Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 066-2018

Saskatchewan Health Authority

April 27, 2018

Summary: Through the investigation, the Commissioner found that an Employee in the Finance Department of the Saskatchewan Health Authority (SHA) inappropriately accessed the personal health information of a new companion of the Employee's former partner. The Commissioner found that the Employee did so despite the confidentiality agreement that the Employee signed. The Commissioner recommended that all employees receive annual privacy training and sign annual confidentiality agreements.

I BACKGROUND

[1] An individual (Individual A) contacted a Saskatchewan Health Authority (SHA) privacy officer in Saskatoon on March 20, 2018. Individual A's former partner was an employee in the Finance Department for the SHA in Saskatoon (the Employee). Individual A was concerned that the Employee was accessing personal health information of Individual A's new partner (Individual B). Individual A and B provided the SHA with an e-mail written by the Employee, which stated Individual B's surgery "wasn't that invasive" as evidence of the access.

[2] The SHA investigated the matter and proactively reported the matter to my office on April 11, 2018.

II DISCUSSION OF THE ISSUES

1. Does HIPA apply in these circumstances?

[3] *The Health Information Protection Act* (HIPA) applies in full when three elements are present. The first element is personal health information, the second element is a trustee, and the third element is if the personal health information is in the custody or control of the trustee.

[4] Personal health information is defined in subsection 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;
> …
> (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] In its internal investigation report, the SHA indicated that the Employee accessed the personal health information of Individual B in an application call Enovation. The SHA has indicated that Enovation holds information such as registration information, information about a presenting complaint, diagnosis and treatment. This information qualifies as personal health information pursuant to subsections 2(m)(i), (ii), (iv) and (v) of HIPA.

[6] The SHA qualifies as a trustee pursuant to subsection 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;

[7] The SHA had custody and control of the personal health information in question. I find HIPA applies.

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

[8] In circumstances where there is no dispute that a privacy breach has occurred, the focus for my office becomes one of determining whether the trustee has appropriately handled the privacy breach. 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's resource, *IPC Guide to HIPA*, recommends five best practice steps be taken by a trustee when responding to privacy breaches. 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 a privacy breach report.

[9] I will use these steps to assess the SHA's response to the breach.

Contain the Breach

[10] Upon learning that a privacy breach has occurred, trustees should immediately take steps to contain the breach. Depending on the nature of the breach, this can include:

a. Stopping the unauthorized practice;
b. Recovering the records;
c. Shutting down the system that has been breached;
d. Revoking access privileges; or
e. Correcting weaknesses in physical security.

[11] The Privacy Officer contacted the supervisor in the Finance Department after learning of the breach on March 20, 2018. The supervisor confirmed that the Employee had access to Enovation. The supervisor indicated that the Employee would have no reason to access the personal health information in question for the purpose of the Employee's work.

[12] The SHA indicated that it ceased using Enovation on April 7, 2018.

[13] The SHA proceeded to interview with the Employee on April 4, 2018. Privacy obligations were discussed at this time.

[14] At the time I issued this report, the SHA had not yet made a decision with respect to further actions. The Employee does not have any future shifts scheduled.

Notify affected individuals and/or appropriate organizations

[15] Notifying an individual that their personal health information has been 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, trustees should always notify affected individuals.

[16] In this case, the SHA was alerted to the breach by Individual A and Individual B. There was no need to provide further notification.

[17] The SHA notified my office of this matter.

Investigate the breach

[18] Once the breach has been contained and appropriate notification has occurred, the trustee should conduct an internal investigation. The investigation is generally conducted by the trustee's privacy officer 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. It should also consider whether the safeguards that were in place at the time of the incident were adequate. 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.

[19] Section 16 of HIPA imposes the following duty to protect personal health information on trustees:

> **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the integrity, accuracy and confidentiality of the information;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the information;
>
> (ii) loss of the information; or
>
> (iii) unauthorized access to or use, disclosure or modification of the information; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[20] This is supported by the need-to-know principle. The need-to-know principle is the principle that trustees and their staff should only collect, use or disclose personal health information needed for the diagnosis, treatment or care of an individual or other authorized purposes. Personal health information should only be available to those employees in an organization that have a legitimate need-to-know that information, for the purpose of delivering their mandated services. A trustee should limit collection and use of personal health information to what the employee needs-to-know to do their job, not collect or use information that is nice to know.

[21] The SHA interviewed the Employee's supervisor. The supervisor confirmed that the Employee had access to Enovation. The supervisor indicated that the Employee would

have no reason to access the personal health information in question for the purpose of the Employee's work. The supervisor also indicated that the location of the Employee's shifts did not coincide with the health services received by Individual B.

[22] The SHA then interviewed the Employee. The information gained from the interview can be summarized as follows:

- The Employee deals with payment for charges. The Employee answers questions about charges which requires access to Enovation. Sometimes when working at one site, the Employee will take calls and answer questions from patients who received health services at another site.

- The Employee had not received any privacy training from the SHA. The Employee had never heard of HIPA. However, the Employee has signed a confidentiality agreement.

- The Employee had access to three electronic systems containing personal health information: Enovation, Oracle and Nicodemus.

- The Employee confessed to accessing Individual B's personal health information without a need-to-know. The Employee was engaged in a bitter divorce with Individual A and was upset about a situation. This was the reason the Employee gave for snooping.

[23] The SHA also reviewed the safeguards in place at the time Individual B's personal health information was accessed. The SHA confirmed that the Employee signed a confidentiality agreement in 2014.

[24] The SHA indicated the following was in the confidentiality agreement signed by the Employee:

> 3. I will use confidential information only as needed to perform my legitimate duties with the Saskatoon Health Region. This means, doing other things, that:
>
> …
>
> c) I will only access confidential information for which I have a need to know in connection with the services I am providing to the Saskatoon Health Region;
>
> d) I will not misuse confidential information or carelessly care for confidential information.

[25] In its internal investigation report, the SHA also noted the following from *SHR Policy 7311-75-003 Confidentiality - Health Information* which was in place at the time of the access:

> **Section 3.1** All staff are responsible for protecting PHI and SHR business information obtained during the course of his/her work within the region.
>
> **Section 3.2.3** Employees, physicians, volunteers and students shall not use their position at SHR in order to collect or access personal health information that is not required for employment-related purposes.

[26] The SHA reported, however, that the Employee did not have privacy training. It indicated that the Employee began working for the Saskatoon Regional Health Authority prior to HIPA coming into force, although the Employee began work in the Finance Department in the past 5 years.

[27] My office has stated that privacy training is an essential safeguard. I have also found in Investigation Report 320-2017 that a non-clinician employee of the SHA, who did not receive privacy training, may have snooped in personal health information in a similar situation. It is shocking that, almost 15 years after HIPA came into force, there are employees of the SHA which have access to an enormous amount of personal health information that have never received privacy training. It is imperative that all SHA employees that have access to personal health information receive privacy training. Annual privacy training is best practice. SHA employees should also sign annual confidentiality agreements.

[28] The SHA concluded that the Employee intentionally accessed Individual B's personal health information despite the safeguards in place. I am of the same mind. The Employee signed the confidentiality agreement that stated: "I will only access confidential information for which I have a need to know in connection with the services I am providing to the Saskatoon Health Region".

Plan for prevention

[29] The next step is to formulate a plan to avoid future breaches of a similar nature. Some changes that are needed may have revealed themselves to the trustee during the investigation phase, such as deficient policies or procedures, a weakness in the system, a lack of accountability measures or a lack of training. This is an important step in addressing a privacy breach because a privacy breach cannot be undone, but the trustee can learn from it and improve.

[30] The SHA has recommended that all staff in the Finance Department receive privacy training. It has not yet decided on consequences for the Employee.

[31] I recommend that the SHA ensure that all employees who have access to personal health information receive annual privacy training. I also recommend that they sign annual confidentiality agreements.

[32] Finally, I recommend that the Employee receive privacy training before permitted access to any further personal health information in the custody and control of the SHA.

III FINDINGS

[33] I find that the Employee inappropriately accessed the personal health information of Individual B.

[34] I find that the SHA did not have adequate safeguards in place.

IV RECOMMENDATIONS

[35] I recommend that the SHA ensure that all employees who have access to personal health information receive annual privacy training.

[36] I recommend that the SHA ensure that all employees who have access to personal health information sign annual confidentiality agreements.

[37] I recommend that the Employee receive privacy training before permitted access to any further personal health information in the custody and control of the SHA.

Dated at Regina, in the Province of Saskatchewan, this 27th day of April, 2018.

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