Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 043-2018

Saskatchewan Health Authority

November 20, 2018

Summary: Kelly's Computer Works reported a privacy breach to the Office of the Saskatchewan Information and Privacy Commissioner (IPC). The private business received another misdirected fax. Around the same time, the Saskatchewan Health Authority (SHA) proactively reported the privacy breach to the IPC. 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 has not appropriately handled the privacy breach in accordance with the five best practice steps. The Commissioner recommended the SHA have its project timelines for its plan to eliminate faxing of personal health information within the health system completed within the next six months and provide them to the IPC. Further, the Commissioner recommended the SHA have a policy of mandatory annual privacy training for all employees.

I BACKGROUND

[1] On March 12, 2018, Kelly's Computer Works, a private business in North Battleford, contacted my office to report it had received another misdirected fax from the Saskatchewan Health Authority (SHA). The fax was received that morning and contained five pages. The fax was a catheterization report for a specific patient.

[2] Later on March 12, 2018, my office notified the SHA that it would be undertaking an investigation into the breach and requested a copy of its internal privacy breach investigation report and copies of written policies and/or procedures. The SHA advised that it had learned of the privacy breach from the media. Further, it advised that the fax

was intended for Dr. Rodriguez's office in Battleford. The SHA began an internal investigation.

II DISCUSSION OF THE ISSUES

1. Does my office have jurisdiction?

[3] 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?

[4] 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.

[5] 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 Royal University Hospital in Saskatoon. The Royal University 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.

[6] 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;

[7] The misdirected fax included a five page catheterization report about a specific patient. The information included (but was not limited to):

- the patient's name;
- health services number;
- date of birth;
- address;
- date of medical procedure;
- diagnostic indicators;
- medical history and risk factors;
- procedures performed;
- conclusions following medical procedures performed; and
- recommendations for treatment.

[8] 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.

[9] 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.

[10] 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?

[11] In circumstances where my office learns of a privacy breach and a trustee proactively reports it, the focus for my office becomes one of determining whether the trustee appropriately handled it. In order to be satisfied, my office would need to be confident that the SHA took the privacy breach seriously and appropriately addressed it. My office recommends 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.

[12] 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

[13] 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.

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

[15] In its internal investigation report, the SHA advised that in response to being asked to delete/destroy the misdirected fax, Kelly's Computer Works indicated that:

> "…the document isn't as easy as you might think. My fax machine forwards it via email to my Gmail account. My Gmail account forwards it to my Microsoft Exchange account. Both of those accounts retain back-ups. I will delete it out of my Exchange inbox and sent items – that I sent it to you with, but there are other copies in multiple locations including backups…I have other work to do, and it would take many hours, and jeopardize the integrity of my email back up system, which currently has over half a million emails. The onus is on you to make sure this doesn't happen, not for me to deal with after the fact. I have deleted these from my Exchange server."

[16] Kelly's Computer Works has been receiving misdirected faxes containing personal health information for at least two years. The response from Kelly's Computer Works is understandable. It is the responsibility of the SHA to get this issue addressed once and for all. It cannot expect a private business to continue to clean up its errors. This is the first my office is hearing that the misdirected faxes going to Kelly's Computer Works are forwarded through Gmail and then through Microsoft Exchange. This raises issues of back-up copies and risks that are inherent to moving personal health information through a webmail server. In Investigation Report 101-2017, I noted the security risks for government records posed by personal email accounts:

> [26] Personal email accounts pose information security risks for government records. For example, records could end up stored on email servers that are outside Canada. In instances where webmail services are used, such as Gmail or Hotmail, email content is scanned and read in order to provide targeted advertising. Personal information in those records is not only stored outside Canada but it is also disclosed to the webmail provider. Government institutions are required under FOIP to take reasonable security measures to protect personal information from unauthorized access, collection, use or disclosure. When government records are stored in a personal email account with data servers located outside of Canada, the government no longer has control of how that information will be protected, disclosed, or accessed.

[17] It appears the SHA has made efforts to contain the breach but the breach has not been contained. As long as there are copies and back-ups floating around, the personal health information remains at risk. As long as Kelly's Computer Works continues to receive misdirected faxes, the SHA will not be able to contain the breaches due to the faxes being passed through a webmail server.

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 notification was immediately provided to the affected patient via telephone and letter. A copy of the letter template was provided to my office.

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

[22] I am satisfied with the steps taken by the SHA.

Step 3: Investigate the breach

[23] 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.

[24] The SHA provided an internal investigation report. The SHA was able to determine the breach was caused by human error. Two employees were involved in the breach. One employee wrote down the fax number incorrectly, the other employee entered the incorrect fax number into the fax machine.

[25] In all cases involving misdirected faxes to Kelly's Computer Works, the cause is always employees incorrectly inputting the fax number. As has been noted in previous reports involving misdirected faxes to Kelly's Computer Works, the fax numbers for the two organizations are very similar:

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

[26] 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

[27] 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.

[28] In its internal privacy breach investigation report, the SHA listed the following preventative measures:

1. It reviewed its policies, protocol and expectations with the involved staff;
2. The Manager of the Cardiac Cath Lab was contacted and made aware of the breach;
3. Assurance was given to the SHA Privacy Officer that the issue would be addressed at the next staff huddle at the Cardiac Cath Lab;
4. A fax cover sheet was not used in this instance despite having a policy requiring them since 2014. The Privacy and Access team will do an education session for the staff at the Non-Invasive Cardiac Cath lab; and
5. The Privacy and Access team has suggested that Dr. Rodriguez's fax number be pre-programmed into the fax machine and a sign be placed above the fax machine reminding staff to use the pre-programmed number.

[29] Misdirected faxes containing personal health information is a recurring issue. In particular, misdirected faxes to Kelly's Computer Works. This is the fourth privacy breach of this nature addressed by my office.

[30] The first time my office was alerted to the issue was 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. 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.

[31] 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, my office 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 a fax cover sheet for Dr. Rodriguez's Office. Again, it appeared a "6" was used instead of a "5" in the fax number.

[32] The issue came to my office's attention again on January 12, 2018. The SHA and Kelly's Computer Works contacted my office to report another misdirected fax. The cause of the breach was a Medical Office Assistant from Shellbrook Hospital incorrectly entering the fax number. The fax number was pulled from the same fax cover sheet for Dr. Rodriguez's Office. Again, it appeared a "6" was used instead of a "5" in the fax number. During that 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 had been received since January 12, 2018. On this breach, I issued Investigation Report 005-2018.

[33] 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.

[34] Effective December 4, 2017, the 12 health regions in Saskatchewan were merged into 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.

[35] In Investigation Report 223-2017, I recommended that the SHA adopt a policy of mandatory annual privacy training for all employees. I learned during Investigation Report 005-2018 that the SHA had put this recommendation into action.

[36] Further, in Investigation Report 005-2018, my office was advised that:

> 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.

[37] In Investigation Report 005-2018, I recommended that the SHA implement its plan to eliminate faxing of personal health information within the health system within the next six to 12 months. That recommendation was made September 4, 2018. On October 1, 2018, my office received a response to this recommendation from the SHA. It indicated that:

> Eliminating faxing of personal health information has been identified as a priority in the Saskatchewan Health Authority. The SHA is working with eHealth our IT service provider on this initiative. The recommended 6-12 month timeline is likely unrealistic considering the complexity of changing workflows and systems across the health system, however we will be advancing this priority as expeditiously as possible. We will provide you with project timelines as they are developed.

[38] I am concerned with the timeline being undefined given that this has been an ongoing issue. Therefore, I recommend that the SHA provide the project timelines to my office within the next six months. Further, I recommend that the SHA have a policy of mandatory annual privacy training for all employees.

III FINDING

[39] I am not satisfied with how the SHA contained this privacy breach.

IV RECOMMENDATIONS

[40] I recommend that the SHA have its project timelines for its plan to eliminate faxing of personal health information within the health system completed within the next six months. Further, that it provide those timelines to my office within six months.

[41] I recommend the SHA have a policy of mandatory annual privacy training for all employees.

Dated at Regina, in the Province of Saskatchewan, this 20th day of November 2018.

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