Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 223-2017

Saskatoon Regional Health Authority

October 10, 2017

Summary: The Information and Privacy Commissioner (IPC) initiated a privacy breach investigation with the Saskatoon Regional Health Authority (SRHA) after receiving notification of a misdirected fax that contained personal health information. The IPC recommended SRHA issue a new letter to the affected individual and follow its internal policy and procedure regarding faxing personal health information.

I BACKGROUND

[1] On September 7, 2017, my office was notified by Kelly's Computer Works in North Battleford, Saskatchewan that it had received a fax that was not intended for them.

[2] A review of the fax cover sheet indicated that the fax originated from the Saskatoon Regional Health Authority (SRHA), Non-Invasive Cardiology, St. Paul's Hospital in Saskatoon, Saskatchewan and was addressed to a Dr. Rodriquez. The fax contained one patient's exercise tolerance test results.

[3] My office contacted SRHA to notify it of the breach of privacy incident and provided notification that my office would be undertaking an investigation.

[4] On September 18, 2017, my office received SRHA's internal privacy breach investigation report as well as a policy and procedure relating to SRHA's faxing practices.

II DISCUSSION OF THE ISSUES

1. Is *The Health Information Protection Act* (HIPA) engaged?

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

[6] First, the errant fax originated from the Non-Invasive Cardiology Unit at St. Paul's Hospital. St. Paul's Hospital is part of SRHA which is a "trustee" pursuant to subsection 2(t)(ii) of HIPA. I find the first requirement is met.

[7] 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;
>
> (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 contained the patient's name, medical record number, provincial health card number, date of birth, age, gender, type of medication the patient was taking,

results of the cardiac test, conclusion of the test and recommendation for an additional cardiac test for the patient. Based on a review of this information, I find that personal health information is involved.

[9] In the IPC Guide to HIPA, custody is defined as "the physical possession of a record by a trustee". As the fax originated from SRHA, I find that SRHA has custody of the record and therefore HIPA is engaged.

2. Did SRHA respond appropriately to the privacy breach?

[10] The IPC Guide to HIPA includes Privacy Breach Guidelines that are specifically geared to trustees. Appendix C in the resource recommends the following five steps for responding to a breach of privacy:

- Contain the breach,
- Notification,
- Investigate the breach,
- Prevent future breaches, and
- Privacy breach report.

[11] I will consider each of these steps to determine if SRHA adequately responded to the privacy breach.

Contain the breach

[12] The first step in responding to a privacy breach is containing the breach, which means to stop the unauthorized practice when the trustee learns of it.

[13] My office was notified by Kelly's Computer Works that it had received a fax that was not intended for them. After receiving a copy of the misdirected fax, my office requested that all copies of the fax be deleted and was provided confirmation that it had done so.

[14] In its internal investigation report, SRHA advised that it had also contacted the Manager of Kelly's Computer Works and confirmed that all copies of the fax had been deleted.

[15] I find that SRHA has adequately contained the breach.

Notification

[16] In the IPC Guide to HIPA, it is recommended that the notification contain the following elements:

- A description of the breach (a general description of what happened).
- A detailed description of the personal health information involved (e.g. name, medical records, etc.).
- Steps taken and planned to mitigate the harm and to prevent future breaches.
- If necessary, advise on actions the individuals 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 your organization who can answer questions and provide further information.
- A notice that individuals have a right to complain to the IPC. Provide contact information.
- Recognition of the impacts of the breach on affected individuals and an apology.

[17] On September 14, 2017, SRHA notified the affected individual, by letter, that a fax containing his exercise tolerance test results intended for Dr. Arstides Rodriquez Naranjo was incorrectly faxed to Kelly's Computer Works. While the letter indicated it contained his exercise tolerance test results, it did not contain the elements of personal health information involved.

[18] The letter from SRHA also included contact information for a representative at SRHA and the contact information for my office, should the individual have any further concerns.

[19] When providing individuals with notification of a privacy breach, it is recommended that SRHA provide the elements of personal health information in the notification.

[20] My office provided SRHA with a draft of this report. After reviewing it, SRHA advised it intended to issue a revised letter to the affected individual providing the elements of personal health information involved in this incident.

Investigate the Breach

[21] SRHA advised my office that the Medical Office Assistant (MOA) in the Non-Invasive Cardiology department had inadvertently sent the fax to the incorrect fax number. The MOA is the only individual responsible for sending faxes from this department. The fax number was manually entered into the fax machine based on the number recorded on the fax cover sheet. The MOA had recorded one digit of the fax number incorrectly which resulted in this fax being sent to the computer company rather than the doctor's office.

[22] This is not the first instance in which the Non-Invasive Cardiology Department at St. Paul's Hospital inadvertently sent a fax to Kelly's Computer Works intended for Dr. Rodriguez. In January 2017, my office was notified by Kelly's Computer Works of a misdirected fax it had received. Our office opened a file with SRHA and after a preliminary investigation the matter was resolved informally and no report was issued.

[23] While it was not the same individual that held the position of MOA for this department in both instances, both individuals inadvertently recorded the fax number incorrectly.

[24] My office asked SRHA to confirm that the source where the MOA recorded the fax number for Dr. Rodriguez was accurate. SRHA advised it had reviewed this and found the fax number to be accurate.

[25] SRHA also provided my office with its internal policy and procedure regarding faxing. In reviewing these documents, it was found SRHA had the following process for faxing sensitive information:

If the information is highly sensitive in nature:

- Notify the recipient by telephone that confidential/personal health information is being transmitted.
- Ask the receiver to stand by the fax machine to receive the information.
- Ask the receiver for confirmation of receipt of the information.

[26] My office asked SRHA if the MOA followed this process when faxing the personal health information involved in this incident. SRHA advised this process was not followed and is generally not followed when sending faxes to doctor's offices. It indicated this would be an onerous task due to the number of faxes sent by SRHA on a daily basis. SRHA indicated this process was more commonly used when sending faxes to third parties, such as insurance companies.

[27] My office asked SRHA to provide details regarding the average number of faxes sent from the department to determine how onerous the task this would be. SRHA advised that, on average, the Non-Invasive Cardiology department sent 20 faxes daily. It also indicated it did not have any fax numbers pre-programed as recipients varied depending on the patient's referring physician. SRHA also indicated that the faxes are sometimes forwarded to specialists as well. SRHA advised 75% of faxes sent from this department were to referring physicians with the other 25% to varying specialists.

[28] To support its position that this process not be used when dealing with a high volume of faxes, SRHA pointed my office to the following statement found in SRHA's internal faxing policy immediately following the faxing process:

> **NOTE:** The above is **not applicable** to areas that send a high volume of faxes to an external agency/office on a regular/recurring basis **or;** use pre-programmed features **and** regularly update/verify pre-programmed features as required.

[29] SRHA has indicated this department does not have any pre-programmed numbers in the fax machine; therefore, the second part of this statement does not apply to this situation. Based on my interpretation of the first part of this statement, the faxing procedure would only be applicable if the high volumes of faxes are sent to ***an*** office or agency on a regular basis.

[30] However, SRHA has indicated the faxes are not sent to any particular office or agency on a regular basis, which is why no numbers are pre-programmed into the fax machine. Therefore, I find SRHA's faxing practices do not follow their internal faxing policy and procedure.

[31] I recommend SRHA ensure their faxing practices follow their internal faxing policy and procedure.

[32] After reviewing the draft investigation report, SRHA advised Non-Invasive Cardiology would be acting on this recommendation for a one month period. Depending on the impact on the department, SRHA hopes this change in practice will become permanent for this department.

Prevent future breaches

[33] SRHA advised that after receiving notification of the incident, it had reviewed its policies and procedures with the MOA and stressed the importance of accuracy when faxing personal health information. However, SRHA indicated in its internal investigation report that no additional safeguards were developed in response to this breach of privacy as it was caused by human error. However, as noted earlier in this report, my office had worked with SRHA on a file earlier this year that dealt with the very same circumstances.

[34] As this issue appears to be a reoccurring issue, my office asked SRHA to explore options to block outgoing fax numbers from either the fax machine or through its telecommunication service provider. My hope was for SRHA to find a way to block the computer company's fax number to prevent personal health information from being incorrectly faxed to that number.

[35] SRHA was willing to explore these options but unfortunately it found that neither the fax machine nor the telecommunication service provider had the ability to block outgoing fax numbers.

[36] My office asked if the MOA had received privacy training, and if so when it last occurred. SRHA advised the MOA received privacy training during new employee orientation four years ago. Based on discussions with SRHA, it was not clear how often employees receive privacy training.

[37] In my draft, I recommended that SRHA implement mandatory annual privacy training for all employees.

[38] In response to my office's draft investigation report, SRHA indicated it was difficult to respond to this recommendation as all 12 Saskatchewan regional health authorities were in the process of transitioning into one provincial health authority.

[39] I recognize the difficulty in this time of transition to the Saskatchewan Health Authority. I am hopeful that SRHA and its staff will encourage and promote mandatory privacy training and the new Saskatchewan Health Authority will adopt a policy of mandatory annual privacy training for all employees.

Privacy Breach Report

[40] This final step is ensuring all the information collected is included in an internal privacy breach report. SRHA provided my office with its internal investigation report on September 18, 2017 detailing steps taken to respond to this breach.

III FINDING

[41] I find that SRHA's faxing practices do not follow its internal policy and procedure regarding faxing personal health information.

IV RECOMMENDATIONS

[42] I recommend that SRHA issue a revised letter to the affected individual containing the elements of personal health information involved in this privacy breach incident.

[43] I recommend that SRHA follow its internal policy and procedure for faxing personal health information.

Dated at Regina, in the Province of Saskatchewan, this 10th day of October, 2017.

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