Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 005-2022, 006-2022

Saskatchewan Health Authority

September 26, 2022

Summary: Two Complainants who were employees of the Saskatchewan Health Authority (SHA), asserted that SHA violated section 27(1) of *The Health Information Protection Act* (HIPA) when it shared the Complainants' personal health information with their managers without proper consent. The SHA agreed with this assertion and apologized to the Complainants. The Complainants were dissatisfied with the SHA's response and asked the Commissioner to investigate the privacy breach. The Commissioner found that HIPA was engaged and confirmed that a privacy breach had occurred. The Commissioner also found that SHA took steps to contain the privacy breach, but should have done so sooner. In addition, the Commissioner found that while SHA provided adequate notice to the Complainants, it did not provide notice to all affected individuals and should have done so. Further, the Commissioner found that SHA conduced an effective investigation. Finally, the Commissioner found that SHA has an adequate plan for preventing similar privacy breaches from occurring in the future. The Commissioner recommended that SHA notify the other 50 affected staff of the privacy breach within 30 days of the issuance of this Investigation report.

I BACKGROUND

[1] On October 1, 2021, the Saskatchewan Health Authority (SHA) Policy Directive entitled, "Proof of Full COVID-19 Vaccination" (policy) came into effect. The policy required "team members", including employees, to provide proof of full COVID-19 vaccination or to participate in the SHA COVID-19 monitored testing program. The policy also provided an employee the opportunity to apply for accommodations that will exempt them from being vaccinated. The policy indicated that an employee's manager would not be informed of the approval/denial of their request for accommodation.

[2] On November 17, 2021, the SHA emailed denial letters to the two Complainants and their managers, addressing the Complainants' requests for COVID-19 vaccination exempt accommodations.

[3] On November 21, 2021, the Complainants emailed the SHA with the following:

> **Complainant 1:**
>
> When SHA introduced the Proof of Vaccination Policy, there is a section of Questions/Answers pertaining to this policy.
>
> Question: "Will My Manager be informed of the approval/denial of my request for accommodation?"
>
> Answer: "No, managers will not know if any employee's request for accommodation is approved or denied".
>
> My accommodation was denied on November 17/2021 and this letter was emailed to me including my supervisor. My letter can be seen below. This is a Privacy Breach.
>
> My health status is private and confidential and is not my manager's business. I have lost faith in SHA. What are you going to do about this?
>
> **Complainant 2:**
>
> When SHA introduced the Proof of Vaccination Policy, there is a section of Questions/Answers pertaining to this policy.
>
> Question: "Will My Manager be informed of the approval/denial of my request for accommodation?"
>
> Answer: "No, managers will not know if any employee's request for accommodation is approved or denied".
>
> My accommodation was denied on November 17/2021 and this letter was emailed to me including my supervisor. My letter has been attached to this email. This is a Privacy Breach.
>
> My health status is private and confidential and is not my manager's business. I have lost faith in SHA. What are you going to do about this?

[4] On December 3, 2021, Complainant 1 sent another email to the SHA with the following:

> I am requesting an update on my complaint from Nov 21/21.

[5] On December 3, 2021, the SHA replied to Complainant 1 with the following:

> I have been in contact with the Director of Accommodations and Attendance Management and we are going to connect next week so I can find out more about what had happened.
>
> What I have completed is contacting the two managers that were notified by email that they were to delete the email they had received as they were not to have received it and then delete it from [SIC] deleted items and they both informed me that they had done that.

[6] On January 5, 2022, Complainant 1 emailed the SHA with the following:

> It's been over a month and my privacy complaint with SHA is still not resolved.

[7] On January 10, 2022, the SHA replied to Complainant 1 with the following:

> The incident has been resolved please find attached a letter for you and [Complainant 2].

[8] In the letter from the SHA to Complainant 1, the SHA stated the following:

> …You are correct that managers are to not receive any notification of whether an employee was approved or denied accommodation.
>
> The breach was investigated, the error was identified, and the process for sending such emails was corrected immediately. As per my email on Dec 3, 2021 your manager has been contacted and instructed to delete the email she received as she was not to have received it and to also delete it from her deleted items, she has confirmed that this has been done.
>
> This is considered a breach of privacy under the Local Authority Freedom of Information and Protection of Privacy Act, section 23 1(a) and Health Information [SIC] Act, section 2(m), the Saskatchewan Health Authority (SHA) has an obligation under these Acts.
>
> On behalf of the Saskatchewan Health Authority, we extend our sincerest apologies. The SHA takes the protection of your personal information very seriously, and we are continuously working to improve our privacy and security measures.

> If you are not satisfied with the response of the SHA, you have the right to make a formal complaint to the Office of the Information and Privacy Commissioner. You may call (306) 787-8350 or toll free 1-877-748-2298 or visit their website at www.oipc.sk.ca.

[9] In the letter from the SHA to Complainant 2, the SHA stated the following:

> …You are correct that managers are to not receive any notification of whether an employee was approved or denied accommodation.
>
> This breach was investigated, the error was identified, and the process for sending such emails was corrected immediately. As per my email on Dec 3, 2021 your manager has been contacted and instructed to delete the email he received as he was not to have received it and to also delete [SIC] from his deleted items, he has confirmed that this has been done.
>
> This is considered a breach of privacy under *The Local Authority Freedom of Information and Protection of Privacy Act*, section 23(1)(a) and *Health Information Protection Act*, section 2(m), the Saskatchewan Health Authority (SHA) has an obligation under these Acts.
>
> On behalf of the Saskatchewan Health Authority, we extend our sincerest apologies. The SHA takes the protection of your personal information very seriously, and we are continuously working to improve our privacy and security measures.
>
> If you are not satisfied with the response of the SHA, you have the right to make a formal complaint to the Office of the Information and Privacy Commissioner. You may call (306) 787-8350 or toll free 1-877-748-2298 or visit their website at www.oipc.sk.ca.

[10] On January 11, 2022, the Complainants emailed the SHA with the following:

> An apology is not enough from SHA. This is the second time an email error has occurred regarding the vaccination status. We are requesting that SHA pay for our testing. As of last week in the daily rounds, SHA [SIC] recommended all staff to test regularly.

[11] On January 11, 2022, SHA replied to Complainant 1 with the following:

> I am sorry our apology is not enough, but as indicated in the letter that was sent to you that if you are not satisfied with the response of the SHA, you have the right to make a formal complaint to the Office of the Information and Privacy Commissioner…

[12] On January 11, 2022, the Complainants made a request for my office to investigate the alleged breaches of privacy. I note that my investigation focuses only on the alleged privacy breaches and how SHA addressed them, and not on the Complainants' requests for compensation.

[13] On January 21, 2022, my office provided notification to the Complainants and the SHA of my office's intention to undertake an investigation into the alleged privacy breach.

[14] On April 4, 2022, the SHA submitted to my office their description of the privacy breach and how they handled the breach.

II DISCUSSION OF THE ISSUES

1. Is HIPA engaged?

[15] HIPA is engaged when three elements are present: (1) personal health information, (2), a trustee, (3) the personal health information is in the custody or control of the trustee. If HIPA is engaged, then my office is able to determine if privacy breaches have occurred under HIPA. A privacy breach occurs when personal health information has been collected, used, and/or disclosed without authority under HIPA.

[16] In my office's Review Report 177-2021 concerning the Ministry of Corrections, Policing and Public Safety I considered that information relating to an individual's vaccination and COVID-19 status qualifies as "personal health information", as defined by section 2(m)(i) of HIPA, which provides as follows:

> **2** In this Act:
>
> …
>
> (m) **"personal health information"** means, with respect to an individual, whether living or deceased:
>
> (i) information with respect to the physical and mental health of the individual;

[17] As this matter pertains to information relating to both Complainants' COVID-19 statuses, I am satisfied that personal health information is involved.

[18] Second, SHA qualifies as a "trustee" pursuant to section 2(t)(ii) of HIPA as follows:

> **2** In this Act:
>
> …
>
> (t) **"trustee"** means any of the following that have custody or control of personal health information:
>
> …
>
> (ii) the provincial health authority or a health care organization;

[19] There is a trustee, so now I will consider if the personal health information is in the custody or control of the SHA. In my office's Investigation Report 306-2019, I stated that "custody" is the physical possession of a record by a trustee with a measure of control. "Control" connotes authority, meaning the trustee has the authority to manage the records, including restricting access to it. Since the SHA was engaged in the practice of collecting personal health information in accordance with its policy regarding requests for an exemption, I am satisfied this personal health information was in its possession or control.

[20] I find, therefore, that HIPA is engaged and that I have jurisdiction to conduct this investigation.

2. Did SHA properly manage the privacy breach?

[21] The Complainants alleged that the SHA violated section 27(1) of HIPA. In this matter, an individual from within SHA's "Accommodations and Attendance Management" department shared the results of the Complainants' accommodation denial with their manager, who is also part of the SHA. This constitutes a use of that information, rather than a disclosure. "Use" is described at section 2(u) of HIPA as follows:

> **2** In this Act:
>
> …

> (u) "use" includes reference to or manipulation of personal health information by the trustee that has custody or control of the information, but does not include disclosure to another person or trustee.

[22] SHA admitted on its Privacy Breach Questionnaire that it improperly sent the Complainants' accommodation request denial letters to each of the Complainants' managers. That is, SHA does not deny that the "use" of the Complainants' accommodation denial was unauthorized. I find, therefore, the use was not authorized, and that a privacy breach occurred.

[23] As SHA does not dispute that a privacy breach occurred, I will move on to consider if it appropriately addressed the privacy breach. My office's *Rules of Procedure* outlines that my office will analyze whether the trustee properly managed the breach and took the following steps in responding to the privacy breach:

- Contained the breach (as soon as possible);
- Notified affected individuals (as soon as possible);
- Investigated the breach; and
- Prevented future breaches

[24] I will now analyze each of the four steps. I will make any necessary recommendations following my analysis.

Contained the breach (as soon as possible)

[25] SHA indicated it was able to contain the breach as follows:

> When it was reported to privacy I reached out to Accommodations and Attendance Management. They then stopped sending the emails until they could have the system programmed not to send to managers.

[26] Upon learning that a privacy breach has occurred, steps should be taken to immediately contain the breach. Depending on the nature of the breach, this can include:

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

(*Privacy Breach Guidelines*, p. 4)

[27] Effective and prompt containment may reduce the magnitude of a breach and, in some instances, the risks to individuals.

[28] Once SHA became aware of the breach from the Complainants, it immediately took steps to stop all notifications from uploading into "My Connection", which meant no letters were sent to employees or managers. Approximately a week later, SHA asked the Complainant's managers to delete the emails they had received in error.

[29] SHA's investigation later determined that accommodation denial letters had been erroneously sent to 59 managers, affecting 52 staff in total. Approximately three weeks after first discovering the breach, SHA asked the remaining managers to double delete the emails they had received in error (i.e., delete from both inbox and deleted items folder). While I find SHA took steps to contain the breach, it should have taken such steps sooner.

Notified affected individuals (as soon as possible)

[30] It is a best practice to inform affected individuals and my office of a privacy breach. The following is a list of individual organizations that may need to be notified as soon as possible after learning of the incident:

- The organization's privacy officer
- My office
- The police, if criminal activity is suspected

- The affected individual(s) (unless there are compelling reasons why this should not occur)

(*Privacy Breach Guidelines*, pp. 4 to 5)

[31] SHA described its notification efforts with the following:

> The Managers [SIC] the ones that received notification to delete the email they received.
>
> The breach was within the organization and it was decided that we could reach the Manager as they did not have a need to know and they check their emails every day. Staff do not check [SIC] emails on a regular basis[SIC] we agreed that contacting the managers was the best way to contain the breach.

[32] Providing notice to individuals affected by the breach should occur as soon as possible after key facts about the breach have been established. It is best to contact the affected individuals directly.

[33] While the Complainants notified SHA of the privacy breach, the SHA followed up with them by letters dated January 10, 2022. SHA's letter advised the Complainants of the steps it took to contain the breach, as well as the steps it was taking to prevent the breach from occurring again. SHA also offered an apology, as well as information regarding making a complaint with my office. These are all elements that a notice should contain.

[34] SHA, however, confirmed with my office that it did not notify the other 50 affected individuals whose denial letters were erroneously sent to each of their managers. While SHA provided proper notice to the Complainants, I find it did not provide notification to all affected individuals and should have done so.

Investigated the breach

[35] Investigating the privacy breach to identify root causes is key to understanding what happened. It is an important step in mitigating the risk of a future breach of a similar nature from occurring. Following are some key questions to ask during a privacy breach investigation:

- What and how did your organization learn of the privacy breach?
- What occurred?
- How did the privacy breach occur?
- What is the applicable legislation and what specific sections are engaged?
- What safeguards, policies, and procedures were in place at the time of the privacy breach?
- Was the duty to protect met?
- Who are the affected individuals?

(*Privacy Breach Guidelines*, pp. 6 to 7)

[36] To investigate a privacy breach is to determine the root cause, or why the privacy breach occurred.

[37] SHA explained its efforts to investigate the breach with the following:

> …first I took it to our privacy huddle on Nov 23, 2021 and discussed to see if anyone else had received any questions or email about this incident and no one had, but told me who to contact. Nov 23 email to the Director of Accommodations and Attendance Management with what has happened and a Privacy reporting form (PIR) for him to fill out. Nov 24 he returned the PIR form and [sic] what had happened…
>
> I was unaware that managers would receive copies of the auto notification from My Connection. After processing accommodation requests, results are entered into My Connection. This is to facilitate notifications required to identify employees who are not required to pay for participating in the SHA Monitored Testing Program (MTP). (The SHA will pay for Employees with approved accommodations to participate in the MTP.) Development of the Accommodation tile in My Connection happened at the same time as we developed our accommodation processes, which is a different process from how accommodations are typically received and processed. We have never used My connection for processing accommodations previous to the PoV process. Reviewing my notes during process development, I do not see any references regarding an employee's manager being sent a copy of the auto notification. I was informed by one of my team members on Monday, November 22, 2021 when she forwarded a copy of one of the notifications she was sent from a manager. As part of my investigation to determine how the manager obtained the information I followed up with the My Connection rep. The My Connection rep confirmed the notification was sent via My

> Connection. Also on Monday following more investigation, I advised that the notifications need to be stopped and the rep advised her team that these notifications are to be turned off.

[38] SHA's investigation determined that accommodation denial letters had been erroneously sent to 59 managers, affecting 52 staff in total. SHA determined that the root cause of the breach was a technological system failure of the "My Connection" software. It appears the development of the Accommodation tile in "My Connection" was new and the new system had not undergone enough testing to determine faults. For example, in this matter where the Complainants' managers were copied on their accommodation application results. SHA confirmed the breach with the software service provider and asked that notifications be turned off as soon as possible. As SHA was able to identify the root cause and address it, I find that it conducted an effective investigation of the privacy breach.

Prevented future breaches

[39] The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring. Essentially, this is what steps can be taken to prevent a similar privacy breach from occurring. To assist, some questions trustees can ask are:

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

(*Privacy Breach Guidelines*, p. 7)

[40] SHA described measures to prevent future breaches as follows:

> …Immediately after reading the incident report, in addition to the above, I advised my team to stop all uploads into My Connection until we receive notification the process in My Connection has been corrected. This will ensure no additional notifications are

> sent out to anyone (employee or manager). I then contacted the manager that had received the email and got them to delete the letter from their inbox and deleted folder. December 3, 2021 I sent email to employee to update them on what has been done (with the managers) Dec 14, 2021 talked with the Director and decided on a plan to send one email to all to delete the email they received. Dec 17, 2021 the list of managers was able to be generated. Dec 20, 2021 I sent the draft of the email to be sent out to the Director and Claims Manager and RTW who is covering for the Director at this time. Dec 22, 2021 the letters were sent out to the managers to delete the emails. January 10, 2022 sent letter to the staff member.

[41] SHA indicated to my office that the breach was caused by a technological error. SHA took steps to correct the error soon after it had been discovered. SHA took steps to stop email uploads until the My Connection system was fixed. The breach was caused by a system issue, and it is up to SHA's IT service provider to ensure that future breaches related to such system issues are prevented. SHA explained that the system issue in the My Connection software was corrected to ensure that no additional notifications are sent out. As a result, I find SHA has an adequate plan for preventing the same or similar privacy breaches from occurring in the future.

III FINDING

[42] I find that HIPA is engaged and that I have jurisdiction to conduct this investigation.

[43] I find that the use of the Complainants' accommodation denial information was not authorized, and that a privacy breach occurred.

[44] I find that SHA took steps to contain the privacy breach, but should have done so sooner.

[45] I find that while SHA provided adequate notice to the Complainants, it did not provide notice to all affected individuals and should have done so.

[46] I find that SHA conducted an effective investigation of the privacy breach.

[47] I find that SHA has an adequate plan for preventing the same or similar privacy breaches from occurring in the future.

IV RECOMMENDATION

[48] I recommend SHA notify the other 50 affected staff of the privacy breach within 30 days of the issuance of this Investigation Report.

Dated at Regina, in the Province of Saskatchewan, this 26th day of September, 2022.

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