged the snooping, was completed on April 7, 2025, and covered the employee's accesses from January 6, 2025, to April 4, 2025. The second audit report reached back further in time and was completed on April 9, 2025 - it covered the employee's accesses from October 1, 2024, to December 31, 2024.

[4] The third audit was an audit of the OR Manager database that was completed on April 28, 2025, and covered the employee's access to that database from January 20, 2025, to April 17, 2025. These three audits revealed that the employee had improperly accessed a total of 323 records during the period of October 1, 2024, to April 17, 2025, with respect to the two EMR databases.

[5] SHA suspended the employee on April 28, 2025, and the employee resigned on May 1, 2025.

[6] On July 7, 2025, OIPC notified SHA that an investigation would be conducted into the privacy breaches. On August 6, 2025, SHA provided this office with its internal *Report of Personal Information/Personal Health Information Privacy Breach* form in lieu of OIPC's *Privacy Breach Investigation Questionnaire* (Questionnaire).[3] On June 9, 2025, SHA also provided this office with the contact information for the former employee responsible for the inappropriate access to the personal health information of 323 individuals.

[7] On July 7, 2025, OIPC notified the former employee in question by letter of its investigation into the privacy breaches. Among other things, the notice informed the

[3] See OIPC *Privacy Breach Investigation Questionnaire*.

individual that this office would be investigating whether there was a willful violation of the legislation. There was also notice that if a willful violation was determined, the matter may be referred to the Attorney General of Saskatchewan for prosecution pursuant to section 64 of *HIPA*. Section 64 of *HIPA* was attached to the notice along with the notification that the individual may be publicly named in the report. The individual was invited to submit a statement but it was made clear that there was no obligation and that legal counsel was welcome to respond. The individual provided a submission on July 29, 2025.

[8] On September 26, 2025, OIPC informed SHA that it would be issuing an Investigation Report on the matter.

II DISCUSSION OF THE ISSUES

1. Does OIPC have jurisdiction?

[9] *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

[10] As noted above, and during the material time, the former employee worked as an MOA at Primary Care and as an OR Scheduler at BUH. In this dual capacity, the individual had access to two EMR databases: MedAccess for Primary Care and the OR Manager system for BUH.

[11] The information accessed by this individual in MedAccess included information such as patient name, date of birth, home address, and details of their medical records. The information accessed by the employee in the OR Manager system included: patient name, date of birth, home address, date of surgery, doctors' comments, nursing notes, and previous surgeries. Altogether, the snooper looked at the personal health information

records of friends, family, co-workers and strangers. 323 individual records were examined, many on a repeated basis.

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

> **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] The first element is present for *HIPA* to be engaged.

ii. Second element – a trustee

[14] SHA qualifies as a trustee pursuant to section 2(1)(t)(ii) of *HIPA*. In an email on September 25, 2025, SHA advised that BUH is owned and operated by SHA, and that Primary Care was an SHA-operated facility located in a city-owned building.

[15] *The Health Information Protection Regulations, 2023* (*HIPA Regulations*) provides the following definition of an employee:[4]

> **2**(1) In these regulations:
>
> …
> **"employee"** means:
>
> (a) an individual:

[4] *The Health Information Protection Regulations, 2023*, H-0.021 Reg 2, as amended.

> (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.

[16] In this matter, SHA advised in an email on September 25, 2025, that the individual in question was an employee of SHA. The individual also had access to personal health information. Therefore, the section 2 definition of "employee" pursuant to *HIPA Regulations* applies to the individual at the time they committed the privacy breaches.

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

[17] "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.[5]

[18] There are two systems at issue in these breaches. MedAccess is "the electronic health records used in Primary Health Clinics" and OR Manager system is "the electronic system used to schedule surgeries and medical procedures."[6] Since all the personal health information was stored on SHA EMR databases (MedAccess and OR Manager system), there will be a finding SHA had custody of the personal health information.[7] Therefore, the third element is also present.

---

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

[6] Definitions of the electronic systems at issue provided in a follow up document from the SHA to OIPC on August 6, 2025.

[7] SHA submitted on August 6, 2025, that "the SHA is the trustee of the personal health information in both systems."

[19] 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 privacy breaches occur?

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

[21] "Use" is defined in 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.

[22] Where personal health information within SHA's systems is accessed by an employee of SHA, the access qualifies as a "use" of personal health information.[8] Therefore, the employee's accesses to patients' records in MedAccess and the OR Manager system were "uses" as defined in section 2(1)(u) of *HIPA*.

[23] The authority to collect, use and disclose personal health information are 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 necessary for the authorized purpose. This rule or principle is commonly referred to as the "need-to-know principle" and it is set out in section 23 of *HIPA* which states, in part:

> **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

[8] See OIPC Investigation Report 193-2024, 043-2025 at paragraph [26].

> 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.
>
> …

[24] Section 26 of *HIPA* is also relevant here because it further restricts use of personal health information by trustees for specific purposes only. 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.

[25] SHA advised that the employee's access of personal health information of patients in these cases were completely unauthorized. In arriving at its conclusion regarding the access, SHA provided this office with the relevant audit reports from MedAccess and OR Manager system that confirmed the unauthorized access on multiple occasions. There were three audits in total as explained in paragraph [3] of this Report and they revealed that the employee's use of the personal health information between October 1, 2024, and April 17, 2025, was not for the purposes of a program, activity or in the service of the trustee. The employee was not providing patient care, and no consent was ever obtained from the snooped parties.

[26] As noted earlier in this Investigation Report, on July 7, 2025, this office provided the employee with notice of this investigation and notice of possible prosecution under section 64 of *HIPA.* The employee was offered an opportunity to file a submission. The employee provided a submission on July 29, 2025, in which they conceded that they had not accessed the EMR databases on a "need to know basis". Rather there were many reasons given for

the snooping – none of which fulfill the statutory mandate for access to personal health information:

- "Sometimes I struggled to understand how to complete certain notes or tasks, so I would refer to past patient entries to get an idea of how similar notes were written…"
- "Constant switching between databases may have contributed to confusion around what systems I was authorized to access…"
- "My sole intention was to help patients and ensure smooth service. At the time I did not realize that accessing MedAccess for this purpose might be considered unauthorized…"
- "I was not given any clear warning or communication indicating that my access in that context was unauthorized…"
- "…out of confusion and eagerness to help, I searched for information to assist them [patients][9]. I was unfamiliar with the boundaries of access during this transition and received no specific instruction that this type of use was inappropriate."
- "To ensure proper communication, I sometimes used MedAccess to find the updated phone number or next of kin information so I could contact the patient and confirm or reschedule their appointment."
- "I want to acknowledge that I accessed a few files out of curiosity, particularly of some colleagues and family members."
- "Coming from a country where patients usually receive copies of their records directly from physicians, I had a different understanding of patient privacy."

[27] As we will see further in this Report, the employee confirmed that they had received privacy training from SHA with respect to the privacy requirements of *HIPA*, but almost inexplicably, the employee repeatedly claimed to not have "fully grasped the depth or seriousness" of the privacy obligations required by the legislation.

[9] This was an amendment for clarity by OIPC in square brackets.

[28] This office has previously provided a definition for "snooping."[10] Based on the information provided to OIPC, the employee's accesses to MedAccess and OR Manager system qualified as 323 acts of snooping. Throughout the remainder of this Investigation Report, the employee will be referred to as the "Snooper".

[29] For the reasons set out above, there will be a finding that the Snooper did not have lawful authority to access/use the personal health information of the affected individuals in question. There will be a finding that multiple (323) privacy breaches occurred involving personal health information.

3. Did SHA respond appropriately to the privacy breaches?

[30] There are several determinants of whether a trustee's response to a privacy breach is appropriate. Section 7-7 of OIPC's *Rules of Procedure* sets out the considerations as follows:

a) Contained the breach (as soon as possible);

b) Notified affected individuals (as soon as possible);

c) Investigated the breach;

d) Taken steps to prevent future breaches.

[31] What follows is an analysis of the response by SHA to the privacy breaches.

a) Containment of the Breach

[32] Upon learning that a privacy breach has occurred, a trustee should immediately take steps to contain the breach. These steps will depend entirely on the nature of the breach, but they may include:

- Stopping the unauthorized practice.

[10] *Supra* footnote 8, at paragraph [35].

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

[33] 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.[11]

[34] The following is a timeline of key events based on information provided by SHA in its internal investigation report, emails with OIPC, and audit logs for each EMR database:

- **August 16, 2023** – first privacy training provided to Snooper. Snooper successfully completed the training and received a certificate of compliance. Snooper swore a *Pledge of Confidentiality* with respect to personal health information. Snooper made no complaint of inability to understand the English language.
- **June 12, 2024** – second privacy training provided to Snooper. Snooper successfully completed the training and received a certificate of compliance. Snooper swore a second *Pledge of Confidentiality* with respect to personal health information. Snooper made no complaint of inability to understand the English language.
- **October 4, 2024** - First inappropriate MedAccess access by the Snooper.
- **January 6, 2025** – According to the Human Resources record, the Snooper left their MOA position and voluntarily moved to the position of OR Scheduler. Unfortunately, on this date, the Snooper's access to MedAccess should have been immediately terminated but it was not until April 4, 2025 when SHA learned of the breaches in MedAccess.
- **January 20, 2025** - First inappropriate OR Manager system access by the Snooper. This first unauthorized use was only four days after having been given access to that EMR database.
- **April 2, 2025** – Last inappropriate access of MedAccess by the Snooper.

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

- **April 4, 2025** – SHA learned of the breaches in MedAccess because of a proactive audit in MedAccess. Access to MedAccess was revoked on this date.

- **April 7, 2025** – SHA Privacy Office was notified of the MedAccess breaches.

- **April 17, 2025** – Last inappropriate access to OR Manager system.

- **April 28, 2025** – An audit of OR Manager system revealed further snooping breaches on the part of the employee. On this date, the Snooper was suspended from employment with SHA and access to OR Manager system was terminated.

- **May 1, 2025** – the Snooper voluntarily resigned from their employment with the SHA.

[35] In an email on August 29, 2025, SHA clarified that the timeline of the first MedAccess audit report was from January 6, 2025 to April 4, 2025. The audit was triggered by the Snooper viewing the records of patients who had the same last name. During an audit there are many events that should trigger a formal investigation. This office, in conjunction with eHealth Saskatchewan, has produced a helpful manual that lists such events and we list them here:[12]

- A user has viewed their own record;

- The type of access is not related to the role of the user who made the access (e.g., a pharmacist views information outside their scope of practice);

- A user views a record of an individual who has the same last name as the user;

- The viewed record belongs to an employee of the organization;

- The number of accesses to one particular record is quite high;

- A record has been viewed 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);

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

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

[36] When a user, as in the case of this Snooper, "breaks the glass" or overrides a mask on a patient's record, the "need to know" basis is required for the invasion of privacy. This can include a valid medical reason for treatment or consent. In this matter, the Snooper entered reasons that did not qualify under the need-to-know requirement such as: "need to check appointment" or "need to check task." If the Snooper needed to check an appointment or check a task, the patient should have been called or a colleague consulted for the information.

[37] Based on the above timeline of events, the Snooper left their MOA job on January 6, 2025, but access to MedAccess was not revoked until April 4, 2025 when SHA became aware of the breaches. Unfortunately, SHA did not audit the Snooper's access to OR Manager system until April 28, 2025. On that day the Snooper's access to OR Manager system was revoked, and the Snooper was placed on suspension pending an investigation. The Snooper then voluntarily resigned from SHA on May 1, 2025.

[38] This office has previously recommended that:[13]

> …when the SHA has grounds to <u>believe an individual is inappropriately accessing personal health information, that the SHA should immediately suspend the individual's access</u> to the [electronic medical record]…
>
> [Emphasis added]

[13] See OIPC Investigation Report 203-2019, 214-2019, 257-2019 at paragraph [65].

[39] According to the SHA audit, the last inappropriate access by the Snooper in MedAccess was on April 2, 2025. Simultaneously between January 20, 2025, and April 17, 2025, the Snooper was actively snooping on OR Manager system until the access to that EMR database was revoked on April 28, 2025.

[40] In a previous OIPC investigation report, a physician accessed personal health information of some of the Humboldt Broncos hockey team members from the clinic's EMR database.[14] The physician then accessed personal health information on the electronic health record viewer. The finding was that this physician should not have accessed the personal health information in either system because their reasons for snooping did not meet the requisite "need-to-know" for treatment pre-condition pursuant to section 23 of *HIPA*. The fact that the physician had a virtuous motive is of no moment, the privilege of patient health information can only be accessed on the "need to know" for treatment basis.

[41] In the present case, SHA failed to revoke the Snooper's access to MedAccess when the Snooper resigned from that position and moved to a new job on January 6, 2025. Access to MedAccess was allowed until April 4, 2025, after discovery of the snooping. SHA only revoked the Snooper's access to OR Manager system on April 28, 2025, even though it had learned of the employee snooping in MedAccess on April 4, 2025. Therefore, there will be a finding that SHA did not adequately contain the privacy breaches as soon as it could have.

b) Notification of Affected Individuals

[42] OIPC has developed *Privacy Breach Guidelines for Trustees*, and it provides that trustees should notify affected individuals as soon as possible when there is a privacy breach. 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[15]:

[14] See OIPC Investigation Report 161-2018 at paragraphs [56] and [57].
[15] See OIPC resource *Privacy Breach Guidelines for Trustees* at pages 3 and 4.

- 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.
- 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

[43] On May 16, 2025, SHA notified all 323 affected individuals of these privacy breaches by letter. This was a reasonable period of time for an investigation and communication. As of the date of this Report, no complainants have come forward.

[44] The SHA letter was admirable in that it referenced the most vital elements listed above, including instructions on accessing the audit reports. The audit reports contain vast detail with respect to the privacy breaches. OIPC applauds SHA for its transparency to the affected individuals. There will be a finding that SHA has provided appropriate and timely notice to the affected individuals upon discovery of the privacy breaches.

c) Investigation of the Breach

[45] The recommended steps in investigating an allegation of snooping include:[16]

- Record the details of how the breach came to light.

[16] *Supra*, footnote 8 at paragraph [76].

- Suspend the employee's access to the personal health information.
- Retrieve the information log, 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 and record the privacy training the employee in question has received (have warnings of routine audits been given?).
- Review any relevant employment contracts.
- Consider who needs to be notified (e.g., supervisor, union, police, eHealth Saskatchewan, etc.).
- Decide if the identity of the employee in question will be disclosed to the affected individual when providing notification.
- Proactively report to OIPC.

[46] Based on a review of the materials and information provided by SHA the following steps were pursued:

- SHA retrieved and reviewed audit reports from MedAccess which captured the Snooper's accesses to patient records, the identity of the patients, the nature of the information viewed, the date of the accesses and the computer used to access MedAccess.
- SHA immediately revoked the Snooper's access to MedAccess once it became aware of the breaches.
- An audit of OR Manager system found further breaches by the Snooper on April 28, 2025. This led to an immediate interview of the employee and an immediate suspension on the very same day.
- SHA identified snooping, curiosity, and access to database privileges not deactivated in a timely manner as the root causes of the breaches.

[47] This office has previously recommended that users of personal health information databases should be required to complete privacy and security training and sign a

confidentiality pledge or undertaking as a condition of gaining access to systems which contain personal health information.[17] Since August of 2023, *HIPA Regulations* includes specific requirements regarding training and pledges of confidentiality in section 5. Section 5 of *HIPA Regulations* states:

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

[48] Previous investigation reports from OIPC have been clear that privacy training and confidentiality pledges should be refreshed annually.[18]

[49] The Snooper received excellent privacy training on August 16, 2023, and then again on June 12, 2024. The 2024 training provided to the Snooper (*Privacy Training 2024: Privacy and the Need-to-Know*) outlined the following:

- It described access to information and privacy legislation in Saskatchewan, specifically *The Local Authority Freedom of Information and Protection of Privacy Act* (*LA FOIP*)[19] and *HIPA*.

[17] *Supra* footnote 8 at paragraph [83].
[18] See OIPC Investigation Report 413-2019, et al at paragraph [38] and Investigation Report 164-2023, et al at paragraph [76].

[19] *The Local Authority Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. L-27.1, as amended.

- It emphasized the "need-to-know" principle, including a direct emphasis on the rejection by SHA of the "Circle of Care" model and inclusion of its "Need to Know versus Circle of Care" directive.[20]

- It *specifically* commented on snooping, gossiping, and the public discussion of personal health information, stating that the names of snoopers may be released to affected individuals.

- It imparted warnings about audits and the digital traces evident in SHA electronic systems.

- It discussed privacy breaches in the form of unauthorized collections and uses, notably drawing upon a wide array of examples of privacy breaches relevant to a health-care environment.

- It addressed how to respond to privacy breaches, with a focus on containment, notification, and prevention.

- It highlighted high-profile cases wherein snoopers working in health care environments have been named and prosecuted.

[50] In a submission to OIPC, the Snooper acknowledged the completion of these two online privacy training courses and yet, almost unbelievably, the Snooper submitted at the time of the breaches they "did not fully grasp the depth or seriousness of the privacy obligations."[21] This contention is difficult to comprehend considering that the Snooper's submission to this office was crafted in perfect English. Further, the training that was given to the Snooper comprehensively covered the prohibition against snooping and the possible ramifications which could occur – such as the release of the snooper's name to the affected individuals and possible prosecution.

[51] This office has noted that the training provided by SHA leaves snoopers in a difficult position to allege they did not understand the full significance of the invasion of privacy

[20] See SHA resource *Privacy Guidance Document: Need-to-Know vs Circle of Care*.
[21] Snooper's submission to OIPC provided on July 29, 2025, page 3.

related to snooping in records containing personal information and/or personal health information.[22]

[52] SHA requires all employees to sign the *Pledge of Confidentiality* on an annual basis.[23] The *Pledge of Confidentiality* explicitly states that viewing, use, or disclosure is only with a "legitimate need-to-know," employees will not access their own personal health information or the information of "family, friends, acquaintances, co-workers, etc. without a professional need-to-know."

[53] The *Pledge of Confidentiality* was signed by this snooper at the completion of the training modules on August 16, 2023, and June 12, 2024.

[54] The *Pledge of Confidentiality* makes no secret of the actions that could be taken on a failure to comply:

> 10. I understand that a 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.

[22] See OIPC Investigation Report 266-2024, 031-2025 at paragraph [98]; See also *Supra*, footnote 8 at paragraph [153].

[23] *Ibid*, at paragraph [78].

[55] It is abundantly clear that this Snooper should have known their actions contradicted the training they had received and, in turn, violated *HIPA*. There will be a finding that SHA sufficiently investigated the privacy breaches.

d) Prevention of Future Breaches

[56] This office has previously stated that prevention is one of the most important steps in this entire process of breach review.[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?

Proactive Audit Policy

[57] Previous OIPC investigation reports have addressed auditing as a technical safeguard.[26] There are benefits to conducting regular monitoring and auditing of EMR databases to determine if users are complying with privacy and security policies of the organization and it can act as a deterrent to unauthorized access. Further, completing regular proactive audits can identify snoopers earlier on and potentially those who would ordinarily not be caught.

[24] *Supra*, footnote 8 at paragraph [137].

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

[26] For example, see OIPC Investigation Report 176-2015 at paragraph [34].

SHA caught the breaches in this matter as a result of proactive auditing. This is a very positive step taken by SHA.

[58] The proactive audit completed in this case appears to have caught the Snooper's unauthorized accesses in MedAccess and SHA was triggered to investigate the Snooper's accesses in OR Manager system.

[59] This office has previously requested SHA provide a copy of its completed proactive audit policy.[27] As of August 29, 2025, SHA indicated it was still working on the policy. On September 12, 2025, SHA advised that there is a three to six month timeline for completion. A recommendation will follow that SHA provide this office with a copy of the proactive audit policy within 90 days of completion of this policy.

Access Controls

[60] OIPC has previously stated that "access controls are important to manage and limit access to personal health information to mitigate privacy and security risks and ensure compliance with policy and *HIPA*."[28]

[61] SHA conceded that the Snooper's user accounts were not revoked as soon as the Snooper left the first position and assumed the second position.

[62] SHA outlined that "account deactivation" as a key element of access management. OIPC is content that SHA is aware of the risks of delayed access deactivation as seen in these privacy breaches.

[63] Currently, there is an *Access Management Policy* being developed by SHA which is a positive step to determine when employees' accesses are to be revoked or disabled. The *Access Management Policy* is estimated to be completed within three to six months.

[27] *Supra*, footnote 22 at paragraph [82].

[28] *Supra*, footnote 8 at paragraph [103].

[64] There is a recommendation for SHA to finalize the *Access Management Policy* as soon as possible, and to immediately deactivate all user accounts for an individual when they terminate/resign or on an extended leave from a position. Further, there is a recommendation for SHA to immediately suspend user accounts when there are grounds to believe that the individual is inappropriately accessing personal health information.

Long Term Prevention Strategies

[65] In regard to long-term strategies to mitigate and prevent future occurrences of snooping breaches, SHA asserted that it held a two-day event in July of 2025, to discuss access management. Further, it also held a privacy "town hall" for all SHA staff to voluntarily attend on June 27, 2025 "highlighting the 'need-to-know' concept and walked through three recent breaches." These events both highlight the commitment of SHA to prevent future breaches and are nothing short of admirable.

[66] As mentioned in the previous section, confidentiality and privacy training is required by all employees on an annual basis. SHA has also developed "*privacy guidance documents*" available to employees and the public which clearly outline the "need-to-know" concept, when disclosing personal health information, among other topics.

[67] In both its internal report and Quality Improvement (QI) training slides, SHA asserted that one of the root causes of the breaches was that the access to MedAccess was not revoked when the Snooper left the first MOA position and moved on within the employment of SHA. In an email from SHA to OIPC on September 4, 2025, SHA asserted the following:

> There is not a written process for deactivation other than the Med Access Account Request form, however, the manager was aware of the requirement to remove the employee's access, however due to miscommunication between the Manager of Nutrition Services and [the Snooper] the access was not removed.
>
> [Emphasis added]

[68] On September 12, 2025, SHA provided the following in regard to the miscommunication between the manager and the Snooper:

> The manager retained the employees access to MedAccess during her 3-month trial period of her full-time position as OR Scheduler. However, the access should have been removed when she left her primary health care position.

Evidence of Willful Knowledge – Mask Overrides

[69] In addition to the outright and inappropriate accesses of patient health records, the Snooper also completed "mask overrides" and set the override, in some cases, for up to 180 days to a patient's health record which lends a special, willful element to the snooping in this case. Certain EMR databases allow for users to "mask" their personal health information which eHealth Saskatchewan describes as "a control mechanism that allows individuals the opportunity to hide, or 'mask,' their personal health information...".[29] eHealth can only mask profiles in the eHR Viewer and Pharmaceutical Information Program (PIP); however, each EMR database used within physician offices or SHA may have the capabilities to have profiles masked.

[70] Depending on the type of mask selected, (selective, global, or full block), an employee may be able to override the mask, or "break the glass" on a patient's record. When a record is unmasked, the EMR database requires a reason. The Saskatchewan EMR Program outlines that when a patient's profile has been unmasked, "the users should select the minimum time necessary to fulfill the identified purpose for the unmasking." [30]

[71] The audit logs and the Snooper's submission in this case provide insight into the snooper's state of mind by the use of the mask override time frame. In the first MedAccess audit the employee selected a varied number of days for different patients. Some patients were overridden for one day, some for 180 days when it came to coworkers and family members. The Snooper fully understood the nature of her improper actions.

[29] See eHealth Saskatchewan guidance on *Restricting Access to Your Information.*
[30] See The Saskatchewan EMR Program resource Privacy and Security Resource Materials for Saskatchewan EMR Physicians: Guidelines, Samples and Templates at pages 67 to 69.

[72] In regard to organizational guidance on the appropriate timeline for unmasking a patient profile, SHA asserted the following in an email from September 2, 2025:

> The SHA does not have a procedure or policy which outlines when each time frame for the override should be selected. The individual facility/site/department/clinic would have their own policy or procedure for them. This area does not have one, but Privacy will work with Primary Health Care on a break the glass procedure which outlines when each time frame for the override should be selected.
>
> [Emphasis added]

[73] As of the issuance of this Investigation Report, no timeline or further details have been shared by SHA on the development of a policy or procedure on when employees should break the glass and for how long; however, SHA did commit to working with the primary health care team to develop a procedure.

[74] As a result of the above, there will be a finding that SHA has taken appropriate steps to prevent future breaches from occurring.

4. Should prosecution of the Snooper be recommended under section 64 of *HIPA*?

[75] At this time, it must be considered if the privacy breaches at issue warrant consideration that the Snooper be prosecuted for a violation pursuant to section 64 of *HIPA*.

[76] With the personal health information of 323 patients involved in these privacy breaches, it is necessary to consider the merit of a costly prosecution in this case: we feel it is crucial to ensure justice for the vulnerable citizens of Saskatchewan who are subjected to the unauthorized accesses to their personal health information, and to maintain trust and ensure the inviolability of health services of this province.

[77] In a publication entitled, *Detecting and Deterring Unauthorized Access to Personal Health Information* (January 2015)[31], the former Information and Privacy Commissioner of Ontario, Brian Beamish, advocated for an increase in the number of prosecutions of those who snoop. The former Commissioner 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.
>
> [Emphasis added]

[78] In Saskatchewan, snoopers of personal health information could be subject to the offence provisions in section 64 of *HIPA*. In the 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 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.

[31] See Ontario IPC's resource *Detecting and Deterring Unauthorized Access to Personal Health Information* at page 9.

[79] Based on the training provided by SHA to the Snooper, and as acknowledged by the Snooper in their submission to this office, there will be a finding that the Snooper willfully and knowingly violated section 23 of *HIPA* in this matter.

[80] There are several factors that must be considered when recommending a prosecution of a matter of this nature. We list those factors here: (1) overall strength of the case; (2) public interest; (3) harm to community; (4) number of complaints from community; and (5) litigation resources.

[81] In this case, counsel would have to produce documentary evidence and call witnesses to testify to this matter, all witnesses from SHA. 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 acted swiftly and carefully once the evidence of snooping was discovered but it failed to contain the privacy breach at the earliest opportunity. Adequate notice was given to the affected individuals, including the right to complain to this office. There were no complaints. In light of the actions of SHA, the fact that litigation of this nature would be costly to the people of Saskatchewan and the fact that the harm caused was minimal – from the lack of public complaints - this office concludes that the public interest in a prosecution is low.

[82] We stop short of seeking consent of the Attorney General of Saskatchewan in this matter but we do choose to name the Snooper: Fahmida Shipa.[32] 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

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

[32] See *Stebner v Canadian Broadcasting Corporation, 2019 SKQB 91* on the inherent right of this office to publish a snooper's name and the eventual dismissal of an application for injunctive relief and dismissal of an application for a publication ban at paragraphs [164] to [167].

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

[85] The Snooper did not have the lawful authority to access/use personal health information of the affected individuals in question.

[86] Multiple (323) privacy breaches occurred involving personal health information.

[87] SHA did not adequately contain the privacy breaches as soon as it could have.

[88] SHA has provided appropriate and timely notice to the affected individuals upon discovery of the privacy breaches.

[89] SHA sufficiently investigated the privacy breaches.

[90] SHA has taken appropriate steps to prevent future breaches from occurring.

[91] The Snooper willfully and knowingly violated section 23 of *HIPA*.

IV RECOMMENDATIONS

Prevention of Future Breaches

[92] I recommend that SHA provide OIPC with a copy of its proactive audit policy within 90 days of completion of this policy.

[93] I recommend that SHA finalize the *Access Management Policy* as soon as possible, and to immediately deactivate all user accounts for an individual when they terminate/resign from a position.

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

Dated at Regina, in the Province of Saskatchewan, this 6th day of October, 2025.

Grace Hession David
Saskatchewan Information and Privacy Commissioner