Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 014-2018, 016-2018

Saskatchewan Health Authority

July 18, 2018

Summary: Two lab reports containing personal health information were sent to the incorrect physician. These two privacy breaches occurred as a result of employees from the SHA selecting the incorrect physician's name in the Laboratory Information System (LIS). The Information and Privacy Commissioner (IPC) recommended that the Saskatchewan Health Authority (SHA) require employees to search physicians in LIS by the physician's unique identification number, or require employees to use two pieces of information about the physician to search (for example, searching for the physician by entering in both the first and last name). The IPC also recommend that the SHA explore options so that LIS is configured in such a way that if users only enter in the physician's last name to search, that LIS will prompt the user to enter the physician's unique identification number or an additional piece of information (such as a first name).

I BACKGROUND

[1] On January 22, 2018, Dr. Suzanne Meiers (Dr. S. Meiers) reported to my office that she received the two lab reports of two patients that were not hers. She received the first lab report on December 19, 2017 and the second one on January 17, 2018. Based on a review of the lab reports, the lab reports originated from Saskatoon Regional Health Authority's (SRHA) Department of Pathology and Laboratory Medicine.

[2] It should be noted that the SRHA was amalgamated into the Saskatchewan Health Authority (SHA) on December 4, 2017. Therefore, on January 26, 2018, my office notified the Saskatchewan Health Authority (SHA) that it was undertaking an investigation into each of the misdirected lab reports.

II DISCUSSION OF THE ISSUES

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

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

[4] First, 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;
>
> …
>
> (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;

[5] Based on a review of the two lab reports, I find that personal health information is present.

[6] Second, the term trustee is defined by subsection 2(t)(ii) of HIPA as follows:

> 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;

[7] I find that SHA is a trustee.

[8] Third, the lab reports originated from SHA's Department of Pathology and Laboratory Medicine. I find that SHA has control over the personal health information.

[9] Based on the above, I find that HIPA is engaged.

2. Were there unauthorized disclosures of personal health information?

[10] 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. A trustee should only be disclosing personal health information in accordance with HIPA.

[11] In these cases, SHA disclosed personal health information to Dr. S. Meiers due to errors. I find that unauthorized disclosures occurred.

3. Did SHA respond to this privacy breach appropriately?

[12] My office suggests that trustees undertake the following five steps when responding to a privacy breach:

- Contain the breach,
- Notify affected individual(s),
- Investigate the privacy breach,
- Prevent future privacy breaches,
- Write an investigation report.

[13] Below is an analysis of each step.

Contain the breach

[14] To contain the privacy breach is to ensure that the personal health information is no longer at risk. This may include recovering the record(s), revoking access to personal health information, and/or stopping the unauthorized practice.

[15] In these two cases, the personal health information was contained when Dr. S. Meiers' office sent the records to my office. In an email dated April 25, 2018, Dr. S. Meiers' office confirmed that it had deleted the reports.

[16] I find that the breach has been contained.

Notify the affected individuals

[17] Notifying the affected individuals of the privacy breach is important so that they can determine how they have been impacted and take steps to protect themselves. A notification should include the following:

- A description of what happened,
- A detailed description of the personal information or personal health information that was involved,
- If known, 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,
- The contact information of the Office of the Information and Privacy Commissioner,
- Where appropriate, recognition of the impacts of the breach on affected individuals and an apology.

[18] SHA identified that there are two individuals who were affected by these two unauthorized disclosures. It provided my office with a copy of the notification letters sent to the affected individuals. Based on a review of the two letters, it contains the necessary elements.

[19] I find the affected individuals have been notified.

Investigate the privacy breach

[20] Investigating the privacy breach to identify the root cause is key to understanding what happened and to prevent similar privacy breaches in the future.

[21] In both cases, the lab requisition had indicated that the lab reports were to be sent to Dr. P. Meiers, not Dr. S. Meiers. However, the clerical staff member selected the incorrect physician in the Laboratory Information System (LIS). As a result, the lab reports were sent to the incorrect physician.

[22] The SHA provided my office with two screenshots from LIS. The first screenshot is of the "Doctor Search Screen". This screen has eight text fields. Users may enter a term into one of the text fields to search for a physician. For example, a user can enter the last name of a physician into the "last name" text field to search for a physician.

[23] When the last name "Meiers" is entered into the last name field, Dr. S. Meiers and Dr. P. Meiers are listed. Dr. S. Meiers' name appears first. As a result, Dr. S. Meiers' name is automatically highlighted. If the user does not manually select Dr. P. Meiers, then Dr. S. Meiers is selected.

[24] The second screen shot is of the "Doctor/Clinic lookup". This screen has four text fields to enter a term into to search for a physician. When a user enters "Meiers" into the last name field, Dr. S. Meiers and Dr. P. Meiers are listed. Again, Dr. S. Meiers is automatically highlighted so if the user does not manually select Dr. P. Meiers, then Dr. S. Meiers is selected.

[25] The automatically selecting of Dr. S. Meiers' name in LIS appears to increase the likelihood of a user incorrectly selecting Dr. S. Meiers' name.

Prevent future privacy breaches

[26] Preventing future breaches means to implement measures to prevent similar breaches from occurring.

[27] SHA indicated to my office that its Department of Pathology and Laboratory Medicine has had a discussion with its clerical staff regarding the seriousness and impact of these types of privacy breaches. It has also requested that SHA's privacy officers provide privacy training to its staff.

[28] I find that the above steps taken by SHA are appropriate.

[29] My office has issued four other investigation reports which discuss a similar issue. They are:

- Investigation Report 152-2017 and 219-2017 and Investigation Report 151-2017, 208-2017, 233-2017, 235-2017 are about privacy breaches that occurred when physicians did not dictate the first name of the receiving physician, and transcriptionists would select the incorrect physician as the receiving physician. For example, transcriptionists selected Dr. S. Meiers when the transcribed report should have been Dr. P. Meiers, and vice versa.

- Investigation Report 305-2017 is about how a privacy breach occurred when a staff member of the Regina Physician Group (RPG) incorrectly selected Dr. S. Meiers as a patient's family physician instead of a Dr. C. Meier.

- Investigation Report 083-2018, 084-2018 is about two privacy breaches. The first privacy breach was due to staff misinterpreting the physician's signature on the lab requisition and selecting the incorrect physician to send the lab report. The second privacy breach was due to staff not matching the physician's name on the lab requisition to the name that was appearing on the form in LIS.

[30] This investigation report and the above investigation reports suggest that these types of breaches are occurring frequently throughout the province but not all of them are being reported to my office. It may be worthwhile to explore methods of identifying physicians by something other than their last names to minimize the number of these types of breaches. After all, it is common for physicians to have the same or similar last names and these privacy breaches are resulting from physicians having the same or similar last names. The SHA has indicated that physicians have a unique identification number, and it can be used to search for physicians in LIS. Systems should be identifying physicians in a different way such as a unique identification number.

[31] I recommend that SHA require employees to search physicians in LIS by the physician's unique identification number, or require employees to use two pieces of information about the physician to search. For example, searching for a physician by entering in both the first and last name of the physician. I recommend that the SHA explore options so that LIS is configured in such a way that if users only enter in the physician's last name to search, that LIS will prompt the user to enter the physician's unique identification number or an additional piece of information (such as the first name).

Write an investigation report

[32] Documenting privacy breaches and the trustee's investigations into the breaches is a method to ensure the trustee follows through with plans to prevent similar breaches in the future.

[33] SHA provided my office with its internal investigation report into the two privacy breaches that described the breaches, how it responded to the breaches, and steps it took to prevent similar privacy breaches.

III FINDINGS

[34] I find that HIPA is engaged.

[35] I find that unauthorized disclosures occurred.

[36] I find that SHA responded to these two privacy breaches appropriately.

IV RECOMMENDATIONS

[37] I recommend that SHA require employees to search physicians in LIS by the physician's unique identification number, or require employees to use two pieces of information about the physician to search. For example, searching for a physician by entering in both the first and last name of the physician.

[38] I recommend that the SHA explore options so that LIS is configured in such a way that if users only enter in the physician's last name to search, that LIS will prompt the user to enter the physician's unique identification number or an additional piece of information (such as the first name).

Dated at Regina, in the Province of Saskatchewan, this 18th day of July, 2018.

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