Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 080-2022

Saskatchewan Health Authority

September 27, 2022

Summary: The Saskatchewan Health Authority (SHA) reported a privacy breach to the Commissioner's office involving a misdirected fax. The fax included the personal health information of 46 affected parties. The Commissioner investigated the privacy breach and found that it was a result of SHA's failure to have policies and practices in place to mitigate privacy risks. He also found that SHA efforts to contain the breach, notify affected parties and prevent further breaches were not adequate, but the steps taken to investigate the breach were adequate. To help address the systemic problem of misdirected faxes within SHA, he recommended that it provide his office with the terms of reference for SHA's working group on the privacy risks of using faxes and monthly reports on SHA's work. The Commissioner made a number of other recommendations which are set out at the conclusion of this Report.

I BACKGROUND

[1] On April 19, 2022, 48 patient care reports relating to 46 individuals, one of whom was deceased, were sent by fax to an individual (the recipient) by 3sHealth in error. The reports were intended to be sent to a specific physician.

[2] At the material time, 3sHealth was providing transcription services in relation to these patient care reports on behalf of the Saskatchewan Health Authority (SHA) under a shared services agreement.

[3] On April 21, 2022, SHA's Privacy Office advised my office of the incident. On April 26, 2022, 45 affected individuals were notified of the incident by SHA. SHA did not notify anyone on behalf of the affected party who is deceased.

[4] On May 4, 2022, my office notified SHA that it would be undertaking an investigation pursuant to section 52(d) of *The Health Information Protection Act* (HIPA). In the notification, my office requested SHA investigate the matter and provide my office with a completed *Privacy Breach Investigation Questionnaire*.

[5] On June 14, 2022, SHA provided my office with:

- Privacy Breach Investigation Report
- 3sHealth *Work Standard - Adding Physician or Clinic to Database*
- 3sHealth *Work Standard - Fax Number Verification Process*
- 3sHealth sample fax cover sheet

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[6] HIPA applies when three elements are present: (1) "personal health information" (2) "trustee" and (3) the personal health information is in the custody or control of the trustee.

[7] All the patient care reports contained patients' name, telephone number and address, date of birth and health number. The other information in the reports varied for each affected patient, but included information about consultations, discharge summaries, operating room reports, outpatient reports and inpatient progress notes. This information qualifies as "personal health information" as defined by section 2(m)(i) and (ii) 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 second criteria has also been met because SHA is a "trustee" pursuant to section 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;

[9] I turn to consider if SHA had custody or control over the personal health information at issue. "Custody" is physical possession with a measure of control. "Control" connotes authority. A record is under the control of a trustee when the trustee has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition. Custody is not a requirement for control (*Guide to HIPA*, "Appendix A - Glossary". December 2016, [*Guide to HIPA*], p. 151).

[10] The misdirected fax was sent by 3sHealth. Previous reports of my office found that 3sHealth was an information service provider for the Saskatoon Regional Health Authority (the predecessor to SHA) pursuant to section 2(j) of HIPA (see for example Investigation Report 152-2017 and 219-2017). Section 2(j) of HIPA provides:

> **2** In this Act:
>
> …
> (j) "information management service provider" means a person who or body that processes, stores, archives or destroys records of a trustee containing personal

> health information or that provides information management or information technology services to a trustee with respect to records of the trustee containing personal health information, and includes a trustee that carries out any of those activities on behalf of another trustee, but does not include a trustee that carries out any of those activities on its own behalf;

[11] Given the relationship between 3sHealth and SHA, the personal health information that 3sHealth processed on behalf of SHA is within the control of SHA. Therefore, the third criteria for the application of HIPA has been met.

[12] In light of the above, I find that HIPA applies, and 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 and/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 organization. Before disclosing personal health information, a trustee should ensure it has authority to do so under HIPA.

[15] In this case, 3sHealth sent a fax containing 46 patients' personal health information to the wrong fax number. As noted above, the fax was sent to the recipient and not received by the physician for whom it was intended. This qualifies as an unauthorized disclosure. Therefore, I find that a breach of privacy occurred.

3. Did SHA respond appropriately to the privacy breach?

[16] Where a trustee proactively reports a privacy breach to my office, my office determines whether the trustee appropriately responded to the privacy breach. In accordance with my office's *Rules of Procedure*, my office will analyze whether the trustee appropriately managed the breach and took the following steps in responding to the privacy breach:

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

[17] I consider below if SHA followed these steps and will make any recommendations as necessary at the end of my analysis.

Contained the breach (as soon as possible)

[18] 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 to personal health information
- Correcting weaknesses in physical security.

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

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

[20] According to SHA's Privacy Breach Investigation Report, 3sHealth took steps to contain the breach by contacting the recipient by telephone on two occasions asking them to delete the patient care reports and not to share them. The individual refused to identify themselves and confirm that they had deleted the personal health information. However, SHA was able to confirm that the records were transferred to the recipient electronically and not printed.

[21] In the circumstances of this breach, when the recipient of the fax proved to be uncooperative, SHA should have written to them seeking their written confirmation that they had deleted the records and had not/would not print or share the information with others. I find, therefore, that SHA did not take sufficient steps to contain the breach. I note that the challenges SHA faced in containing this breach illustrate the significant risk that can arise from misdirected faxes. I recommend that where efforts at containing a privacy breach via the telephone are not successful, SHA senior staff should send a demand letter to the recipients of the personal health information asking them for written confirmation that they have deleted and have not/will not print or share the information with others.

Notify affected individuals (as soon as possible)

[22] Notifying an individual that their personal health information was inappropriately accessed is important for several reasons. Not only do individuals have a right to know, but they also need to know to protect themselves from any potential harm that may result from the inappropriate access or disclosure. Unless there is a compelling reason not to, trustees should always notify affected individuals. A notification should include:

- A description of what happened (a general description of what happened)
- A detailed description of the personal health information involved (e.g., name, medical record, etc.)
- A description of the types of harm that may possibly come to them because of the privacy breach
- 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] In addition to notifying individuals, depending on the type of the breach, trustees may want to notify other organizations, for example, my office, law enforcement or other regulatory bodies that oversee professions.

[24] Given the ongoing problems with the use of faxes to communicate personal health information, discussed in more detail below, I recommend that SHA proactively report all misdirected fax breaches to my office. This would enable my office to track and report publicly on the progress of SHA's efforts to address the privacy risks and bring some transparency and accountability to its work to address this problem.

[25] According to SHA's Privacy Breach Investigation Report, it notified affected individuals by mail on April 26, 2022. SHA provided my office with the template used for its notification letters.

[26] Upon review of the template, it informs affected individuals that their records were faxed to an individual in error. The template includes an apology and indicates SHA is investigating the root cause of the breach. The letter also provides the affected individuals the contact information for my office if they are not satisfied with SHA's response to the breach.

[27] The template does not include a description of the types of harm that may occur because of the privacy breach. As the names, addresses and dates of birth of the affected individuals were included in the misdirected fax, SHA's notification to affected individuals should have included a warning about the risks of identity theft and the steps that could be taken to minimize the risk, such as credit monitoring. I recommend that SHA's notifications to affected parties include a description of the types of harm that may occur as a result of the breach, and the steps that can be taken to mitigate the risk. This will not only assist affected parties, but it ensures SHA is considering the risks and impacts of all breaches.

[28] SHA confirmed to my office that it did not take any steps regarding notification of the affected individual who is deceased. When an affected party is a deceased person, trustees

should notify the deceased person's personal representative where known. If the deceased person's personal representative is unknown, a letter should be placed on the person's file. I recommend that SHA ask the deceased person's physician to place a notification letter on the deceased patient's medical files. This approach to notification is consistent with the approach recommended by the Ontario Information and Privacy Commissioner in PHIPA Decision 102.

[29] As a result of the above, I find that the notification provided by SHA to the affected individuals was not sufficient.

[30] I note that in response to my office's Investigation Report 032-2022, SHA stated that it is developing a work standard for patient notification which will detail how it provides verbal and/or written notification to a person affected by a privacy breach. During the investigation into this breach, SHA advised my office that it is committed to developing the work standard, however the work is still in progress.

[31] I recommend that SHA's work standard include instructions on how to notify affected parties who are deceased at the time of the breach and require that affected parties be informed about risks that may result from an unauthorized disclosure. I also recommend that SHA provide my office with a copy of the completed work standard within 30 days of issuance of this Report.

Investigated the breach

[32] Once the breach has been contained and appropriate notification has occurred, the trustee should continue its internal investigation. At the conclusion of its investigation, the trustee should have an understanding of the cause of the breach which will inform how to prevent future breaches.

[33] According to SHA's Privacy Breach Investigation Report, on April 20, 2022, 3sHealth was notified by the recipient that they had received the patient care reports in error.

[34] 3sHealth immediately commenced an investigation. It removed the incorrect fax number from the system used to store the numbers – the Fluency Manager System. On April 21, 2022, 3sHealth contacted the physician's office to inquire about the correct fax number. As the office was closed, 3sHealth did not obtain the correct fax number until April 25, 2022. On that day, the patient care reports were sent by fax to the physician's office using the correct fax number.

[35] 3sHealth contacted the recipient on two occasions to advise them to destroy and dispose of the records securely. However, as noted above, the recipient would only confirm that the records were not printed.

[36] The 3sHealth Technical Coordinator (TC) responsible for sending the misdirected fax was interviewed by 3sHealth as part of the investigation. The TC provided the following description of the circumstances surrounding the breach.

[37] The TC was tasked with sending the patient care reports by fax using 3sHealth's Fluency Manager System to the physician's office. When the TC was unsuccessful in sending the fax, they contacted the physician's office and were provided with a fax number by the receptionist. On March 21, 2022, the TC entered the fax number provided by the receptionist in the Fluency Manager System and made another attempt to send the records. However, the fax did not go through.

[38] On April 20, 2022, for an unknown reason, the patient care reports were automatically sent to the fax number entered into the Fluency Manager System on March 21, 2022. As 3sHealth and SHA subsequently learned, the fax number that was supplied by the physician's office on March 21, 2022 was not the correct number. As a result, the patient care reports were misdirected to the recipient.

[39] Once 3sHealth notified SHA of the breach, SHA took over the investigation. Notification was sent by SHA to the affected individuals, but for the deceased person, and my office on April 26 and 29, 2022, respectively.

[40] 3sHealth contacted TELUS, the telephone service provider to the physician, to investigate why the fax number initially provided by the physician's office resulted in the patient care reports being sent to the recipient.

[41] As a result of conversations with TELUS staff, 3sHealth determined that the fax number initially provided by the physician's office was a number that had been disabled in May of 2021 and replaced with a new number. Sometime later the number was reassigned to the recipient. Staff in the physician's office had not remembered that the number had been replaced and provided it to the TC in error.

[42] At the time of the privacy breach, 3sHealth did not have any written policies in place that required the TC to verify that fax numbers to be entered in the Fluency Manager System were correct. My office was advised however that it was 3sHealth's practice to contact the physician's office to seek verbal verification before entering a fax number into that system. This practice was followed by the TC in this case.

[43] Based on the information provided, this privacy breach was caused in part by the failure of the physician's office to provide 3sHealth's TC with the correct fax number for its clinic. However, the fact that 3sHealth did not have a system in place to test the accuracy of the fax numbers before they are used, contributed to the breach. A testing process would have caught this error and other errors that arise when a fax number is entered incorrectly into the system. Therefore, I find that the failure of 3sHealth to have policies in place to mitigate the potential privacy risk contributed to the breach.

[44] Based on the information provided, I find that the steps taken to investigate the breach were adequate.

Taken appropriate steps to prevent future breaches

[45] Prevention is perhaps one of the most important steps. A privacy breach cannot be undone, but a trustee 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 formulate a prevention plan. Necessary changes may have been identified 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.

[46] With respect to its efforts to prevent further breaches of this kind, SHA's Privacy Breach Investigation Report asserted:

> To prevent faxes from being sent to the incorrect recipient or mitigate the risks of this happening again, a new Work Standard was created. This new fax number verification process will implement two factor verification (verbal and documented) before faxing confidential patient care reports to physicians/clinics/departments etc. This verification process is required for new fax number entries, or any changes or updates to the current system.
>
> The SHA, 3sHealth, and eHealth are working to eliminate these errors from occurring by strengthening processes and procedures, and educate staff and physicians to prevent these types of errors.
>
> In February of 2022 the OIPC released a report recommending the SHA work toward the elimination of the use of traditional faxing. As a result, the SHA formed a working group to review all of the recommendations in the OIPC report, and determine the feasibility of the recommendations, and timelines for possible implementation. The working group is also reviewing any work that may have been completed prior to the release of the recent OIPC report to determine the next steps.

[47] A copy of 3sHealth's new Work Standard relating to fax number verification was provided to my office. In summary it states, in every case where the fax number is not already saved in the system, staff must telephone the physician's office and request verbal clarification of the fax number. If the fax number provided by the physician's office is listed on the physician's website or there is an automated message that includes the fax number, then verbal verification of the number is sufficient. If the fax number is not documented anywhere, then a test fax must be sent to the physician's office. Once the physician's office responds to the test fax confirming the number, then the number can be added to the system.

[48] I appreciate that SHA has taken steps to address the specific circumstances surrounding this breach. I note that in response to my office's Investigation Report 032-2022, where I

recommended that SHA prioritize eliminating the use of fax machines immediately, SHA's letter dated August 3, 2022, stated:

> The SHA is committed to reducing our faxing footprint and has taken strides through COVID to automate critical workflows wherever possible. We will continue to work with eHS to prioritize and request funding for related initiatives where needed.

[49] I also appreciate learning that SHA, 3sHealth and eHealth are working to eliminate errors from occurring when using fax to transmit personal health information by strengthening processes, procedures and through education. Other information about measures to reduce the number of misdirected faxes was provided to my office in its August 3, 2022 letter.

[50] However, I am concerned about the lack of detailed information provided to my office about SHA's efforts to address the privacy risks of faxing on a systemic basis. As noted in my office's Investigation Report 032-2022, the history of my office's experience with breaches involving misdirected faxes goes back to a report on the subject written in 2010, *Report on Systemic Issues with Faxing Personal Health Information*. Investigation Report 032-2022 includes a summary of numerous previous privacy investigations involving misdirected faxes and describes the significant, ongoing privacy risks arising from the use of faxes to communication personal health information.

[51] According to information provided by 3sHealth, the privacy risks of using fax to transmit personal health information were noted by TELUS during its investigation of the breach. TELUS staff advised 3sHealth that it should consider using a service other than faxing for transfers of personal health information. TELUS described faxing as "old and outdated technology." It provided 3sHealth with information about other services available through its company.

[52] The privacy risks of misdirected faxes were the subject to a recent Federal, Provincial and Territorial Information and Privacy Commissioners and Ombudspersons with Responsibility for Privacy Oversight Resolution. The resolution calls for a concerted effort across the healthcare sector to modernize and strengthen privacy protections for sharing

personal health information. It urges stakeholders to develop a plan to phase out the use of traditional fax and unencrypted email to address the privacy risks and thereby protect and bolster public trust in digital healthcare.

[53] In these circumstances and based on the information provided to my office, I find that SHA's plan to prevent further breaches arising from the use of fax to communicate personal health information is not adequate to address the systemic issues.

[54] I recommend that SHA provide my office with any terms of reference for the working group on misdirected faxes referred to in its submission. I also recommend that SHA provide my office with monthly updates on the work of its working group. The terms of reference and first monthly update should be provided within 30 days of the release of this report. Through its monthly updates SHA will have an opportunity to demonstrate accountability and transparency in relation to its attempts to reduce these privacy risks. This will also help build public trust in SHA's ability to protect personal health information.

III FINDINGS

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

[56] I find that a breach of privacy occurred.

[57] I find that SHA's efforts to contain the breach were not adequate.

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

[59] I find that the steps taken to investigate the breach were adequate.

[60] I find that SHA's plan to prevent further breaches is not adequate.

IV RECOMMENDATIONS

[61] I recommend that, in the future, where efforts at containing a privacy breach via the telephone are not successful, SHA senior staff send a letter to recipients of the personal health information asking them for written confirmation that they have deleted and have not/will not print or share the information with others.

[62] I recommend that SHA proactively report all misdirected fax breaches to my office.

[63] I recommend SHA's notifications to affected parties include a description of the types of harm that may occur as a result of the breach, and steps that can be taken to mitigate the risk.

[64] I recommend that SHA notify the deceased affected party by asking their physician to place a notification letter on the patient's medical file.

[65] I recommend that the work standard for patient notification being developed by SHA include instructions on how to notify affected parties who are deceased at the time of the breach and require that affected parties be informed about the risks that may result from an unauthorized disclosure.

[66] I recommend that SHA provide my office with a copy of the work standard for patient notification within 30 days of issuance of this report.

[67] I recommend that, to address the systemic problem of misdirected faxes, SHA provide my office with any terms of reference for its working group on misdirected faxes referred to in its submission.

[68] I recommend that SHA provide my office with monthly updates on the work of its working group on misdirected faxes. The terms of reference and 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 27th day of September, 2022.

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