Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 005-2018

Saskatchewan Health Authority

September 4, 2018

Summary: The Saskatchewan Health Authority (SHA) proactively reported a privacy breach to the Office of the Information and Privacy Commissioner (OIPC). According to the SHA, a fax containing the personal health information of one individual was faxed to Kelly's Computer Works instead of Dr. Rodriguez's Medical Office. The Commissioner found that the SHA appropriately handled the privacy breach in accordance with the five best practice steps. The Commissioner recommended the SHA implement its plan to eliminate faxing of personal health information within the health system within the next six to 12 months.

I BACKGROUND

[1] On January 12, 2018, the Saskatchewan Health Authority (SHA) contacted my office to proactively report a breach of privacy. The SHA advised that a fax containing personal health information that was intended for Dr. Rodriguez's office in Battleford was received by a private business, Kelly's Computer Works, in North Battleford. The incident occurred on January 9, 2018.

[2] The SHA advised my office that it learned of the breach when a reporter from the CBC contacted representatives from the SHA. The owner of Kelly's Computer Works had contacted the CBC to inform them that it had received personal health information via fax. A CBC article about the incident appeared on January 10, 2018.

[3] On January 16, 2018, my office notified the SHA that it would be monitoring the matter and requested a copy of SHA's internal investigation report and copies of written policies

and/or procedures. On February 7, 2018, my office received an internal investigation report from the SHA.

II DISCUSSION OF THE ISSUES

1. Does the Commissioner have jurisdiction?

[4] The SHA is a "trustee" pursuant to subsection 2(t)(ii) of *The Health Information Protection Act* (HIPA). Thus, I have jurisdiction to conduct this investigation.

2. Is HIPA engaged?

[5] HIPA is engaged when three elements are present: (1) a trustee, (2) personal health information is involved, and (3) the trustee has custody or control over the personal health information.

[6] First, in order for there to be a trustee, the organization must fall within one of the enumerated clauses in subsection 2(t) of HIPA. The misdirected fax originated from the Parkland Integrated Health Centre in Shellbrook (Shellbrook Hospital). The Shellbrook Hospital is part of the SHA. The SHA is a trustee under HIPA pursuant to subsection 2(t)(ii). Therefore, I find that the first element is present.

[7] Second, in order for there to be personal health information involved, at least some of the information in the misdirected fax must fall within the definition of personal health information in subsection 2(m) of HIPA. Subsection 2(m) of HIPA 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;

(iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;

(iv) information that is collected:

(A) in the course of providing health services to the individual; or

(B) incidentally to the provision of health services to the individual; or

(v) registration information;

[8] The misdirected fax included the fax cover sheet and a 21 page medical report about a specific patient. The SHA only provided my office with a copy of the fax cover sheet. It did not provide a copy of the 21 page medical report. It also did not detail what personal health information was breached in its internal investigation report. However, on the day of the breach, January 9, 2018, Kelly's Computer Works contacted the Commissioner about the breach and provided him with a full copy of what it received. The information included (but was not limited to):

- the patient's name;
- health services number;
- date of birth;
- health diagnosis;
- blood work results;
- discharge plans;
- medications prescribed;
- the results of a sexually transmitted disease test;
- urine analysis results;
- allergies;
- physical symptoms displayed; and
- PAP smear results.

[9] This information would qualify as the personal health information of the patient pursuant to subsections 2(m)(i), (ii), (iii), (iv) and (v) of HIPA. Therefore, I find that the second element is also present.

[10] Finally, in order for the third element to be present, the trustee must have custody or control of the personal health information. *Custody* is defined as the physical possession of a record by a trustee. As the fax originated from the SHA, I find that the SHA had custody of the personal health information. It is only necessary to find that there was either custody or control. Both are not necessary to engage HIPA. Therefore, as I have found the SHA had custody, the third element is also present.

[11] In conclusion, I find that HIPA and the rules around the protection of personal health information in Parts III and IV of HIPA are engaged in this matter.

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

[12] In circumstances where a trustee proactively reports a privacy breach, the focus for my office becomes one of determining whether the trustee appropriately handled the privacy breach. In order to be satisfied, my office would need to be confident that the SHA took the privacy breach seriously and appropriately addressed it. I recommend five best practice steps be taken when a trustee discovers a breach of privacy has occurred. These are:

1. Contain the breach;
2. Notify affected individuals and/or appropriate organizations;
3. Investigate the breach;
4. Plan for prevention; and
5. Write an investigation report.

[13] I will now consider the appropriateness of the SHA's handling of the matter against these five best practice steps.

Step 1: Contain the breach

[14] Upon 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 privileges; or
- Correcting weaknesses in physical security.

[15] Effective and prompt containment reduces the magnitude of a breach and the risks involved with personal health information being inappropriately disclosed.

[16] In its internal investigation report, the SHA advised that Kelly's Computer Works had indicated that the misdirected fax was deleted and unread. It did not indicate when this occurred so my office followed up requesting this information. The SHA advised that it spoke to Kelly's Computer Works on January 10, 2018 and the owner confirmed that he deleted the fax.

[17] It appears the breach was appropriately contained in a timely manner.

Step 2: Notify affected individuals and/or appropriate organizations

[18] Notifying an individual that their personal health information was inappropriately accessed is important for a number of reasons. Not only do individuals have a right to know, they need to know in order to protect themselves from any potential harm that may result from the inappropriate access. Unless there is a compelling reason not to, public bodies should always notify affected individuals. An effective notification should include:

- A description of what happened;
- A detailed description of the personal health information that was involved;

- A description of possible types of harm that may come to them as a result of the privacy breach;
- Steps that the individuals can take to mitigate harm;
- Steps the organization is taking to prevent similar privacy breaches in the future;
- The contact information of an individual within the organization who can answer questions and provide further information;
- A notice that individuals have a right to complain to the Office of the Information and Privacy Commissioner; and
- Recognition of the impacts of the breach on affected individuals and an apology.

[19] In addition to notifying individuals, trustees may want to notify other organizations, for example, my office, law enforcement or other regulatory bodies that oversee particular professions.

[20] The SHA indicated that, after attempting to reach the patient by telephone several times without success, the SHA sent the patient a letter to the address it had on file, asking the patient to contact the SHA Privacy Officer. The letter also indicated the SHA had an issue to discuss regarding the privacy of the patient's personal health information. The patient did not call the Privacy Officer back.

[21] The SHA did not provide the dates for the telephone calls it made to the patient or a copy of the letter it sent to the patient. My office requested this information from the SHA. The SHA advised that it attempted to call the patient on January 18, 19, 22 and 25, 2018. There was no ability to leave a telephone message for the patient. The SHA also provided a copy of the letter it sent to the patient which stated in part:

> …
>
> I have been attempting to contact you by telephone to advise you of a matter regarding the privacy of your health information. Could you please call me at your earliest convenience at [telephone number]…

[22] The SHA also explained the rationale for not sending a breach notification letter to the patient. The SHA was concerned that if the first letter did not make it to the patient or was opened by someone else, a second letter could further breach the patient's privacy.

[23] The SHA also notified my office of the privacy breach on January 12, 2018.

[24] I am satisfied with the attempts taken by the SHA to notify the affected patient.

Step 3: Investigate the breach

[25] Once the breach has been contained and appropriate notification has occurred, the trustee should conduct an internal investigation. The trustee's Privacy Officer generally conducts the investigation because they have the appropriate privacy expertise to do so and understand what the relevant privacy legislation requires of their organization. The investigation should address the incident on a systemic basis and should include a root cause analysis. The investigation should be documented in an internal privacy breach investigation report. At the conclusion of its investigation, the trustee should have a solid grasp on what occurred.

[26] The SHA provided an internal investigation report. It was approximately one page long and lacked details regarding what personal health information was breached, dates of when events occurred and prevention steps that would be taken. My office discussed this with the SHA and it advised a new form was being used for the report but it was willing to provide the information in its old format, which provided more detail. Additional information was received from the SHA on August 1, 8 and 9, 2018.

[27] The SHA was able to determine the breach was caused by human error. A Medical Office Assistant entered the fax number into the fax machine incorrectly. The fax number was taken from a fax cover sheet with Dr. Rodriguez's contact information on it. According to the SHA, the fax number was small and the Medical Office Assistant mistook the "6" for a "5" in the fax number.

[28] However, the owner of Kelly's Computer Works provided my office with the misdirected fax. The fax cover sheet shows the opposite. The correct digit is a "5" but was mistakenly typed in as a "6". The fax numbers for the two organizations are very similar:

Dr. Rodriguez:	306-445-3131
Kelly's Computer Works:	306-446-3131

[29] The error is clearly due to human error and the misreading of the fax number. The investigation appears to have successfully determined what happened and why. Therefore, I am satisfied with the investigation that was conducted.

Step 4: Plan for prevention

[30] Prevention is perhaps one of the most important steps. A privacy breach cannot be undone but a trustee can learn from one and improve its practices. To avoid future breaches, a trustee should formulate a prevention plan. Some changes that are needed may have revealed themselves during the investigation phase. For example, deficient policies or procedures, a weakness in the system, a lack of accountability measures or a lack of training.

[31] The SHA listed three preventative measures or long-term strategies to correct the situation:

1. A letter was sent to Dr. Rodriguez's office on March 15, 2018 requesting it change its letterhead/fax cover sheet so the telephone and fax numbers are clearer. Dr. Rodriguez's office made this change.

   A sample of the change was provided to my office and the telephone and fax numbers are much clearer.

2. The SHA was working on a project to eliminate faxing of personal health information within the health system. The plan has been developed and options have been proposed to the Ministry of Health. The timeline for implementation has not been established.

3. The SHA was currently working on a plan to provide annual privacy education to all employees. Testing for the project would begin in the fall of 2018.

[32] Misdirected faxes containing personal health information is a recurring issue. In particular, misdirected faxes to Kelly's Computer Works. This is the third privacy breach of this nature addressed by my office. On January 19, 2017, Kelly's Computer Works contacted my office because it had received a misdirected fax. A Medical Office Assistant from the Royal University Hospital in Saskatoon sent a fax intended for Dr. Rodriguez's office to Kelly's Computer Works. Again, the fax number was entered incorrectly. It appeared a "6" was used instead of a "5" in the fax number. During the investigation, it was learned from Kelly's Computer Works that it received misdirected faxes on average every two weeks to a month and the issue had been going on for the past 18 months to two years. My office opened a file, conducted a preliminary investigation and resolved the matter informally.

[33] The issue came to my office's attention again on September 7, 2017. Kelly's Computer Works contacted my office advising it had received another misdirected fax. After investigating the breach, I issued Investigation Report 223-2017. The cause of the breach was a Medical Office Assistant from St. Paul's Hospital in Saskatoon incorrectly entering the fax number. The fax number was pulled from the same fax cover sheet for Dr. Rodriguez's Office used in the current investigation. Again, it appeared a "6" was used instead of a "5" in the fax number.

[34] During the current investigation, my office contacted Kelly's Computer Works to see how frequently the company was still receiving misdirected faxes containing personal health information. Kelly's Computer Works advised my office on August 9, 2018, that approximately three to four more misdirected faxes containing personal health information have been received since the opening of this file.

[35] The broader issue of misdirected faxes has also been previously dealt with by this office. In Investigation Report H-2014-001, 10 trustee organizations were responsible for misdirected faxes affecting 1000 different patients. In November 2010, former Commissioner, Gary Dickson Q.C., issued a special report titled, *Report on Systemic Issues with Faxing Personal Health Information*. The special report involved 60 faxes sent by 31 different trustee organizations that the then intended recipient did not receive.

[36] Effective December 4, 2017, the 12 health regions in Saskatchewan dissolved to form one provincial body called the SHA. Previously, breaches resulting from misdirected faxes were being handled by individual health regions. However, they can now be addressed provincially and hopefully end the ongoing breaches of patient privacy. Kelly's Computer Works advised my office that it has a direct contact now at the SHA where it can forward the misdirected faxes. As well, it advised that Kelly's Computer Works will be "assisting [the SHA] in some way to completely eliminate faxing from the Health Industry in Saskatchewan".

[37] The preventative measures proposed by the SHA appropriately flow from what was found to be contributing factors during its investigation. Further, I recommended in Investigation Report 223-2017, that the SHA adopt a policy of mandatory annual privacy training for all employees. I am pleased the SHA has put this recommendation into action. Eliminating the faxing of personal health information is also an excellent response. I would like to see this preventive measure implemented within the next six to 12 months.

[38] In conclusion, I am satisfied with the preventative steps taken by the SHA.

IV FINDING

[39] I am satisfied with how the SHA addressed this privacy breach.

V RECOMMENDATION

[40] I recommend that the SHA implement its plan to eliminate faxing of personal health information within the health system within the next six to 12 months.

Dated at Regina, in the Province of Saskatchewan, this 4th day of September 2018.

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