Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 193-2024, 043-2025

Saskatchewan Health Authority

April 23, 2025

Summary: The Saskatchewan Health Authority (SHA) proactively reported a privacy breach to the Commissioner's office after it discovered that a registered nurse (Snooper), working at the Jim Pattison Children's Hospital in Saskatoon, had accessed the personal health information of 314 patients without legal authority. The A/Commissioner investigated the incident under *The Health Information Protection Act* (HIPA). He found that there were privacy breaches involving personal health information. He also found that the SHA did not have adequate safeguards in place at the time of the breach to protect the personal health information. In terms of the breach response, the A/Commissioner found that SHA took appropriate action to contain the breach. However, the SHA's notification to affected parties was not adequate and timely. In addition, he found that the investigation and the proposed steps to prevent further breaches of this nature are not adequate. The A/Commissioner recommended that the SHA, within 30 days of the issuance of this Investigation Report, take any necessary steps to ensure that privacy training and signing of a pledge of confidentiality is completed annually; notify its staff of the name of the Snooper and of the disciplinary actions taken in relation to the privacy breaches at issue here; review and revise policies and procedures regarding notification to affected parties and his office; contact the affected parties whose health services card numbers were involved to advise them how to apply for a new card; finalize audit policies that applied to some systems and develop plans for the creation of other audit policies; amend existing work standards on removing access rights and develop a plan to create other work standards or polices regarding access rights; and develop a plan to add pop-up or warning flags for all electronic health systems. He also recommended that the SHA forward their investigation files to the Ministry of Justice and Attorney General, to allow prosecutors to consider whether an offence has occurred and if charges should be laid under HIPA or any other statute.

I BACKGROUND

[1] This Investigation Report considers privacy breaches that were proactively reported to my office under *The Health Information Protection Act* (HIPA) by the Saskatchewan Health Authority (SHA) on August 16, 2024. The breaches involved allegations of snooping by a registered nurse (RN).

[2] In its breach report, SHA stated that the RN, who was employed in the maternity department of the Jim Pattison Children's Hospital (JPCH) in Saskatoon, had accessed patient records without legal authority and for a purpose unrelated to patient care – a practice commonly referred to as snooping.

[3] In this Investigation Report, I find that the RN engaged in multiple incidents of snooping into patient records without legal authority. These breaches, and the snooping breaches involving the SHA that were investigated in Investigation Report 266-2024, 031-2025 are concerning.

[4] Snooping has been a problem in this province and elsewhere in Canada for some time. In one of my first blogs, Snooping: When Will People Learn?, written almost ten years ago, I addressed the problem of snooping on personal information and personal health information. I expressed the hope that in the future Saskatchewan's public bodies and health care institutions would experience a shift in culture towards a greater respect for privacy rights.

[5] While it appears that progress has been made in Saskatchewan towards building privacy protective cultures, systems and practices over the last 10 years, I continue to be concerned about the incidents of snooping. If people cannot trust their health care providers to protect their privacy, they may withhold or falsify information about their health. This, in turn, poses a substantial risk to the quality of the health care they may receive. I cannot overstate how important it is for Saskatchewan's trustees to make every reasonable effort to ensure that those who are tempted to snoop are not successful and that personal health information

is protected. As I said in Investigation Report 308-2017, 309-2017, 310-2017, issued on June 4, 2018, upholding trust is key to upholding the integrity of the health care system.

[6] In response to the breaches at issue here, the SHA made efforts to contain the breaches, conduct an investigation and notify affected parties. It terminated the RN's position and proposed some changes to the work standards applicable to one of the systems used by the RN in JPCH's maternity department.

[7] I commend the SHA for taking these actions. However, in this Investigation Report, I conclude that it did not have adequate measures in place to protect the privacy of personal health information at the time of the breaches and that it should have taken further steps in responding to the breaches. I also find that its efforts to prevent future breaches of this kind are not adequate. My analysis, findings and recommendations are set out later in this Investigation Report.

[8] I now turn to the circumstances surrounding the breaches and SHA's investigation. Prior to the breaches, the RN worked one day a week from home using an SHA issued laptop. According to the SHA's proactive breach report, the privacy breaches occurred between August 23, 2021 and December 14, 2021, when the RN used the SHA issued laptop computer to remotely access personal health information of individuals without a need to know the information. During this period, the RN was on leave of absence and was not supposed to be working and accessing any SHA information. SHA's investigation concluded that the RN accessed personal health information without legal authority.

[9] SHA initially reported that the breach affected 313 individuals. The information accessed was stored on JPCH's electronic record system for maternal services called IntelliSpace Perinatal (ISP) and the SHA's Sunrise Clinical Manager (SCM) system.

[10] On the ISP system, the SHA initially stated that the RN accessed patients' obstetrical history, prenatal details and assessments and care information. Regarding the SCM system, the SHA initially stated that the RN accessed patients' information such as assessments,

care, procedures and lab results related to treatment provided at the Intensive Care Unit (ICU) of the Royal University Hospital (RUH) in Saskatoon.

[11] The SHA subsequently advised my office that the unauthorized accesses involved 2,437 records and 314 patients. Some of the records accessed included sensitive personal health information. In relation to some patients, the information accessed also included sensitive demographic information such as the patient's name, contact details, date of birth, hospital medical record number and health services card number. According to the SHA, six of the patients were co-workers and two of them had confidentiality flags on their files requiring the user to "break the glass" or override the warning flag or screen to gain access. I will be discussing this in more detail later in this Investigation Report.

[12] On September 6, 2024, my office notified the SHA that the A/Commissioner would be conducting an investigation into the privacy breaches. On October 9, 2024, the SHA provided my office with its completed *Privacy Breach Investigation Questionnaire* (Questionnaire).

[13] On February 27, 2025, the SHA provided my office with the name and contact details for the RN. The same day, my office sent a registered letter to the RN notifying them that the A/Commissioner is conducting an investigation into SHA's allegations of snooping. Investigation File 043-2025 was opened to process that investigation. My office invited the RN to provide a submission on the matter by March 7, 2024. My office also advised the RN that if they required more time to complete their submission, they should contact my office immediately to discuss possibly extending the response deadline.

[14] According to the Canada Post tracking receipt, the RN received the registered letter on March 3, 2025, and signed for delivery. However, the RN did not contact my office and did not provide my office with a submission.

[15] During the investigation, the SHA provided information and responses to questions posed by my office on January 20, 2025, February 26, 2025, February 27, 2025, April 4 and 10, 2025.

[16] I have decided to issue one investigation report dealing with Investigation File 193-2024 and Investigation File 043-2025.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[17] HIPA applies when three elements are present: (1) personal health information, (2) a trustee, and (3) the personal health information is in the custody or control of the trustee.

[18] The information accessed by the RN included information related to maternal and infant health care history, services, tests and medications. In some cases, the patients' addresses, telephone numbers, birthdates, gender and health services numbers were involved.

[19] I find that this qualifies as personal health information, as set out at subsections 2(1)(m)(i), (ii) and (v) of HIPA which states as follows:

> **2**(1) In this Act:
>
> ...
> (m) "personal health information" means, with respect to an individual, whether living or deceased:
>
> (i) information with respect to the physical or mental health of the individual;
>
> (ii) information with respect to any health service provided to the individual;
>
> …
> (v) registration information;

[20] Further, the SHA qualifies as a trustee pursuant to subsection 2(1)(t)(ii) of HIPA. As noted in Investigation Report 164-2023 et al, the SHA manages the JPCH and RUH.

[21] Finally, I must determine if the SHA had custody or control over the personal health information at issue. "Custody" is physical possession with a measure of control.

[22] Since all the personal health information was stored on systems managed by the SHA, I find that it had custody of the personal health information. Therefore, the third element is also present.

[23] As all three elements are present, I find that HIPA applies, and I have jurisdiction to investigate these matters.

2. Did a privacy breach occur?

[24] A privacy breach occurs when a trustee collects, uses, or discloses personal health information in a way that is not authorized by HIPA.

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

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

[26] Where personal health information is accessed by an employee or a contractor of the SHA, the access qualifies as a "use" of personal health information (see Investigation Report 065-2021, 068-2021, 069-2021, 073-2021). Therefore, the RN's accesses to patients' records in the ISP and in the SCM system were "uses" as defined in subsection 2(1)(u) of HIPA.

[27] 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 required by the employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.
>
> …
> (4) A trustee must, where practicable, use or disclose only de-identified personal health information if it will serve the purpose.

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

> **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.

[29] The SHA alleged that the RN accessed personal health information and did not have the legal authority to do so because at the time of the accesses they were on a leave of absence from work. During the leave of absence, the RN was not supposed to be working.

[30] In arriving at its conclusion regarding the accesses, it referred to audit reports of the ISP and SCM systems and logs that revealed the RN's accesses. It also relied on the information it gathered during its interview with the RN.

[31] During those interviews, the RN did not deny that the accesses had occurred. However, they could not explain why they looked at the patient records. They were asked specifically

about the records relating to six employees and did not have any explanation for those accesses either. When asked if they had approval from their manager to access the SHA network and systems while on leave of absence, the RN is reported to have said "No." According to the SHA, the RN eventually admitted that they did not need to access the patient records and apologized for having done so.

[32] During the SHA investigation, the RN stated that they did not access any other systems, and there were not any "emails/texts/messages/documents relating to these accesses." The RN also denied discussing the information with anyone.

[33] As noted earlier in this Investigation Report, my office provided the RN with notice of this investigation and an opportunity to make a submission. The RN did not file a submission.

[34] Based on the information provided to my office by the SHA, the RN's use of the personal health information was not for the purposes of a program, activity or service of the trustee because they were on leave and not providing patient care at the time, nor was the use made with the consent of the patients involved. Moreover, it is apparent from the information provided by the SHA that the RN did not have a need-to-know this information as required by section 23 of HIPA.

[35] My office defines "snooping" as the "unauthorized access of personal information or personal health information by employees without a need-to-know" (*Guide to LA FOIP*, Chapter 6, "Protection of Privacy" [*Guide to LA FOIP*, Ch. 6], p. 334). Based on the information provided by the SHA, the RN's accesses to the ISP and SCM systems qualified as "snooping." Throughout the remainder of this Investigation Report, I will refer to the RN as the "Snooper."

[36] For the reasons set out above, I find that the Snooper did not have the lawful authority to use personal health information of the affected individuals. I find that multiple breaches of privacy occurred.

3. Did the SHA respond appropriately to the privacy breach?

[37] As I have found that privacy breaches occurred, I will now consider if the SHA appropriately handled the breaches.

[38] As described in section 5-4 of my office's *Rules of Procedure* and my office's *Privacy Breach Guidelines for Trustees*, at pages 3 to 6, my analysis of SHA's responses to the privacy breach looks at its efforts to:

1. Contain the breach (as soon as possible);
2. Notify affected individuals (as soon as possible);
3. Investigate the breach; and
4. Prevent future breaches.

[39] I turn to consider if SHA appropriately addressed each of these steps.

Contain the breach (as soon as possible)

[40] My office's *Privacy Breach Guidelines for Trustees* at page 3, states that upon learning that a privacy breach has occurred, government institutions and trustees should immediately take steps to contain the breach. Depending on the nature of the breach, this may include:

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

[41] In my office's Investigation Report 197-2022, 215-2022, I stated that in assessing efforts to contain the breach, my office applies a reasonableness standard. We want to have some

reassurance that the institution or trustee has reduced the magnitude of the breach and the risk to affected individuals.

[42] The following timeline of key events is based on information provided by the SHA:

- August 24, 2021 – the Snooper took a leave of absence from work. It was initially for a short period of time. After multiple extensions, the leave of absence totaled approximately 16 months.
- Between August 23, 2021 and December 14, 2021 – the Snooper accessed 314 patient records. The Snooper was on leave during this entire period.
- December 14, 2021 – SHA discovered what it believed were unauthorized accesses by the Snooper while reviewing an audit report related to another employee.
- December 14, 2021 – SHA disabled the user account for the Snooper which took away access rights to all SHA systems and deactivated SHA IT assets. It also made "arrangements to have the laptop returned" although it is unclear when that occurred.
- January 3, 2022 – a manager from the maternity department reported the breach to SHA's privacy office.
- October 18, 2022 – SHA's privacy team began its investigation by running a full audit report on the ISP and SCM systems.
- January 2024 – the Snooper returned to work.
- January 16 and February 5, 2024 – hospital staff and the privacy officer met with the Snooper.
- March 7, 2024 – the SHA terminated the Snooper's employment.

[43] The SHA stated that during the interviews with the Snooper it asked why they accessed the patient records. The Snooper suggested that they required the access to facilitate "hand offs" of those files to other staff. However, the Snooper later admitted that they "did not need to go back into the charts." SHA concluded that the Snooper's explanation was not credible, and that the Snooper did not need to know the information that was accessed. As noted above, six of the patients involved were employees of JPCH for whom the Snooper was not providing care.

[44] The SHA also asked if they had copied, printed or shared the information with other parties at any time. The Snooper stated that they did not do so. On this subject, the SHA confirmed to my office that the Snooper did not have the ability to print records using the SHA issued laptop.

[45] Regarding the 13-month delay in conducting the interviews, the SHA stated that it could not interview the Snooper until they were cleared to return to the workplace due to employment related restrictions. It was not able to point to a specific provision in the collective agreement or elsewhere that set out these restrictions. It added that the interview was a necessary part of its investigation as it was required to make a determination on whether the Snooper had the authority to access the personal health information before it could conclude that the privacy breaches had occurred.

[46] As I said above, in assessing efforts to contain the breach, my office applies a reasonableness standard. By immediately disabling the Snooper's access to SCM and ISP and retrieving the laptop upon discovering the breaches, I find that the SHA took reasonable steps to contain the breaches.

Notify affected individuals (as soon as possible)

[47] Section 28.1 of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) requires local authorities to notify individuals when their personal information has been breached, and a real risk of significant harm exists for the affected individuals.

[48] Section 28.1 of LA FOIP states:

> **28.1** A local authority shall take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the local authority if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

[49] Even where section 28.1 of LA FOIP does not apply, unless there is compelling reason not to, a local authority should always notify affected individuals of a privacy breach. Trustees should follow the same practice.

[50] It is important to notify affected individuals for several reasons. Affected individuals have a right and need to know to protect themselves from any harm that may result. This is particularly important where sensitive information such as social insurance numbers are involved.

[51] My office's *Privacy Breach Guidelines for Trustees* at page 4, which is based on findings and recommendations made in previous investigation reports of this office and best practices, sets out the information that should be included in every notice to affected individual(s). The notice should include:

- A description of the breach (a general description of what happened).
- A detailed description of the personal information involved (e.g., name, credit card numbers, medical records, financial information, etc.).
- A description of possible types of harm that may come to the affected individual because of the privacy breach.
- Steps taken and planned to mitigate the harm and prevent future breaches.
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g., how to contact credit reporting agencies).
- 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 my office (provide contact information).
- Recognition of the impacts of the breach on affected individuals and, an apology.

[52] On August 16, 2024, the breach was reported to my office. The SHA notified the 314 affected parties on August 19, 2024. This was approximately five and one-half months after the investigation was concluded and over two years after the breach was discovered.

[53] SHA also notified the Snooper's professional regulatory college, namely the College of Registered Nurses of Saskatchewan (College), of the breach. On a review of the College's website, it appears that the Snooper's license to work in the province is still in effect.

[54] Three types or templates of notices to affected parties were sent. One notice was sent to parents whose infant's information was accessed. Another notice was sent to patients being treated in the ICU of the RUH and the third notice was sent to mothers receiving care in the JPCH maternity ward.

[55] Each of the notices included some information about the personal health information accessed, the cause of the breach in general terms, a statement about SHA's inability to comment on personnel matters, and that it has taken appropriate steps to ensure compliance with SHA and privacy requirements. The notices also included an apology and information about how to file a complaint with my office and with the SHA.

[56] In its *Questionnaire*, the SHA stated that there was a "low risk" to individuals because they were not "targeted specifically" by the Snooper. It is not clear how the SHA arrived at that assessment.

[57] In the discussion that follows, I will address the SHA's failure to identify the Snooper in the notification to affected parties, the delay in notifying affected parties and my office, the lack of detailed information about the personal health information involved and SHA's failure to notify the affected parties that their health services card number was involved.

[58] In my office's *Privacy Breach Guidelines for Trustees* at page 7, my office recommends that a trustee share any discipline measures taken against an employee who has snooped with other employees in the organization and the affected individuals. I also recommend in cases such as these that the name of the snooper and the actions taken to discipline the snooper be provided to affected parties. This is because affected individuals are in the best position to understand and assess the impacts of a privacy breach upon themselves. Knowing who the snooper is will help evaluate those risks. Disclosure of the discipline would help to ensure that Saskatchewan residents trust that the SHA is protecting their personal health information appropriately (see Investigation Report 266-2024, 031-2025).

[59] This approach is consistent with the approach taken by other privacy oversight authorities in Canada (see for example the Ontario Information and Privacy Commissioner's (ON IPC) Order HO-010 and the Information and Privacy Commissioner of Prince Edward Island's Breach Report HI-18-005).

[60] As noted above, the notice to the affected parties and to my office was sent approximately five and one-half months after the SHA concluded its interview process and determined that the Snooper was responsible for the privacy breaches. This was more than two years after the date of discovery of the accesses via the audit report.

[61] While it is concerning that more than two years had passed following the date of the discovering of the accesses, I acknowledge that the SHA may have been required to interview the Snooper before it could conclude that a privacy breach had occurred. I have said in the past that an important step in a breach investigation is the meeting with the individuals suspected of snooping in order to establish what had occurred (see for example Investigation Report 162-2023).

[62] The circumstances of the Snooper's leave were such that holding that meeting was not possible until they had returned to work. However, at a minimum, the notice to affected parties should have been sent as soon as SHA was satisfied that a breach had occurred – that is, after the interview concluded.

[63] The SHA may have felt constrained by its employment relationship with the Snooper. However, it should have considered notifying my office of the breach within ten calendar days of initiating containment. It is not necessary to conduct an interview before notifying my office. Early notification to my office will enable my staff to support and assist the trustee as it identifies and navigates the appropriate breach response.

[64] Regarding the description of the information involved, in one notice template, the information was described as health information relating to the affected parties' obstetrical history, prenatal details, assessment and care while at the JPCH. In addition, information

collected while in the Intensive Care Unit at the RUH was involved, which included information about assessments, care, procedures and lab results.

[65] The other notice template described the information accessed as details of their child's stay at the JPCH Maternal Services Unit including their assessments, care and any lab results for tests taken during their stay.

[66] The third notice template described the information as assessments, care, procedures and lab results relating to a stay at the RUH.

[67] As discussed above, during our investigation, we learned that in addition to the clinical information that was accessed, the Snooper accessed, in some cases, demographic information such as the name, address, date of birth and health services card number. The notices should have included this detailed information about the nature of the information that was accessed so that individuals could have made an informed decision about the risk to them of this privacy breach.

[68] Before I turn to address my recommendations regarding the content of the breach notices, I note that the SHA has been managing privacy breaches under HIPA since it was created at the end of 2017. On June 29, 2018, I issued Investigation Report 083-2018, 084-2018, setting out my office's expectations regarding the contents of the notice to affected parties.

[69] The failure to inform affected parties of the demographic information involved in the breach such as the affected parties' names, dates of birth, addresses and health services numbers was contrary to recommendations made by my office in previous reports such as Investigation Report 032-2022. It should also include a requirement to provide copies of the audit logs which reflect the dates and name of any snooper that is involved (see Investigation Report 266-2024, 031-2025).

[70] As set out above, no information was provided to the affected individuals about the risk of identity theft and of any precautions that they could take to protect themselves, including by applying for a new health services card.

[71] The notification letters should have included an offer to arrange for the replacement of the individual's health services card or provided the affected parties with information about how to do that. As set out in my office's *Privacy Breach Guidelines for Trustees* and in Investigation Report 080-2022, the notice should have included information about the actions the individual can take to further mitigate the risk of harm and protect themselves.

[72] I recommend that, within 30 days of the issuance of this Investigation Report, the SHA review its policies and procedures regarding notification and take steps to ensure there are clear requirements to notify affected individuals of a privacy breach at the earliest opportunity and to notify my office within ten calendar days of initiating its "containment" of a privacy breach.

[73] I recommend that, within 30 days of the issuance of this Investigation Report, the SHA review and revise its work standard on notification to the affected individuals to ensure that it specifically addresses incidents of snooping and requires measures are in place to:

- identify the Snooper and the disciplinary action taken against them;
- provide detailed information about the nature of the information that was accessed, the risks that may arise from the breach and how to address the risks;
- include copies of excerpts from electronic logs which apply to the affected individual, highlighting the access(es) which reflect the breach(es), including the dates of unauthorized accesses and the name of the snooper; and
- where health services card numbers were accessed, provide information setting out an explanation of the risk of identity theft and advice about how to change their health services numbers.

[74] Given the passage of time since the breaches occurred, I will not recommend that SHA resend its notices to affected parties except in relation to those affected parties whose health services card was involved.

[75] Accordingly, I recommend that, within 30 days of issuance of this Investigation Report, the SHA contact the individuals whose health services card number was involved in the

breach and advise them of the steps that they can take to apply for a new health services card number.

Investigate the breach

[76] After containing the breach and notifying affected parties, government institutions and trustees should conduct an internal investigation. Where snooping is involved, my office's *Privacy Breach Guidelines for Trustees* at pages 6 to 7, recommends the following steps when doing an investigation:

- Record details of how the breach came to light.
- Suspend employee's access to the personal health information.
- Retrieve log information if available, Interview the employee in question (establish if the employee may have shared their user account and identification and routinely logged out of account).
- Identify and interview any witnesses.
- Review the privacy training the employee in question has received (have warnings of routine audits been given?).
- Review any relevant contracts.
- Consider who needs to be notified (e.g., supervisor, union, police, 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 the IPC for further advice.

[77] Based on a review of the materials and information provided by the SHA to my office, it appears that the SHA took the following steps to investigate the breach:

- The SHA retrieved and reviewed audit reports on the SCM and ISP system which captured the Snooper's access to patient records, the identity of the patients, the nature of the information viewed, the date of the access and the computer used to access the systems.

- The SHA immediately terminated the Snooper's access rights and deactivated SHA IT assets. It also "made arrangements to have the laptop returned" although it was unclear on when that occurred.

- The SHA conducted two interviews of the Snooper when they returned to work in January of 2024. It determined that the Snooper accessed personal health information without a need-to-know.

- The SHA identified snooping as the root cause of the breach. The SHA reviewed the safeguards in place and also identified the need to amend its Work Standard on "Removing Access" to ISP so that it clarified when to terminate access rights for employees who are on a leave of absence. It reviewed the role-based access controls for the ISP system and eliminated the position formerly occupied by the Snooper.

[78] These were important first steps. However, it appears that the SHA did not give sufficient consideration to the need for further safeguards, policies and procedures.

[79] Section 16 of HIPA sets out the duty of trustees to take steps to protect personal health information in their custody or control. It is one of the most important provisions of HIPA, placing a duty on trustees to make sure they have comprehensive written policies and procedures to keep trustees from falling short in their duties. That section states:

> **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.

[80] This provision requires the implementation of measures such as privacy policies, procedures and practices, audit functionality, privacy training and awareness raising initiatives (see my office's *Privacy Breach Guidelines for Trustees*).

[81] Subsection 23(2) of HIPA also includes requirements that are relevant here. It states:

> **23**(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.

[82] One of the consequences of a failure to have adequate safeguards in place as required by section 16 and subsection 23(2) of HIPA is that there is a greater risk that patients' personal health information will be collected, used, or disclosed without legal authority. In the analysis that follows, I will consider the factors that contributed to the breach and make recommendations on how the SHA can improve its practices to help ensure compliance with section 16 and subsection 23(2) of HIPA.

Training and Confidentiality Pledges

[83] I have repeatedly stated that users of systems that contain personal health information should be required to complete privacy and security training and sign a confidentiality pledge or undertaking as a condition of gaining access to systems that contain personal health information (see for example Investigation Report 161-2018). These are important administrative controls and are required pursuant to subsection 16(1) of HIPA.

[84] In addition, since August of 2023, *The Health Information Protection Regulations, 2023* (HIPA Regulations) includes specific requirements regarding training and pledges of confidentiality in section 5. Section 5 of the 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.

[85] Previous investigation reports from my office have been clear that the privacy training and confidentiality undertakings or pledges must be refreshed annually (see Investigation Report 320-2017, Investigation Report 161-2018, Investigation Report 413-2019, et al and Investigation Report 164-2023, et al.)

[86] According to the SHA, the Snooper received privacy training on January 19, 2021 using the SHA privacy training module that was dated 2019. It appears that the *Pledge of Confidentiality* was signed at the same time.

[87] It appears that the Snooper may not have been offered privacy training after January 2021, because they were on leave from August 30, 2021. However, when asked if additional privacy training was needed to mitigate the risk of a similar breach occurring in the future, the SHA stated that "additional training would be provided as staff expand their levels of care." This appears to contradict the SHA's *Policy: Privacy and Confidentiality* (revised April 19, 2024) which states that all SHA staff are required to complete privacy training annually and/or as directed by their supervisor. It also appears to contradict what the SHA stated in Investigation Report 266-2024, 031-2025 where it stated that it required employees to sign its *Pledge of Confidentiality* annually.

[88] Consistent with my comments in Investigation Report 266-2024, 031-2025, I also encourage the SHA to place greater emphasis on educating its staff about the potential for prosecutions for privacy breaches within the *Pledge of Confidentiality*, as it is silent on this possibility.

[89] My recommendation regarding training and confidentiality pledges appears in the next section of this Investigation Report.

[90] Below I will consider if the SHA had adequate safeguards in place relating to audits, access controls and warning flags and whether they were followed.

Audit

[91] I addressed the requirement to develop an audit program in Investigation Report 176-2015. That case involved a technologist who accessed personal health information of family members without legal authority. Regarding the requirement for audits, I stated:

> [34] Auditing is a technical safeguard. It is a manual or systematic measurable technical assessment of employee access to a system or application. Auditing of information systems is necessary to:
>
> - Assess compliance with and measure effectiveness of policies and procedures;
> - Assess compliance with legislative requirements;
> - Assess whether appropriate measures are in place to control access; and
> - Monitor access.

[92] Regarding the purpose and benefits that flow from an auditing program, I stated:

> [35] … An audit program includes regular monitoring of behavior to determine whether users are complying with the organizations privacy and security policies when accessing and using data. Further, it serves as a deterrent to unauthorized access to patient records, and it supports other privacy activities, including providing evidence for the investigation of privacy breaches and privacy complaints. Monitoring for compliance with policies and procedures can identify gaps in user training and awareness, and areas that need reinforcement. It can also provide information useful for modifying a role-based access control model.

[93] In my office's Investigation Report 176-2015, the Saskatoon Regional Health Authority (SRHA), which has now been subsumed by the SHA, stated that it did not have in place a "broader audit policy for its electronic health record systems." During the investigation, my office was advised that the policy had been worked on and was in draft form. Because it did not have the policy in place, I found that the SRHA was "not in compliance with section 16 or subsections 23(1) and (2) of HIPA." I recommended that SRHA "finalize its broader audit policy and procedure for all electronic health record systems by July 1, 2016 and have it implemented by October 1, 2016."

[94] In my office's Investigation Report 284-2017, which also involved the SHA and a snooping incident, I recommended the SHA implement an auditing program and the development of an auditing work standard for the Procura system that was used to store personal health information of patients receiving homecare.

[95] In 2016, my office issued a blog entitled, *Unauthorized Access* which recommended that audits be conducted regularly to ensure policies and procedures are being followed. In May of 2017, my office issued guidance in *Audit and Monitoring Guidelines for Trustees* where I stated that auditing and monitoring of accesses are necessary to safeguard personal health information and are required pursuant to section 16 of HIPA. The auditing program should include random audits and focused auditing. I stated:

> **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.
>
> The trustee should consider the following when developing a random audit process:
>
> - The individual(s) responsible for conducting random audits of user activity;
> - The frequency of random auditing. Where the number of users and the volume of accesses are great, the frequency of monitoring should increase;
> - The reasonable number of users to randomly audit each audit cycle; and
> - Events that may trigger a focused audit.
>
> **Focused Auditing**
>
> A focused audit may be initiated if a complaint is made by a staff member or the general public or if a monitoring activity triggers a more in-depth investigation. All suspected incidents should be investigated and reported in accordance with the trustee's incident management policies and procedures.

[96] More recently, in Investigation Report 168-2024, et al my office investigated allegations of snooping involving the electronic Health Record (eHR) Viewer and the Pharmaceutical Information Program. I recommended that the Ministry of Health and eHealth

Saskatchewan ensure that random user audits for both systems are put in place as soon as possible, while noting that I had made these recommendations in the past.

[97] In the context of my investigation in Investigation Report 266-2024, 031-2025, SHA stated that it is "working on building standard auditing processes."

[98] Other Information and Privacy Commissioners have spoken about and made rulings addressing the importance of random auditing programs to address snooping. In ON IPC issued guidance entitled *Detecting and Deterring Unauthorized Access to Personal Health Information*. In that guidance, the ON IPC stated that logging, auditing and monitoring can be an effective deterrent to unauthorized access if all agents are made aware that all of their activities in relation to electronic records of personal health information will be logged, audited and monitored on an ongoing, targeted and random basis.

[99] In Order HO-013, the ON IPC described the role of auditing in protecting personal health information:

> Auditing of electronic information systems is particularly important in ensuring that the privacy of individuals and the confidentiality of personal health information are protected. Audits are essential technical safeguards for electronic information systems. They can be used to deter and detect collections, uses and disclosures of personal health information and the copying, modification or disposal of records of personal health information that contravene the Act. As such, they help to maintain the integrity and confidentiality of personal health information stored in electronic information systems. The ability to conduct audits of personal health information and the activities of agents or users (referred to in this section as users) in an electronic information system also ensures that a health information custodian is able to respond to requests from patients for information about who has collected, used or disclosed their personal health information.

[100] I issued Investigation Report 176-2015 on January 29, 2016, which is over eight years ago. The SHA, who has assumed authority over the SRHA, has advised my office that it does not have an audit policy. More specifically, it stated that for the SCM and ISP systems "no formal audit policy was in place" and audits were completed on request.

[101] I am concerned that the SHA has not taken steps to address the need for an auditing program for the SCM and ISP systems in use in the hospitals it manages. I find that SHA's failure to have in place a policy or work standard that requires regular random and focused audits of the SCM and ISP systems is contrary to section 16 and subsection 23(2) of HIPA. Therefore, I find that the SHA did not comply with section 16 and subsection 23(2) of HIPA.

[102] My recommendations regarding audit appear in the next section of this Investigation Report.

Access controls

[103] Access to personal health information in systems should be subject to reasonable technical, administrative and physical controls having regard to a user's need to know for the purpose of providing health care. 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. These controls include technical controls such as the use of login usernames, minimum requirements for passwords, multifactor authentication, requirements for automatic system timeouts, and search and access controls based on the user's role in providing health care services. Administrative controls include policies prohibiting sharing passwords, remote access controls and acceptable use policies. Training and confidentiality pledges, discussed earlier, are also a type of administrative control.

[104] Role-based access controls, which the SHA had in place in the ISP system, that limit who has access to what information are one of the best ways to protect information based on a need to know (Office of the Privacy Commissioner of Canada, Office of the Privacy Commissioner of Alberta and Office of the Information and Privacy Commissioner of British Columbia, *Getting Accountability Right with a Privacy Management Program*, April 2012).

[105] However, role-based access controls are not sufficient by themselves. As set out in the ON IPC's guidance, *Detecting and Deterring Unauthorized Access to Personal Health Information* at page 18, where a person only requires access for a specified period of time, policies and procedures should set out the process for ensuring that access and use is only permitted for that period of time.

[106] In this case, the need to terminate the Snooper's access rights arose because they had an SHA issued laptop that they used to work from home one day a week. Once they went on leave, that access was no longer required. Based on a review of applicable policies and work standards, it is apparent that one of the shortcomings of SHA's policies and work standards that govern access rights was that they did not consider the need to terminate access rights to SCM and ISP for staff who were on leave of absence, as was the case here. In addition, it is apparent that the Snooper and their Manager did not comply with SHA policies and work standards. I now turn to the analysis supporting these findings.

[107] The relevant SHA policies are:

- "Acceptable Use of Information Technology (IT) Assets."
- "Remote Access."
- "Privacy and Confidentiality."
- "Workplace Expectations Policy."

[108] Also relevant to the analysis that follows are the following work standards applicable to the use of the ISP system in the maternity unit of the JPCH:

- WS User accounts – "Assigning ISP user permissions."
- WS User accounts – "Removing ISP users."

[109] SHA's "Acceptable Use of Information Technology (IT) Assets" policy dated September 14, 2023, defines Information Technology Assets (IT) as:

> All IT equipment and components, managed and owned by SHA and/or eHealth; … as well as information transmitted, processed and stored through these technologies.

[110] Among the various purposes of this policy was the requirement to protect IT assets from unauthorized access. It includes requirements for users to comply with HIPA. There are

requirements for users to follow all SHA policies, access only the required IT assets to perform their job responsibilities, "access only the minimum identifiable confidential information, sensitive information PI and PHI required to perform their job function and maintain confidentiality of all SHA information."

[111] Under the same policy, managers are required to restrict or remove IT assets for team members if they violate this policy and "disable or terminate SHA issued user accounts in a timely manner."

[112] In response to questions posed by my office, the SHA stated that:

> Managers are responsible for ensuring that only staff who require access in order to deliver patient care are provisioned with an SCM account.

[113] Other than the policies listed above, SHA stated that there is no access control policy or work standard applicable to the SCM system and added that:

> Managers are responsible for submitting user account request forms for their staff on their department that require access to use SCM for their daily work. Managers are also responsive for submitting a similar user account request form when staff leave their department to have access terminated.

[114] The "Remote Access" policy dated December 4, 2017, was applicable to the Snooper whose job required them to work from home once a week. It included the following requirements:

- Access to SHA networks and data is intended for SHA business only and remote access will be granted on a "need-to-use basis and on an event-by-event basis based on the minimum requirement for functional roles."
- Remote access must be terminated once the user's role or job responsibilities no longer require it.

[115] Paragraph 4.2 of the above noted policy states:

> **Managers**
>
> 4.2.1 Evaluate requests for remote access and either approve or reject requests.

> 4.2.2 Review the need for remote access when users have changed roles or jobs, including promotion or demotion, and, where necessary, submit requests to remove unnecessary access.
>
> 4.2.3 Ensure that remote access privileges are immediately removed or blocked when users have left the organization.

[116] As noted above, the Snooper used an SHA-issued computer to access personal health information. Initially, the SHA stated that "Digital Health teams work with managers and or human resources teams when permissions need to be temporarily disabled for various reasons." While there appears to have been in place a general requirement to terminate access rights where there is a change in job roles or where a person no longer requires it, there was no specific requirement to terminate access rights when staff went on leave of absence.

[117] Despite that, I find that the Manager's failure to terminate the Snooper's access rights after it was clear that the Snooper would be on an extended leave of absence was a failure to comply with SHA's "Acceptable Use of Information Technology (IT) Assets" and "Remote Access" policies. Both of these policies require the Manager to terminate the access rights when employees no longer require it for their role, as was the case here.

[118] The SHA's "Workplace Expectations" policy number SHA-06-007 was also applicable here. It requires that staff are responsible and accountable to the SHA for efficient, effective and ethical use of resources.

[119] The Work Standard relating to "Removing ISP" states that when a user no longer requires access to the ISP system, the accounts will be removed from the ISP application. It provides three examples: 1) students who were working on a temporary basis departed; 2) physicians working on a temporary basis departed; and 3) users have left the department because they were transferred to other service lines, terminated or retired. The work standard includes information about how to remove access. It does not mention leaves of absence.

[120] The SHA stated that it is working on updating this ISP work standard to clarify that when staff are on leave for more than 30 days, access rights will be terminated. I agree that this amendment is necessary and will include it in my recommendations.

[121] Policies that permit work from home create privacy and security risks that need to be addressed by all trustees and public bodies. The SHA should have considered how it would manage the risk of unauthorized access given that the work from home has been permissible for some staff since COVID 19.

[122] It also appears that there was no requirement to retrieve IT assets, such as laptop computers, that enable access to SHA systems, when staff no longer require these assets because of a leave or for any other reason.

[123] I find that SHA failed to comply with section 16 of HIPA by not having policies or work standards in place to ensure that access rights and IT assets such as laptop computers, are terminated or retrieved within 30 days of an indefinite leave, such as a sick leave. Where a leave of absence is for a defined period, such as a maternity leave, the policies or work standard should have required the termination of the access rights and retrieval of the IT assets at the start of the leave and for that defined period.

[124] My recommendations regarding termination of access rights appear in the next section of this Investigation Report.

[125] The JPCH did not have a work standard regarding access that applied to the SCM system. The SHA stated that the SCM system is controlled by the SHA.

[126] The SHA advised my office that SCM has a "built-in process" for employees that are on a maternity leave or sick leave. After 180 days of leave, the employees' access automatically turns off. However, access is only terminated if the employee does not access the system for 180 days. If an employee accessed the SCM system from home while on their maternity leave, even if they did so without lawful authority, for example, the clock would not start running on the 180 days and the employee would continue to have remote access despite

the fact that they don't need it for their work. This is not sufficient to ensure that only employees with a need-to-know personal health information stored in the SCM can access it.

[127] My other concern is that 180 days is too long. If the SHA knows that an employee will be away from work for a defined period, access should be terminated, and IT assets should be retrieved at the beginning of the defined period. If the leave is for an undefined period, the access rights should be terminated on the 30th day of the leave.

[128] These SCM access controls are not adequate and are a violation of subsection 16(b)(iii) of HIPA because they do not protect against any reasonably anticipated unauthorized access to the SCM system by staff with work from home privileges. The SHA should take steps to address this on an urgent basis. My recommendations appear in the next section of this Investigation Report.

Warning Flags

[129] I now consider the system warning flags that the SHA had in place in the SCM and ISP.

[130] Privacy notices and warning flags that are built into systems are helpful tools to remind users of their obligations to protect personal health information and of the consequences of accessing this information in contravention of HIPA or applicable policies. As awareness raising tools, they may prevent or reduce the risk of unauthorized access to personal health information and deter unauthorized access. Similar conclusions have been made in other jurisdictions such as in Ontario where the ON IPC issued Order HO-013 on December 16, 2014 under the Ontario *Personal Health Information Protection Act*. In that Order, the ON IPC stated that notices alerting users of the consequences of using or disclosing personal health information in contravention of Ontario's health privacy law can be effective tools for protecting privacy.

[131] According to the SHA, in SCM a warning flag is attached to all closed patient files and to patient files for whom a user is not known to be providing health care. Warning flags may

also be attached to records of co-workers. Users would have to bypass or click through a screen to obtain access to the file. On each of the occasions when the Snooper clicked through the warning screen to access the charts, they entered as the reason "Audit/Chart Review" and clicked on the "OK" button thereby asserting that they had authority to access the information.

[132] In the ISP system, if a patient chart is closed and a user tries to open it, they will encounter a "warning window" stating that the chart is closed and asking if they are sure that they want to open it. The user must indicate either "yes" or "no." If the user enters "yes", then the file is opened and the "Patient Access Warning Window" disappears.

[133] According to the audit logs provided to my office, the Snooper encountered both types of warnings or notices when they accessed the SCM and the ISP systems. These are helpful measures to remind users that they may not have a need or right to go further.

[134] However, it is apparent that in this matter, the Snooper disregarded or clicked through the warnings or notices that appeared on the SCM and ISP system for some patient files and proceeded to access them despite the lack of authority or need-to-know. By disregarding the system warnings without a need-to-know, the Snooper's actions were a blatant violation of SHA policy and HIPA.

[135] The SHA should take steps to ensure that the warning flags in place include information about the risks of accessing personal health information without authority. It should also ensure that these are in place after logging into a system and are implemented throughout the SHA. My recommendations appear in the next section of this Investigation Report.

[136] As all of these issues were overlooked by the SHA, I find that the SHA did not conduct an adequate investigation. In particular, the SHA failed to identify the shortcomings in its technical and administrative safeguards that contributed to the breaches. I also find that the SHA failed to comply with section 16 and subsection 23(2) of HIPA.

Take appropriate steps to prevent future breaches

[137] Once trustees contain a breach and identify a root cause, they should consider and implement solutions that help prevent the same type of breach from occurring again. Prevention is one of the most important steps. A privacy breach cannot be undone but a trustee can learn from one and take steps to help ensure that it does not happen in the future.

[138] To address the privacy breach, the SHA terminated the Snooper's employment and identified the root cause of the breach as snooping/curiosity. Regarding the factors that contributed to the breach it said that user accounts were not disabled as soon as it was determined that the employee was to be off work for more than a brief period of time. I agree.

[139] The Manager's failure to terminate the Snooper's access rights after 30 days of leave appears to have been contrary to SHA's own policy and a contributing factor. However, the specific Work Standards that applied to removing access to the ISP system should have been made clearer so that Managers and supervisors would know that absence due to a leave was a factor triggering a requirement to terminate access rights.

[140] Regarding additional changes proposed by SHA, it stated:

> We will be developing a policy for employees with remote access to suspend accounts if away from the workplace for greater than 30 days.

[141] It added:

> Additional training will be provided to all staff as they expand their levels of care with the continued emphasis on privacy and the principles of "need to know."

[142] In the previous section of this Investigation Report, I set out my findings regarding the SHA's safeguards in place to protect personal health information. To address the shortcomings, I will make the following recommendations.

[143] I recommend that the SHA, within 30 days of issuance of this Investigation Report, take any steps necessary to ensure that privacy training and signed confidentiality pledges are made mandatory annually for all staff with access to personal health information.

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

[145] I recommend that the SHA, within 30 days of issuance of this Investigation Report, develop a proactive or routine audit policy for ISP and provide it to my office.

[146] I recommend that the SHA, within 30 days of issuance of this Investigation Report, amend the ISP work standard, "Removing ISP Users" to add the following additional requirements:

- for indefinite leaves, access rights should be terminated and IT assets such as laptops should be retrieved on the 30th day of the leave and continued until the user returns to work.
- for leaves for a defined period, such as a maternity leave, access rights should be terminated and IT assets such as laptops should be retrieved on the first day of the leave and be continued for the period of the leave.

[147] I recommend that the SHA, within 30 days of issuance of this Investigation Report, develop a plan to address the need to improve the access controls on the SCM by aligning them with the ISP controls recommended above and provide my office with a copy of the plan.

[148] I recommend that the SHA, within 30 days of issuance of this Investigation Report, develop a plan to add a pop-up or warning screen to all of the electronic health records systems in place in the province that warns users logging in to the system that access is only permitted where there is a need to know the information; access is regularly audited, and that inappropriate access may lead to suspension or termination of the users employment and prosecution. The user should be prompted to acknowledge that they have authority to access the information by clicking yes or no.

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

[149] At this time, I must consider if the privacy breaches at issue warrant a recommendation that the Snooper be prosecuted for a violation of HIPA pursuant to section 64 of HIPA.

[150] Prosecution of snooping employees can be an effective deterrent. In *Detecting and Deterring Unauthorized Access to Personal Health Information*, the ON IPC called for an increase in the number of prosecutions of those who snoop. He stated:

> 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.

[151] By its nature, snooping is harmful and intrusive, and, as noted above, it erodes the public's trust in an institution.

[152] In Saskatchewan, snoopers of personal health information are subject to the offence provisions embedded in section 64 of HIPA. In the present case, subsections 64(1)(a) and (3.2) of HIPA are relevant:

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

[153] Based on information provided by the SHA about its training and the applicable policies, it appears that the Snooper would have known that their actions would be in contravention of HIPA, and the JPCH and SHA policies. Moreover, the Snooper was required to actively

assert a reason for gaining access to personal health information on multiple occasions and subsequently admitted that they did not have the authority to do so.

[154] The two criteria required for subsections 64(1)(a) and (3.2) of HIPA to apply are that the snooper's actions or contraventions of HIPA be *knowingly* and *willfully* committed. These terms are defined in *Black's Law Dictionary* (12th edition, 2024) as follows:

- 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]

[155] In the circumstances of this case, I find that a recommendation that the Ministry of Justice and Attorney General consider a prosecution under section 64 of HIPA is warranted. Therefore, I recommend that the SHA forward its investigation file and this Investigation Report to the Ministry of Justice and Attorney General, Public Prosecutions Division to allow prosecutors to consider whether an offence has occurred and if charges should be laid under HIPA.

III FINDINGS

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

[157] I find that privacy breaches occurred.

[158] I find that the SHA took reasonable steps to contain the breach.

[159] I find that SHA's notices to the affected parties were not adequate.

[160] I find that the SHA conducted an adequate investigation into the breach.

[161] I find that the SHA's plan to prevent future breaches of this nature is not adequate.

[162] I find that the SHA did not comply with section 16 and subsection 23(2) of HIPA.

[163] I find that, based on the information provided by the SHA, the Snooper should have known that their actions contravened SHA policies and HIPA.

[164] I find that a recommendation for prosecution pursuant to section 64 of HIPA is warranted.

IV RECOMMENDATIONS

[165] I recommend that, within 30 days of the issuance of this Investigation Report, the SHA take any steps necessary to ensure that privacy training and signed confidentiality pledges are made mandatory annually for all staff with access to personal health information.

[166] I recommend, as a deterrent to future snooping, the SHA notify its staff of the name of the Snooper and of the disciplinary actions taken in relation to the privacy breaches at issue here.

[167] I recommend that, within 30 days of the issuance of this Investigation Report, the SHA review its policies and procedures regarding notification and take steps to ensure there are clear requirements to notify affected individuals of a privacy breach at the earliest opportunity and to notify my office within ten calendar days of initiating its containment of a privacy breach.

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

[169] I recommend that, within 30 days of the issuance of this Investigation Report, the SHA review and revise its work standard on notification to the affected individuals to ensure that it specifically addresses incidents of snooping and requires measures are in place to:

- Identify the snooper and the disciplinary action taken against them.
- Provide detailed information about the nature of the information that was accessed, the risks that may arise from the breach and how to address the risks.
- Where health services and/or social insurance numbers were accessed, provide information setting out an explanation of the risk of identity theft and an offer of credit monitoring for a period of five years where appropriate and advice about how to change their health services and/or social insurance numbers.

[170] I recommend that, within 30 days of issuance of this Investigation Report, the SHA contact the individuals whose health services card numbers were involved in the privacy breach and advise them of the steps that they can take to apply for new health services card numbers.

[171] I recommend that, within 30 days of issuance of this Investigation Report, SHA develop a proactive or routine audit policy for ISP and provide it to my office.

[172] I recommend that, within 30 days of issuance of this Investigation Report, the SHA amend the ISP work standard on "Removing ISP Users" as follows:

- For indefinite leaves, access rights should be terminated and IT assets such as laptops should be retrieved on the 30th day of the leave and continued until the user returns to work.
- For leaves for a defined period, such as a maternity leave, access rights should be terminated and IT assets such as laptops should be retrieved on the first day of the leave and be continued for the period of the leave.

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

[174] I recommend that, within 30 days of the issuance of this Investigation Report, SHA develop a plan to address the need to improve the access controls on the SCM by aligning them

with the ISP controls recommended in paragraph [172] above and provide my office with a copy of the plan for review and comment.

[175] I recommend that, within 30 days of the issuance of this Investigation Report, the SHA develop a plan to add a pop-up or warning screen to all of the electronic health records systems containing personal health information in the custody or control of the SHA that advises users upon login that:

- access is only permitted where there is a need to know the information;
- access is regularly audited;
- inappropriate access may lead to suspension or termination of users' employment and prosecution under HIPA; and
- the user is required to acknowledge by clicking "yes" or "no" that they have authority to access the personal health information stored in the system.

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

Dated at Regina, in the Province of Saskatchewan, this 23rd day of April, 2025.

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