Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 218-2025[1]

Saskatchewan Health Authority

April 23, 2026

Summary: The Complainant learned that a pharmacy technician (technician) who is an employee of the Saskatchewan Health Authority (SHA) disclosed information about the Complainant's health status to two different individuals on two separate occasions through the messaging app, Snapchat. The Complainant contacted SHA, who investigated. The Complainant was dissatisfied with the SHA investigation and contacted the Office of the Saskatchewan Information and Privacy Commissioner (OIPC) to seek a review. The OIPC opened an investigation file to determine if the handling of the breach on the part of SHA was appropriate.

The Commissioner made several findings, including that: (1) *The Health Information Protection Act (HIPA)* is engaged and OIPC has jurisdiction to investigate; (2) a privacy breach occurred because the SHA technician had no authority under *HIPA* to disclose the Complainant's personal health information and no consent from the Complainant to do so; (3) SHA took appropriate steps with respect to containment of the breach and in terms of notification efforts; (4) SHA had sufficient administrative safeguards in place to prevent the breach from occurring - the root cause being that the technician failed to regard or fully comprehend those safeguards; and (5) SHA took appropriate actions to address the root cause of the privacy breach with the technician, including disciplinary actions and retraining. The Commissioner made no recommendations with respect to this matter.

[1] This Investigation Report includes OIPC files 364-2025, 020-2026 and 021-2026.

I BACKGROUND

[1] On April 8, 2025, the Complainant contacted the Saskatchewan Health Authority (SHA) and complained that a pharmacy technician (technician) had publicly disclosed their health status information on two separate occasions without their consent. The Complainant alleged the following:

> The first incident would have taken place between September 18 2023 – September 20th, 2023. I had gone to the Yorkton regional hospital at about 7:30am on... September 18th, well there we had found out we were expecting, and I had been into the hospital for [health issue][2]. On the morning of the 19th well I'm still in the hospital, my boyfriends sister [recipient one] received a Snapchat message from [the technician] who is the pharmacist tech at the hospital, [the technician] had Snapchat messaged my boyfriends sister and told her something along the lines of "[the Complainant] was admitted to paediatrics floor which can only mean one thing." Implying to my boyfriends sister that I was pregnant. If I had not spoken to her that morning and told her this moment would have been taken from us due to [the technician's] careless actions.
>
> The second incident would have taken place between April 26, 2024 to April 29th, 2024 when we went to the Yorkton regional hospital to have our baby. A mutual friend [recipient two] received a Snapchat message from [the technician], this message was stating that I was at the hospital having my baby. I do not think it's anyone's business to disclose information like this unless the couple choose to themself.

[2] The Complainant acknowledged that the messages were not saved by the recipients (recipients one and two) because they were sent via Snapchat. Snapchat messages typically auto-delete after 24 hours.[3] Neither SHA nor this office ever received copies of the messages for this reason. The Complainant suspected the technician sent the messages intentionally through Snapchat because the messages autodelete and the Snapchat application notifies the sender if and when a recipient saves screenshots of messages.[4] The

[2] All words in square brackets are amendments to ensure the privacy of the parties involved.

[3] *When does Snapchat delete Snaps and Chats?* – Snapchat Support.

[4] When a recipient of a message takes a screenshot of a Snapchat message, the sender receives n icon notification of such (https://help.snapchat.com/hc/en-us/articles/7012315702548-What-do-the-icons-on-the-Chat-Screen-mean).

Complainant acknowledged a several month long delay in filing the complaint but noted that they had no knowledge of the incidents at the time of occurrence and notification occurred much after the fact. On April 9, 2025, SHA requested additional details from the Complainant, which the Complainant provided the same day.

[3] On June 25, 2025, the technician's manager contacted the Complainant to discuss the conclusions of the investigation. The manager advised that "corrective action had occurred" but details were not provided to the Complainant. The manager then advised the Complainant that an audit had been conducted, and it was concluded that the technician had not inappropriately accessed the Complainants personal health information files. Finally, the manager advised the Complainant of the right to contact the Office of the Saskatchewan Information and Privacy Commissioner (OIPC) if dissatisfied with the SHA response.

[4] On June 26, 2025, the Complainant contacted this office with three main concerns. The Complainant was dissatisfied with the SHA response to the privacy breach because SHA: (1) had not contacted the two recipients to obtain their account; (2) had not addressed the root cause of the privacy breach; and (3) had failed to convey details with respect to the corrective actions on the part of SHA.

[5] On January 14, 2026, OIPC sent notice of investigation to the Complainant and SHA. In the notice, OIPC outlined details of the two alleged privacy breaches, and added that it appeared SHA concluded that a privacy breach had occurred. The investigation would commence under sections 42(1)(c) and 52 of *The Health Information Protection Act* (HIPA).[5]

[6] On January 30, 2026, OIPC sent notice to the technician (OIPC files 020-2026 and 021-2026) advising them of the right to make a voluntary submission to OIPC.

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

[7] On February 17, 2026, SHA sent its completed *Privacy Breach Investigation Questionnaire* to OIPC along with several supporting documents.

[8] On March 26, 2026, the technician provided a submission to OIPC.

II DISCUSSION OF THE ISSUES

1. Jurisdiction

[9] *HIPA* is engaged when three elements are present: 1) there is a trustee; 2) there is personal health information; and 3) the trustee has custody or control of the personal health information.

i. First element - trustee

[10] SHA qualifies as a "trustee" pursuant to section 2(1)(t)(ii) of *HIPA*.

[11] The technician is with Yorkton Regional Health Centre (YRHC) in pharmacy services. This is a facility of SHA. According to the SHA job description, pharmacy technicians are responsible for "the acquisition, preparation, checking and distribution of medications/ pharmaceutical products and supplies to Nursing Units, facilities and other community based health care services." Section 2(1)(a)(i), (ii) of *The Health Information Protection Regulations, 2023* (*HIPA Regulations*)[6] defines an employee as follows:

> **2**(1) In these regulations:
>
> …
> **"employee"** means:
>
> (a) an individual:
>
> (i) who is employed by a trustee, including an individual retained under a contract to perform health services for the trustee; and

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

(ii) who has access to personal health information; or

…

but does not include a health professional who is retained under a contract, what is not an employment agreement, to perform services for the provincial health authority;

[12] As an employee of SHA, the technician was bound by *HIPA*.

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

ii. Second element – personal health information

[14] For reasons explained later in this Investigation Report, this office concluded that the second allegation didn't constitute a privacy breach. The second allegation will not be included in our discussion on the second and third elements in this part of the Investigation Report.

[15] The technician stated with respect to the first allegation that while on duty at YRHC, they saw the Complainant's name on a "movement report" that is reviewed in the course of their job duties. The technician is familiar with the Complainant and knows the Complainant's partner and the partner's sister. Based on the nature of the report and the Complainant's ward at YHRC, the technician jumped to the conclusion that the Complainant was expecting. This prompted the first Snapchat message to recipient one. SHA identified this recipient as the sister of the Complainant's partner.

[16] SHA confirmed that a movement report contains the following data elements: name, medical record number, visit number, care level, event (discharge, transfer or admit) and location (room number).

[17] The Complainant's personal health information was involved under sections 2(1)(m) and (ii) of *HIPA*: [7]

[7] OIPC Investigation Report 097-2025 at paragraph [16].

> **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;

[18] The second element is present for *HIPA* to be engaged.

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

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

[20] The technician fairly conceded that the hospital movement report with the Complainant's details was viewed in the course of employment.The movement report contains information that is in the custody or control of SHA.[9]

[21] The third element for *HIPA* to be engaged is present. OIPC has jurisdiction to undertake this investigation under the jurisdiction afforded by *HIPA*.

[8] OIPC Investigation Report 036-2025 at paragraph [25].

[9] *Ibid.*

2. Did a privacy breach occur?

[22] A privacy breach occurs when personal health information is collected, used and/or disclosed with out authority under *HIPA*. *HIPA* does not define *disclosure*, but OIPC defines it to mean the sharing of personal health information with a separate entity, not a division or branch of the trustee with custody or control of that information.[10]

[23] This office concluded the second allegation didn't result in a privacy breach. That is because the information conveyed in the second allegation was provided to the technician outside the course of employment and not as the result of information in the custody and control of SHA. The second allegation certainly involved an imprudent act of common gossip on the part of the technician, but it is not a privacy breach even though SHA treated it as such and the technician conceded as much.

[24] Regarding the first incident, section 27(1) of *HIPA* requires consent before personal health information may be conveyed. The Complainant gave no consent in this matter.

[25] At the time of the first allegation, the technician explained that they were operating under the mistaken belief that the Complainant's pregnancy was common knowledge. The technician conceded that this disclosure was made without consent, and in contravention of *HIPA*. Both SHA and the technician concede the privacy breach.

3. Did SHA properly respond to the privacy breach?

[26] There are several determinants of whether a trustee's response to a privacy breach is appropriate.

a) Was the breach contained;
b) Were the affected individuals notified;
c) Was the breach investigated; and
d) Were appropriate steps taken to prevent future breaches.

[10] OIPC Investigation Report 155-2025 at paragraph [25].

[27] This part of the analysis will focus on these steps.

a) Containment of the Breach

[28] The containment of a breach is assessed on a standard of reasonableness. The institution must demonstrate that it has reduced the magnitude of the breach and the resulting risk to affected individuals within a reasonable consideration. Containment steps include stopping the unauthorized practice, recovering records and, if necessary, revoking system access.[11]

[29] The most important step in containment of this breach was the SHA audit and interview of the technician. SHA first ascertained that there had been no snooping online and the interview revealed that this technician did not fully understand how their actions constituted a privacy breach violation.

[30] SHA also audited the technician past access with respect to SHA information systems to determine if the breach had escalated further. The audits revealed that the privacy breach had not escalated and supported a conclusion that access privileges could continue.

[31] The SHA response to the privacy breach was reasonable.

[32] The Complainant expected that both Snapchat and the recipients should have been contacted during the course of the SHA investigation. Neither of these measures would have contributed to containment of the breach. These measures are investigatory methods and in this case, the privacy breach was immediately conceded by the technician.

b) Notification of Affected Individuals

[33] It is best practice for trustees to inform affected individuals as soon as possible when personal health information has been breached. This step invokes the principles of fairness. Affected individuals should be informed of the possible risks so they can take any remedial

[11] *Supra,* footnote 8 at paragraphs [52] and [53].

steps they deem necessary to protect themselves. In this matter, the Complainant notified SHA, and the duty to inform is not present on these facts.

[34] As noted earlier, the Complainant first contacted SHA with this concern on April 8, 2025. The technician's accesses to SHA information systems were audited on April 14, 2025. Auditing continued through May 2025. The technician was interviewed June 4, 2025. The Complainant was advised of these actions on June 25, 2025. These measures were all reasonable and conducted within a reasonable period of time.

[35] The Complainant was fully advised of the nature of the breach and that there had been no further snooping activity. The manager thanked the Complainant for bringing the concern to the attention of SHA and further advised the Complainant of the right to contact OIPC. These are all elements that a trustee should include in a notice.[12] While it is best practice to follow up in writing with affected individuals, following up in person is also appropriate and perhaps preferrable.[13]

[36] The fact that the Complainant was not advised of the details of the corrective action taken in this matter is not unreasonable. That is because this is an instance where the privacy breach was on the lesser end of the scale and the result of pure ignorance rather than willful violation. The technician immediately conceded the wrongdoing, expressed great remorse and pledged to uphold the SHA privacy obligations in the future.

[37] In addition to being subject to *HIPA*, SHA is also a local authority under section 2(1)(f)(xiii) of *The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP).*[14] The exact nature of the corrective action taken, including any disciplinary actions, would constitute personal information under section 23(1)(b) of *LA FOIP,* and

[12] *Ibid,* at paragraph [56].

[13] OIPC Investigation Report 291-2018 at paragraph [19].

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

consequently protected by section 28(1) of *LA FOIP*.[15] However, section 28(2)(s) of *LA FOIP* read together with section 10(g)(i) of *The Local Authority Freedom of Information and Protection of Privacy Regulations (LA FOIP Regulations)*[16] allows local authorities to disclose certain types of personal information, including disciplinary information under the proper conditions.[17] These sections provide:

> ***LA FOIP***
>
> **28**(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:
>
> ...
> (s) as prescribed in the regulations.
>
> ***LA FOIP Regulations***
>
> **10** For the purposes of clause 28(2)(s) of the Act, personal information may be disclosed:
>
> ...
> (g) to any person where the information pertains to:
>
> (i) the performance of any function or duty or the carrying out of any responsibility by an officer or employee of a local authority;

[38] The decision whether to publicly reveal disciplinary action against an employee is best left to a case- by-case assessment. In the circumstances of this matter, the fact that SHA was not fully transparent with the Complainant is not a matter for further consideration.

[15] OIPC Review Report F-2014-005 at paragraph [17] considered employment history and disciplinary actions in that respect to be personal information under the equivalent provisions of *The Freedom of Information and Protection of Privacy Act*, SS 1990-91, c F-22.01, as amended.

[16] *The Local Authority Freedom of Information and Protection of Privacy Regulations*, RRS c L-27.1 Reg 1 (effective July 1, 1993), as amended.

[17] OIPC Review Report 018-2023 at paragraphs [41] to [44].

c) Investigation of the Breach

[39] The root cause of a breach must be identified in order to prevent a future occurrence. An investigation must address the incident on a systemic basis and include a root cause analysis.[18] Under *HIPA* a trustee has a duty to protect personal health information. Section 16 of *HIPA* mandates the establishment of policies and procedures to maintain administrative, technical and physical safeguards:

> **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the integrity, accuracy and confidentiality of the information;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the information;
>
> (ii) loss of the information; or
>
> (iii) unauthorized access to or use, disclosure or modification of the information; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[40] Administrative safeguards focus on measures intended to keep personal health information secure from unauthorized uses. They include policies and procedures regarding privacy or employee oaths.[19]

[41] As noted, the audit process allowed for a conclusion that snooping was not a contributing factor in this breach.

[42] All parties agree that the privacy breach occurred around the 18th to 20th of September 2023. After the breach, SHA advised that the technician was required to repeat and complete all privacy training modules, which included *Privacy Foundations* training and *Privacy and*

[18] *Supra,* footnote 8 at paragraph [62].

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

the Need-to-Know. SHA also required the technician to re-sign the pledge of confidentiality agreement. According to the SHA *Privacy and Confidentiality Policy*, employees are to complete privacy training annually.[20] This policy expressly states at section 3.5 that employes cannot "use or disclose PHI [personal health information] or PI [personal information] for purposes other than the reason it was collected, except with the consent of the individual or as permitted by law." The policy further states at section 4.1 that employees are to keep "confidential information private whether it is obtained purposefully or inadvertently during the course of duties."

[43] The SHA *Privacy and Confidentiality Policy* warns at section 5 that failure to follow it can result in "discipline up to and including termination/revocation of: employment; contractual relationships; practitioner staff appointment; and/or privileges." SHA's *Pledge of Confidentiality* includes similar language, and warns in item 10 that following a breach, legal action can be taken against the employee by SHA or the patient, a complaint can be made to the licensing body, a report can be made to this office by SHA, or SHA can make a complaint to the Ministry of Justice by the SHA, which could result in a fine up to $50,000.[21]

[44] The administrative safeguards to prevent a breach of this nature were in place by SHA, but the technician either disregarded them or did not fully understand them, which was the root cause of this breach.

d) Prevention of Future Breaches

[45] The need to implement measures that prevent a similar breach from occurring cannot be overstated. Possible prevention measures may include creating (or making changes to) policies and procedures, adding or enhancing safeguards already in place, providing

[20] Section 4.2 of SHA *Privacy and Confidentiality Policy* (SHA-07-003).

[21] See also section 64(2)(a) of *HIPA*.

additional training, and considering whether a practice should be stopped, to prevent a future similar privacy breach.[22]

[46] SHA outlined the disciplinary actions it took to address the breach. Because this information is technically the personal information of the technician, we observe the right on the part of SHA to remain silent in this regard. Once again, the nature of this breach is on the lower end of the scale, the technician fully conceded the breach, was remorseful and voluntarily accepted disciplinary actions and completed all privacy retraining as required by SHA. This office is satisfied with the corrective actions as taken by SHA.

III FINDINGS

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

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

[49] A privacy breached occurred because the SHA technician had no authority under *HIPA* to disclose the Complainant's personal health information and no consent from the Complainant to do so.

[50] SHA took appropriate steps with respect to containment of the breach and in terms of notification efforts

[51] SHA had sufficient administrative safeguards in place to prevent the breach from occurring, and the root cause was that the technician failed to regard or fully comprehend those safeguards.

[52] SHA took actions to address the root cause of the privacy breach with the technician, which included disciplinary measures and retraining.

[22] OIPC Investigation Report 095-2025 at paragraph [55].

IV RECOMMENDATION

[53] There are no recommendations with respect to this matter.

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

Grace Hession David
Saskatchewan Information and Privacy Commissioner