Office of the
Saskatchewan Information
and Privacy Commissioner

# INVESTIGATION REPORT 081-2022

## Saskatchewan Health Authority

**October 7, 2022**

**Summary:** The Saskatchewan Health Authority (SHA) reported a privacy breach to the Commissioner involving a misdirected fax. The fax was sent to a heating and plumbing business by one of SHA's staff when it should have been sent to a physician. The fax included the personal health information of 767 patients. The Commissioner investigated the breach. He found that the breach occurred when an SHA employee entered an incorrect fax number in SHA's electronic medical record system. The Commissioner found that SHA's notice to affected patients and investigation was not adequate. He also found that SHA did not take adequate steps to prevent further breaches. The Commissioner recommended SHA amend its notifications to affected parties, privacy training program and require SHA staff to complete the privacy training annually. He also recommended SHA provide his office with the terms of reference of its working group on misdirected faxes and a monthly update of the group's progress.

## I BACKGROUND

[1] On April 4, 2022, an employee of the Saskatchewan Health Authority (SHA) sent a fax to a heating and plumbing business. The fax contained information of 767 surgical patients and should have been sent to a physician's office.

[2] On April 5, 2022, the heating and plumbing business notified SHA that it had received the fax. SHA's staff immediately retrieved the fax from the business.

[3] SHA's Privacy Office advised my office of the incident on May 2, 2022. It also provided my office with a Privacy Breach Investigation Report and a template of the letter it sent to the 767 affected individuals notifying them of the breach.

[4] On May 5, 2022, my office advised SHA that we would be investigating the breach pursuant to subsection 52(d) of *The Health Information Protection Act* (HIPA). My office requested that SHA complete the *Privacy Breach Investigation Questionnaire*.

[5] SHA subsequently asked my office to treat its Privacy Breach Investigation Report as its response.

## II DISCUSSION OF THE ISSUES

### 1. Do I have jurisdiction?

[6] 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.

[7] The fax contained information about surgical patients. It included their names, surgical waitlist status and other information about their surgical procedures. This is personal health information as defined in subsection 2(m) of HIPA which provides:

> **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;
>
> (ii) information with respect to any health service provided to the individual;
>
> …
> (v) registration information;

[8] The fax also contained the health services number for the patients. I find that this qualifies as registration information in subsection 2(m)(v) of HIPA. Registration information is defined in subsection 2(q) of HIPA which states:

> **2**(q) "registration information" means information about an individual that is collected for the purpose of registering the individual for the provision of health services, and includes the individual's health services number and any other number assigned to the individual as part of a system of unique identifying numbers that is prescribed in the regulations;

[9] Following previous reports of my office, such as Investigation Report 351-2019, I find that the Complainant's health services number is their personal health information.

[10] SHA is a "trustee" pursuant to subsection 2(t)(ii) of HIPA, which provides:

> **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] The fax originated from the surgical patient information management department of SHA. Therefore, I find that SHA had custody or control of the personal health information.

[12] As all three elements for the application of HIPA are present, I find that I have jurisdiction to investigate this matter.

## 2. Did a privacy breach occur?

[13] A privacy breach occurs when personal health information is collected, used or disclosed in a way that is not authorized by HIPA.

[14] 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.

[15] In this case, SHA sent one fax containing personal health information of 767 patients to the wrong fax number. The fax was received by an individual at the heating and plumbing business and not the physician it was intended for. SHA acknowledged that this was an unauthorized disclosure. Therefore, I find that a privacy breach occurred.

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

[16] When a trustee reports a privacy breach to my office, my office determines whether the trustee appropriately responded to the breach. As set out in my office's *Rules of Procedure*, we will analyze whether the trustee appropriately managed the breach. We will also consider if the trustee:

- Contained the breach (as soon as possible)
- Notified affected individuals (as soon as possible)
- Investigated the breach
- Took appropriate steps to prevent future breaches.

[17] I now turn to consider if SHA followed these steps.

### *Contained the breach (as soon as possible)*

[18] 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 can 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)

[19] Trustees can reduce the impact of the breach by effectively and promptly containing it.

[20] When it received notice of the misdirected fax, SHA contained the breach by physically retrieving it the same day. I commend SHA for taking this step. SHA also obtained confirmation from the recipient that they had not shared the fax with anyone else.

[21] I find that SHA took appropriate and timely steps to contain the breach.

***Notified affected individuals (as soon as possible)***

[22] 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)

[23] Trustees may also want to notify other organizations, such as, my office, law enforcement or other regulatory bodies that oversee professions.

[24] In this case, SHA notified affected individuals by mail during the week of May 2, 2022. It provided my office with the template used for the notification letters.

[25] The template informed the affected individuals that their records were faxed to the heating and plumbing business in error. It described the type of information in the records. It included an apology and indicated that SHA is investigating the root cause of the breach. The letter also provided the affected individuals the contact information for my office so that if they were not satisfied with SHA's response to the breach, they can file a complaint.

[26] The template does not include a description of the types of harm that may result from the privacy breach. This is particularly important here as the health services number was involved. Nor does it include any information about actions taken by SHA to mitigate the harm and prevent future breaches. Finally, the notification does not provide information about how the affected individuals could change their health services number.

[27] SHA should ensure it is including this type of information in its notification letters as a standard practice. It not only assists affected individuals, but it ensures SHA is considering the risks and impacts of all breaches.

[28] As a result of the above, I find that SHA's notification to the affected parties was not adequate.

[29] In response to my office's Investigation Report 032-2022, SHA stated that it is developing a work standard for patient notification. The work standard will set out how SHA provides verbal and/or written notification to a patient affected by a privacy breach.

[30] I note that the work standard had not been completed as of the date of my office's Investigation Report 080-2022, which also involved a misdirected fax sent by SHA. In that report, I made some recommendations regarding the contents of the work standard which are also appropriate in this review. Therefore, I will repeat those recommendations here.

[31] I recommend that SHA's work standard on patient notification include requirements to set out the harms that may arise from a breach, the steps that can be taken to mitigate the risk of harm, and SHA's plan to prevent further breaches of this kind. I recommend that SHA provide my office with a copy of the work standard within 30 days of issuance of this report.

***Investigated the breach***

[32] 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.

[33] 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)

[34] SHA commenced its investigation into this incident on April 5, 2022. In its Privacy Breach Investigation Report, it described its investigation as follows:

> The breach was reported by an employee of a local Plumbing and Heating business and was the result of an [SHA] employee not following the Surgeon Waitlist Monthly Notification Work Standard in place when faxing records that contain personal information and personal health information. The first step in the investigation was to contain the breach, in which, the SHA physically retrieved the breached records from the local business. The employee of the business identified that she was the only individual to see the records. The breach involved 767 patient's information including their inpatient/outpatient, priority and waitlist status, name, health services number, procedure length, procedure name, comments and site. Following the retrieval of the breached records, the Manager of Surgical Patient Information Management was contacted.

[35] SHA asserted that the breach was caused by the failure of its employee to select the fax number from a pre-programmed list in the fax machine. The employee entered the fax number manually and entered the wrong fax number. The requirement to use pre-programmed numbers is set out in the Surgeon Waitlist Monthly Notification Work Standard. It states:

> The Scheduler faxes the worksheet to the appropriate surgeon's office. The Scheduler can only use preprogrammed fax numbers when faxing documents that contain Personal Health Information or Personal Information.

[36] Therefore, I find that the breach was caused in part by a failure of SHA's employee to follow the applicable policy.

[37] Other factors may have contributed to the breach. I note that SHA's summary of its investigation did not include any information about the privacy training offered to its staff. When questioned by my office, SHA stated that mandatory privacy training is completed by all SHA staff every three years. It added that the privacy training does not include any discussion about the risks arising from misdirected faxes, emails or other communications.

It also stated that a bulletin regarding the risks of faxing personal health information was sent to staff on two occasions in 2022.

[38] I stated in my office's Investigation Report 045-2021, et al errors will not cease once traditional fax machines are replaced with electronic systems. Breaches can also arise when staff make errors in email and mailing addresses. Therefore, SHA must take steps to ensure that its staff are fully aware of the privacy risks and are trained to be careful when transmitting personal health information. Training and awareness raising initiatives are necessary to reduce the risk of all privacy breaches. They are important administrative controls that should be in place to protect the confidentiality of personal health information and should be considered by SHA in its breach investigations. I will address this below.

[39] Based on the information provided, I find that SHA's investigation of the breach correctly identified that the breach was a result of the failure of its employee to follow applicable policy. However, I find that its investigation into the breach was not adequate because it failed to consider the shortcomings of its privacy training program.

***Took appropriate steps to prevent future breaches***

[40] 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.

[41] The prevention plan should consider the trustees' obligations to establish measures to maintain administrative, technical and physical safeguards of personal health information. This requirement is set out in section 16 of HIPA which 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.

[42] SHA asserted that following the breach, the department manager reviewed the applicable work standard with their staff. They also specifically discussed the requirement to use the pre-programmed fax numbers.

[43] Previous reports of my office involving SHA and misdirected faxes have identified the importance of privacy training. For example, in my office's Investigation Report 043-2018, which involved a misdirected fax, my office recommended that SHA develop a policy on annual mandatory privacy training for all employees. Adequate privacy training is an important administrative control and is necessary to ensure compliance with section 16 of HIPA.

[44] SHA advised that the surgical patient information management group received their first privacy training in 2018 and it is refreshed every three years. Therefore, the current privacy training program does not comply with the recommendation made in my office's Investigation Report 043-2018. SHA also stated that the privacy training does not include any information about the risks of using fax systems to transmit personal health information. I recommend that SHA provide mandatory annual privacy training to all staff who handle personal health information. I also recommend that SHA amend its privacy training program to include information about the risks of using a fax to transmit personal health information.

[45] SHA's Privacy Office made three recommendations to address this breach. It recommended:

> Manager Surgical Patient Information Management should determine if the physicians receiving the Surgical Waitlist Monthly Report have SHA email accounts.

> If the physicians have SHA email accounts, a Work Standard should be developed on emailing personal information and personal health information to them.
>
> When sending large amounts of personal health information, Surgical Patient Information Management team should use password protected documents.

[46] In response to questions posed by my office, SHA stated that the department responsible for the breach:

> …**has not accepted the recommendations** however the area only discloses the Surgical Waitlist report upon request. The area is moving toward utilizing an eHealth Reporting Platform in order to eliminate the need to fax reports similar to that involved in this incident.
>
> [Emphasis added]

[47] For over 10 years, my office has highlighted the problem with SHA's use of fax systems to send personal health information and the need to take steps to address the privacy risks. In my office's Investigation Report 032-2022, I reviewed my office's experience with breaches involving misdirected faxes that goes back to a report on the subject written in 2010, *Report on Systemic Issues with Faxing Personal Health Information*. Since January 1, 2022, my office has opened six breach investigation files involving SHA's use of a fax. This is an extraordinary number.

[48] To date, it appears that SHA has taken a piecemeal or case by case approach to addressing the risks. For example, SHA's Privacy Breach Investigation Report does not address recommendations made by my office in previous reports involving similar breaches. Nor does it provide me with any information about steps being taken to address this issue on a systemic basis. This raises the question of whether there is a coordinated effort in place to address the privacy risks of misdirected faxes within SHA. This is concerning.

[49] I recommended in my office's Investigation Report 080-2022 that SHA provide us with the terms of reference of its working group on misdirected faxes and monthly updates on its progress. I will repeat that recommendation here.

[50] As I said in that report, through its monthly updates SHA will have an opportunity to demonstrate accountability and transparency in relation to its plan to prevent these types of breaches. This will also help build public trust in SHA's ability to protect personal health information.

[51] Based on the information provided to date, I am not satisfied that SHA's plan to prevent further breaches arising from misdirected faxes is adequate.

## III FINDINGS

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

[53] I find that a privacy breach occurred.

[54] I find that SHA took appropriate and timely steps to contain the privacy breach.

[55] I find that SHA's notification to the affected parties was not adequate.

[56] I find that SHA's investigation of the breach was not adequate.

[57] I find that SHA's plan to prevent further breaches arising from misdirected faxes is not adequate.

## IV RECOMMENDATIONS

[58] I recommend that SHA's work standard on patient notification include requirements to set out the harms that may arise from a breach, the steps that can be taken to mitigate the risk of harm, and SHA's plan to prevent further breaches of this kind.

[59] I recommended that SHA provide my office with a copy of the work standard on patient notification within 30 days of issuance of this Report.

[60] I recommend that SHA provide mandatory annual privacy training to all staff who handle personal health information.

[61] I recommend that SHA amend its privacy training program to include information about the risks of using fax to transmit personal health information.

[62] I recommend that SHA provide my office with the terms of reference of its working group on misdirected faxes and monthly updates on the efforts made by the group. The terms of reference and the first monthly update should be provided to my office within 30 days of the release of this Report.

Dated at Regina, in the Province of Saskatchewan, this 7th day of October, 2022.

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