



INVESTIGATION REPORT 157-2022

Saskatchewan Health Authority

January 23, 2023

Summary:

An employee at the Saskatchewan Health Authority (SHA) sent an email to their manager. Attached to the email was a note from the employee's physician indicating the employee required a medical leave. Then, upon an attendance white board within the employee's workplace, office administrative staff recorded that the employee was away due to a medical leave. The Commissioner found that privacy breaches occurred when the manager shared the Complainant's personal health information with office administrative staff and when the office administrative staff recorded the Complainant's personal health information on the attendance white board. The Commissioner made a number of recommendations, including that the SHA send a letter to the Complainant that recognizes the impact of the privacy and an apology.

I BACKGROUND

- [1] On June 6, 2022, an employee at the Saskatchewan Health Authority (SHA) sent an email to their manager. Attached to the email was a note from the employee's physician indicating the employee would require a medical leave.
- [2] Within the employee's workplace is an "attendance white board". Upon the attendance white board, it was noted that the employee was away due to medical leave.
- [3] In a letter dated July 1, 2022, the employee (Complainant) submitted a complaint to the SHA. Within the letter, the Complainant asserted that their manager had written that they were away due to medical leave, which was a privacy breach.

[4] In a letter dated September 9, 2022, the SHA responded to the Complainant. The SHA clarified that it was “office administrative staff” who filled in the attendance white board. The SHA informed the Complainant that it has created a work standard to prevent any personal information from being displayed.

[5] On September 13, 2022, the Complainant informed my office that they were not satisfied with the SHA’s response. They requested that my office undertake an investigation.

[6] On September 20, 2022, my office notified the SHA and the Complainant that my office would be undertaking an investigation.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[7] 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.

[8] First, the information at issue is information regarding the nature of the Complainant’s leave. Subsection 2(m) of HIPA defines “personal health information” 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 or mental health of the individual

[9] I find that personal health information is present.

[10] Second, subsection 2(t)(ii) of HIPA defines “trustee” 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;

[11] I find that the SHA qualifies as a trustee pursuant to subsection 2(t)(ii) of HIPA.

[12] Third, since the personal health information was recorded on an attendance white board at the SHA, I find that the SHA had custody or control of the personal health information.

[13] I find that I have jurisdiction to conduct this investigation.

2. Did a privacy breach occur?

[14] A privacy breach occurs when personal health information is collected, used or disclosed in a way that is not authorized by HIPA. Subsection 2(b) of HIPA defines “collect” as follows:

2(b) **“collect”** means to gather, obtain access to, acquire, receive or obtain personal health information from any source by any means;

[15] Subsection 2(u) of HIPA defines “use” as follows:

2(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.

[16] The term “disclosure” means the sharing of personal health information with a separate entity that is not a division or a branch of the trustee. Before disclosing personal health information, a trustee should ensure it has authority to do so under HIPA ([Investigation Report 081-2022](#) at paragraph [14]).

[17] The sharing of the Complainant’s personal health information with the office administrative staff and recording it on the attendance white board would qualify as a

“use”. Sections 23 and 26 of HIPA provides for the circumstances in which a trustee may use personal health information:

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.

...

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.

(3) Nothing in subsection (2) authorizes a trustee as an employer to use or obtain access to the personal health information of an individual who is an employee or prospective employee for any purpose related to the employment of the individual without the individual’s consent.

[18] Neither sections 23 nor 26 of HIPA authorized the manager to share the Complainant’s personal health information with office administrative staff. Nor did either provision authorize office administrative staff to record the Complainant’s personal health information on the attendance white board. Finally, neither provision authorized staff to

view the Complainant's personal health information. As a result, I find that privacy breaches occurred.

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

[19] When my office finds that a privacy breach has occurred, my office will analyze whether the trustee has properly managed the privacy breach in accordance with my office's [*Rules of Procedure*](#):

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

[20] The following is an analysis to determine if the SHA has followed these steps.

Contain the breach (as soon as possible)

[21] On learning that a privacy breach has occurred, a trustee should immediately take steps to contain the breach. Depending on the nature of the breach, this could include:

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

([*Privacy Breach Guidelines for Health Trustees*](#), August 2022, at p. 3)

[22] The SHA indicated that it contained the privacy breach by stopping the unauthorized practice of recording the reason for an employee's absence on the attendance white board.

It created a work standard where if an employee is absent, the word “Off” is written beside the absent employee’s name.

[23] I find that the SHA has made efforts to contain the privacy breach.

Notified affected individuals (as soon as possible)

[24] It is important to notify an affected individual about a privacy breach for several reasons. Affected individuals have a right to know and they need-to-know to protect themselves from any harm that may result. Unless there is a compelling reason not to, trustees should always notify affected individuals. A notification should include:

- A general description of what happened
- A detailed description of the personal health information involved
- A description of the types of harm that may occur
- Steps taken and planned to mitigate the harm and to prevent future breaches
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g., how to change a health services number)
- Contact information of an individual within the organization who can answer questions and provide information
- A notice that individuals have a right to complain to the IPC
- Recognition of the impacts of the breach on affected individuals and an apology

([*Privacy Breach Guidelines for Health Trustees*](#), August 2022 at p. 4)

[25] In this case, the SHA sent a letter dated September 9, 2022 to the affected individual (the Complainant). The letter contained a general description of what happened and that the SHA has created a work standard to prevent any “personal information” from being displayed on the attendance white board. The letter did not include other elements to make the letter an effective notice letter, including informing the Complainant of their right to complain to my office, recognition of the impacts the privacy breach had on the affected individual, or an apology.

[26] I find that SHA's notification of the privacy breach to the Complainant to not be adequate. I recommend that the SHA send another letter to the Complainant that recognizes the impact of the privacy breach and an apology.

[27] In my office's [Investigation Report 081-2022](#), I recommended that SHA include in its work standard for notifications to affected individuals the harms that may arise from a breach, the steps that can be taken to mitigate the risk of harm, and the SHA's plan to prevent future breaches. As of the writing of this Investigation Report, the SHA has not responded to my office's recommendation yet. I recommend that SHA comply with the recommendation in Investigation Report 081-2022. In addition, I recommend that SHA ensure its notices include all the requirements listed at paragraph [24].

Investigated the breach

[28] Once the breach has been contained and affected parties have been notified, the trustee should conduct an internal investigation. The investigation should address the incident on a systemic basis and should include a root cause analysis. At the conclusion of its investigation, the trustee should understand the cause of the breach which will inform how to prevent future breaches.

[29] The following are some key questions trustees should ask during a privacy breach investigation:

- When and how did your organization learn of the privacy breach?
- What occurred?
- How did the 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 for Health Trustees, p. 5)

[30] Earlier in this Investigation Report, I noted that privacy breaches occurred when 1) the manager shared the Complainant's personal health information with the office administrative staff, 2) when the office administrative staff recorded the Complainant's personal health information on the attendance white board, 3) when staff viewed the Complainant's personal health information on the white board.

[31] In its investigation of this privacy breach, the SHA admitted that the employee's personal health information was breached. In its submission to my office, the SHA said the "employee has the right to not have the reason for a leave shared without their consent, or with anyone that does not have a need-to-know".

[32] Based on the materials provided to my office, I note that a factor that contributed to the privacy breach was that there was no work standard stating who has a need-to-know the reason for an employee's absence and how to record an employee's absence on the attendance white board.

[33] I find that the SHA has investigated the privacy breach.

Prevented future breaches

[34] Prevention is one of the most important steps. Trustees cannot undo a privacy breach. However, they can learn from one and take steps to help ensure that it does not happen in the future. To avoid future breaches, a trustee should make a prevention plan.

[35] Section 16 of HIPA requires that trustees establish measures to maintain administrative, technical and physical safeguards. Section 16 of HIPA provides:

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.

[36] As already noted in this Investigation Report, the SHA created a work standard to prevent any personal information and/or personal health information from being displayed on the attendance white board. Based on a review of this work standard, I note it also requires that the manager keep the reason for an absence confidential and to use the reason for “payment coding purposes only”. Also, when an employee is absent, the attendance white board is to only note that the employee is “OFF”.

[37] I find that the SHA has taken appropriate steps to prevent similar privacy breaches in the future.

III FINDINGS

[38] I find that I have jurisdiction to conduct this investigation.

[39] I find that privacy breaches occurred when the manager shared the Complainant’s personal health information with office administrative staff, when the office administrative staff recorded the Complainant’s personal health information on the attendance white board, and when staff viewed the Complainant’s personal health information on the white board.

[40] I find that the SHA has made efforts to contain the privacy breach.

[41] I find that SHA's notification of the privacy breach to the Complainant to not be adequate.

[42] I find that the SHA has investigated the privacy breach.

[43] I find that the SHA has taken appropriate steps to prevent similar privacy breaches in the future.

IV RECOMMENDATIONS

[44] I recommend that the SHA send another letter to the Complainant that recognizes the impact of the privacy breach and offers an apology.

[45] I recommend that the SHA comply with the recommendation in Investigation Report 081-2022. In addition, I recommend that SHA ensure its notices include all the requirements listed at paragraph [24].

Dated at Regina, in the Province of Saskatchewan, this 23rd day of January, 2023.

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