Office of the
Saskatchewan Information
and Privacy Commissioner

REVIEW REPORT 222-2018

Saskatchewan Health Authority

December 11, 2019

Summary: The Saskatchewan Health Authority (SHA) sent a pathology lab report to the Saskatchewan Cancer Agency for an individual who was not its patient. The Commissioner found that a breach occurred when the SHA failed to verify the identity of the patient but found that the SHA has since made sufficient changes to prevent further breaches of this type from happening again. The Commissioner recommended that the SHA take no further action.

I BACKGROUND

[1] On October 9, 2018, the Plains Surgical Associates (PSA) reported to my office that it received a pathology lab report for its patient. On the lab report, PSA noticed a copy was also sent to the Allan Blair Cancer Centre (ABCC). PSA indicated to my office that this patient was not a patient of ABCC. The ABCC is part of the Saskatchewan Cancer Agency (SCA).

[2] The lab report was created by and originated from the Department of Pathology and Laboratory Medicine (the Lab) of the Saskatchewan Health Authority (SHA).

[3] On October 12, 2018, my office informed the SHA of the issue, requested it investigate the potential breach of personal health information and report back to my office.

[4] On October 15, 2018, the SHA responded to my office indicating that it had determined the disclosure of personal health information to the SCA was authorized, and therefore, not a privacy breach.

[5] On October 24, 2018, my office notified the SHA that my office was undertaking an investigation into this incident to see if my office would reach the same conclusion.

II DISCUSSION OF THE ISSUES

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

[6] 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.

[7] 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;
>
> (iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual 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 lab report contains information on the clinical history, the description of a body part, the diagnosis as well as the registration information of the patient; therefore, I find that the lab report constitutes personal health information.

[9] 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;

[10] I find that the SHA is a trustee.

[11] Third, the lab report was created by and originated from the Lab. I find that SHA had control over the personal health information in question.

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

2. Was there an unauthorized disclosure of personal health information by SHA?

[13] 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.

[14] SCA collects personal health information for the purposes of supporting cancer care and control in the province. There are two processes where this occurs. One is an automated process where SCA pulls lab reports with certain cancer indicators. The second is a manual process whereby the SHA sends the SCA copies of lab reports. The SHA initially identified that the breach occurred during the automated process, however, later determined that it

occurred as a result of the manual process. I will not be reviewing the automated process, as this breach occurred during the manual process.

[15] In this incident, SHA disclosed personal health information to the SCA of an individual who was not a patient of the SCA and, as such, the SCA did not have a need-to-know. I find that an unauthorized disclosure occurred and this was a privacy breach.

3. Did SHA respond to this privacy breach appropriately?

[16] 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; and
- write an investigation report.

[17] Below is an analysis of each of these steps.

Contain the breach

[18] 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.

[19] The copy of the lab report was sent electronically to the SCA. Since this patient is not registered within the SCA's Electronic Medical Record (EMR), it created an alert in the IEM system when it could not link the record to a patient file. The alert was then reviewed by the SCA and then deleted immediately. More background on how this breach occurred is outlined below in the investigating of the breach portion of this Report.

[20] The SHA determined that the SCA received the record in error and had immediately deleted the record and that the SCA has retained no record of this individual.

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

Notify the affected individuals

[22] 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; and
- where appropriate, recognition of the impacts of the breach on affected individuals and an apology.

[23] The SHA indicated that it does not have the individual's current contact information to be able to provide notice as they are no longer in Canada. They were in Regina visiting for a short period. When an out-of-country patient is registered for pathology testing, there are

fields to register only one address. The telephone number and address that was registered was that of a family member living in Regina. When the SHA called the number on file to verify an address to notify the individual, the number was no longer in service.

[24] I find that the SHA made a reasonable attempt to notify the affected individual.

Investigate the privacy breach

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

[26] All patients who attend a hospital are registered in the Sunrise Enterprise Registration system (SER). This system interfaces with all other systems in the hospital including the Laboratory Information System (LIS).

[27] The patient involved in this incident is a non-Saskatchewan resident, therefore, no Health Services Number HSN was registered in SER. In situations where a patient does not have a HSN, a 'dummy' HSN number is assigned to that patient in the LIS. In this instance, this number was then overwritten, during the patient transfer process, by SER. When the Lab then obtained the result and searched for the HSN to determine whether the result should be sent to the ABCC, it did not exist.

[28] When, as in this case, there are no HSN matches in the system, accession staff will then perform a secondary search looking for patients with the same date of birth (DOB) and gender. In this instance, there was a second patient with the same DOB and gender who had a previous cancer diagnosis. The accession staff did not recognize that this was not the same patient and therefore added the ABCC to receive a copy of the report.

[29] In this incident, this lab result was sent electronically to the SCA. The SHA confirmed that the record had been deleted from its system.

[30] During its further investigation, the SHA determined that the breach occurred as a result of the secondary search which subsequently identified a link to a former patient who had a reportable cancer or cancer-related concern; and the lab employee did not verify the patient information before copying the ABCC on the report.

[31] I find that the SHA adequately investigated the breach.

Prevent future privacy breaches

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

[33] New procedures have been implemented where the Lab searches on the Medical Record Number (MRN) rather than the HSN in SLRR. The MRN is a unique identifier that is assigned to every patient regardless if they are from out-of-province or not. This process will prevent this type of breach from occurring again by ensuring the correct patient is identified.

[34] Privacy education refresh courses were be rolled out for 2018/19 for the employees of the SHA.

[35] I find that the SHA has made sufficient changes to prevent further breaches.

Write an investigation report

[36] 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.

[37] SHA provided my office with its internal investigation report which described how the breach occurred, how it responded to the breaches, and steps it took to prevent similar privacy breaches.

[38] I find that the SHA appropriately documented the privacy breach.

III FINDINGS

[39] I find that HIPA is engaged.

[40] I find that a breach occurred when the SHA failed to verify the identity of the patient.

[41] I find that the privacy breach had been contained.

[42] I find that the SHA made a reasonable attempt to notify the affected individual.

[43] I find that the SHA adequately investigated the breach.

[44] I find that the SHA has made sufficient changes to prevent further breaches of this type.

[45] I find that the SHA appropriately documented the privacy breach.

IV RECOMMENDATION

[46] I recommend that the SHA take no further action.

Dated at Regina, in the Province of Saskatchewan, this 11th day of December, 2019.

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