Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 126-2021

Saskatchewan Health Authority

June 9, 2022

Summary: The laboratory requisition for a patient located in Prince Albert, Saskatchewan erroneously listed a physician in Regina as the patient's family physician. Therefore, the laboratory report was then sent to the physician in Regina instead of the patient's actual family physician. The patient's family physician has a similar name of the physician located in Regina. The Commissioner found that a privacy breach occurred. He recommended that the Saskatchewan Health Authority (SHA) prioritize designing and implementing solutions to reduce data entry errors and to provide his office with quarterly updates to his office until the implementation of solutions is complete. He also recommended that the SHA ensure its systems reflect its work standard so that users are indeed entering full names and that the users are verifying with patients.

I BACKGROUND

[1] This Report deals with a misdirected fax reported to my office. I have identified a potential conflict with this misdirected fax. Therefore, I have taken no part in the investigation. I have delegated the Deputy Commissioner to make all decisions related to this matter.

[2] On April 29, 2021, a patient attended a testing site for the coronavirus disease of 2019 (COVID-19) in Prince Albert, Saskatchewan. A laboratory requisition and the test swab was sent to the laboratory department at the Saskatchewan Health Authority (SHA). The laboratory requisition mistakenly listed Dr. J.S McMillan as the patient's family physician instead of Dr. James MacMillan. As a result, the test results were sent to Dr. J.S. McMillan instead of Dr. James MacMillan.

[3] On May 11, 2021, my office learned of this error.

[4] On May 12, 2021, my office notified the SHA that it would be undertaking an investigation.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[5] *The Health Information Protection Act* (HIPA) is engaged 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.

[6] First, personal health information is defined by section 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;
>
> (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] Based on a review of the laboratory results, I find that there is the personal health information of an individual involved as defined by section 2(m) of HIPA.

[8] Second, "trustee" is defined by 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] The laboratory report originated from a laboratory department at St. Paul's Hospital in Saskatoon which is a facility of the SHA. I find that the SHA qualifies as a trustee as defined by section 2(t)(ii) of HIPA.

[10] Third, I must determine if the personal health information is in the custody or control of the SHA.

[11] Since the laboratory report originated from the SHA to Dr. J.S. McMillan through the Laboratory Information System, I find that the SHA had custody or control over the personal health information.

[12] Based on the above, I find that HIPA is engaged and 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 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, the SHA erroneously sent the laboratory report to Dr J.S. McMillan instead of Dr. James MacMillan. This would constitute an unauthorized disclosure. Therefore, I find that a privacy breach has occurred.

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

[16] In my office's resource, *Privacy Breach Guidelines for Trustees* (updated September 2021) (Privacy Breach Guidelines), my office recommends four steps to be taken when a trustee discovers a privacy breach. The four steps are:

1. Contain the breach
2. Notify affected individuals
3. Investigate the breach
4. Prevent future breaches

[17] Below is an analysis to determine if the SHA responded appropriately to the privacy breach based on the four steps.

Contain the breach

[18] To contain a breach is to ensure the personal health information is no longer at risk. This may involve:

- stopping the unauthorized practice
- recovering the records
- shutting down the system that was breached
- revoking access to personal health information
- correcting weaknesses in physical security

[19] Earlier this year, my office issued Investigation Report 045-2021 et al. that covered many misdirected fax cases where Dr. J.S. McMillan was mistaken for Dr. James MacMillan. Dr. J.S. McMillan had confirmed with my office that his office had destroyed copies of the misdirected faxes after reporting the matter to my office. Therefore, I find that the privacy breach has been contained.

Notification

[20] Notifying individuals affected by the breach should occur as soon as possible after key facts about the breach have been established. It is best to contact affected individuals directly, such as by telephone, letter or in person. However, there may be circumstances where it is not possible and an indirect method is necessary or more practical. Such situations would include where contact information is unknown or where there are a large number of affected individuals. An indirect method of notification could include a notice on a website, posted notices, media advisories, and advertisements. It is important to ensure the breach is not compounded when using indirect notification. An effective notification should include the following:

- a description of the breach (a general description of what happened)
- a detailed description of the personal information or personal health information involved (e.g. name, credit card numbers, medical records, financial information, etc.)
- a description of possible types of harm that may come to them as a result 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 contact credit reporting agencies, how to change a health services number or driver's license number, etc.)
- 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 my office (provide contact information)
- recognition of the impacts of the breach on affected individuals and, an apology.

(Privacy Breach Guidelines, p. 4)

[21] In this case, the SHA notified the affected individual by telephone on May 14, 2021, to inform them of the misdirected fax. The patient confirmed that Dr. James MacMillan was the correct physician and also confirmed that they received the test results. Based on the

submission from the SHA, it is not clear that the SHA's phone call to the affected individual included important elements of what makes an effective notification, including advising the affected individual they have a right to complain to my office. I find that the SHA has made efforts to notify the affected individual of the privacy breach. However, I find that the SHA has not demonstrated that it has included the elements of what makes an effective notification in its phone call to the affected individual. I recommend that when the SHA contacts affected individuals by telephone, that it ensure it is including the elements of what makes an effective notification in its telephone call to affected individuals. This may include establishing a telephone script for SHA personnel to ensure they cover all the elements of an effective notification.

Investigation

[22] Investigating the privacy breach to identify the root cause(s) is key to understanding what happened and to prevent similar privacy breaches in the future. Below are some key questions to ask during a privacy breach investigation:

- When and how did your organization learn of the privacy breach?
- What occurred?
- How did the privacy 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, p. 5)

[23] In its investigation, the SHA determined the initial error occurred at the originating requisition stage. A human error occurred as a result of look-alike and sound-alike first and last names of Dr. J.S. McMillan and Dr. James MacMillan. I find that the SHA has investigated this matter to identify the root cause of this misdirected fax.

[24] I note that this error is not a one-off mistake. In my office's Investigation Report 045-2021 et al., my office described two cases ("Category 1, Case #3" and "Category 4, Case #2") where digital requisitions at COVID-2019 testing sites were filled out incorrectly. In those two cases in Investigation Report 045-2021 et al., Dr. J.S. McMillan's name was also mixed-up for Dr. James MacMillan. My office recommended that SHA design and implement a solution (or solutions) that reduces data entry errors. This could include the computer system prompting staff to double-check data if a patient's location does not match the location of the physician. In response to this recommendation, the SHA indicated it "will work on change management and data quality strategy to reduce data entry errors."

[25] As I noted in Investigation Report 045-2021 et al., systems that rely on its users to be on their best and most alert behaviour at all times will fail. Humans will continue to commit human errors. However, we must design systems to help its users to minimize errors and achieve the intended outcomes. SHA's response to my office's recommendation in Investigation Report 045-2021 et al. acknowledges the importance of reducing such errors.

[26] I recommend that the SHA prioritize designing and implementing solutions to reduce data entry errors. I recommend that the SHA provide quarterly updates to my office until the implementation of solutions is complete.

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, the 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 this case, the SHA noted that the "confirmation of correct provider needs to be ensured". It noted that its work standard entitled, "Physician Naming Convention ADT System"

regarding carbon copying family physicians instructs employees to enter a full name and does not allow nicknames or abbreviations. It also requires the employee to verify the information with the patient. I find that such a work standard is helpful, but it still relies on its users being on their best and most alert behaviour. As such, I find that the SHA has not implemented a sufficient prevention strategy. I recommend that the SHA come up with a strategy to ensure its systems reflect its work standard by testing to ensure its users are indeed entering full names and that users are verifying information with the patient.

III FINDINGS

[29] I find that HIPA is engaged and that I have jurisdiction to investigate this matter.

[30] I find that a privacy breach has occurred.

[31] I find that the privacy breach has been contained.

[32] I find that the SHA has made efforts to notify the affected individual of the privacy breach.

[33] I find that the SHA has not demonstrated that it has included the elements of what makes an effective notification in its phone call to the affected individual.

[34] I find that the SHA has investigated this matter to identify the root cause of this misdirected fax.

[35] I find that the SHA's work standard entitled, "Physician Naming Convention ADT System" is helpful, but it still relies on users being their best and most behaviour at all times.

[36] I find that the SHA has not implemented a sufficient prevention strategy.

IV RECOMMENDATIONS

[37] I recommend that when the SHA contacts affected individuals by telephone, that it ensure it is including the elements of what makes an effective notification in its telephone call to affected individuals. This may include establishing a telephone script for SHA personnel to ensure they cover all the elements of an effective notification.

[38] I recommend that the SHA prioritize designing and implementing solutions to reduce data entry errors. I recommend that the SHA provide quarterly updates to my office until the implementation of solutions is complete.

[39] I recommend that the SHA come up with a strategy to ensure its systems reflect its work standard by testing to ensure its users are indeed entering full names and that users are verifying information with the patient.

Dated at Regina, in the Province of Saskatchewan, this 9th day of June, 2022.

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