Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 320-2017

Saskatchewan Health Authority

April 27, 2018

Summary: Following an audit, the Saskatchewan Health Authority (SHA) discovered that an emergency department Employee inappropriately accessed the personal health information of the new companion of the Employee's former partner. The Employee maintains that someone else used the Employee's account to do so. The Employee had signed a confidentiality agreement that states employees should only access personal health information if there is a need to know. It also states employees should protect user names and passwords. The Commissioner found that it was an inappropriate access of personal health information. The Commissioner recommended that all employees receive annual privacy training and sign annual confidentiality agreements. He also recommended shortening the automatic log out period for Sunrise Clinical Manager.

I BACKGROUND

[1] An individual (Individual A) contacted a Saskatchewan Health Authority (SHA) privacy officer in Saskatoon on November 14, 2017. Individual A's former partner was an employee in the emergency department at a hospital in Saskatoon (the Employee). Individual A was concerned that the Employee was accessing personal health information of both Individual A and Individual A's new partner (Individual B).

[2] The SHA obtained consent from both Individual A and Individual B to run an audit on access of their personal health information in Sunrise Clinical Manager (SCM). The audit concluded that the Employee accessed the personal health information of Individual B that could be found in SCM.

[3] The SHA reported the matter to my office on December 13, 2017.

II DISCUSSION OF THE ISSUES

1. Does HIPA apply in these circumstances?

[4] *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.

[5] 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;

[6] In its internal investigation report, the SHA indicated that the Employee accessed the personal health information of Individual B in SCM. The SHA noted that it was not able to audit specifically what personal health information of Individual B the Employee accessed. However, the SHA has indicated that SCM holds information such as registration information, information about emergency department visits, discharge summaries, a variety of reports (consultations, labs, operating room) and imaging results.

This information qualifies as personal health information pursuant to subsections 2(m)(i), (ii), (iv) and (v) of HIPA.

[7] 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;

[8] The SHA has custody and control of the personal health information in SCM.

[9] However, prior to December 4, 2017, the Saskatoon Regional Health Authority had custody and control of the personal health information in question. At that time, it qualified as a trustee pursuant to subsection 2(t)(ii) of HIPA prior to an amendment made to HIPA which facilitated the creation of the new health authority. I find HIPA applies.

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

[10] 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.

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

Contain the Breach

[12] 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.

[13] Upon receiving the concerns of Individual A and Individual B, the SHA ran an audit. After the audit, it interviewed the Employee on November 20, 2017.

[14] As a result, the Employee received a 20 day suspension. The SHA's reaction to this breach was timely.

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. It reported that it has been in regular contact with Individual B throughout the investigation process. 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 for 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 reported that it began its investigation by interviewing the Employee. It summarized the meeting as follows:

- The Employee had not attended any privacy education sessions, but did acknowledge signing a confidentiality agreement.

- The Employee denied knowing Individual B at the beginning of the interview. The SHA then indicated to the Employee that Individual B had reported that the two had met on occasion. The Employee then acknowledged that they had met.

- When asked, the Employee denied accessing the personal health information of Individual B.

- The Employee offered the theory that someone may have used the Employee's computer. The Employee admitted not consistently logging out of the Employee's account before leaving. The Employee also allows others to use the Employee's account.

[22] The SHA reported that the access from the Employee's account was made before Individual B was discharged from the emergency department. Further, the SHA noted that SCM automatically logs employees off the system only after two hours of inactivity.

[23] The SHA also noted that a previous audit had shown the Employee had accessed the Employee's own personal health information in SCM. This is against SHA policy. The Employee was subsequently warned not to do this.

[24] 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 August 2017.

[25] The SHA noted the following from 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.
>
> 4. I will safeguard and will not disclose or share my passwords, user ID's, clearance badges, access cards, keys or other codes or devices assigned to me (or created by me) that allow me to access confidential information. I accept responsibility for all activities undertaken using such code and devices.

[26] 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.

[27] However, the SHA was unable to point to any privacy training received by the individual. My office has stated that privacy training is an essential safeguard. I have also found in Investigation Report 066-2018 that a non-clinician employee of the SHA, who did not receive privacy training, 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 that 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 cannot make that determination. However, I am also of the view that the Employee should have known that it was inappropriate to access Individual B's personal health information as the Employee did not have a need-to-know. This is expressly noted in clause 3(c) of the confidentiality statement that was signed. Further, the Employee should have known to log out of their user account when stepping away from the computer as this was also agreed to in section 4 of the

confidentiality agreement that was signed. Privacy training by the SHA would have assisted to impress these messages upon the Employee.

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 did not identify any steps it planned to take to prevent future snooping by its employees.

[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] In Investigation Report H-2013-001, my office suggested a log off feature that is in line with the International Organization of Standardization (ISO). The updated ISO/IEC 270002:2013 indicates:

> A good log-on procedure should:
> …
> terminate inactive sessions after a defined period of inactivity, especially in high risk Locations such as public or external areas outside the organization's security management or on mobile devices;

[33] The *American Health Insurance Portability and Accountability Act* (HIPAA) establishes national standards for electronic health care transactions. A benchmark set for HIPAA is a 10-minute period before the logoff capability locks the device and makes information inaccessible. Devices in high-traffic areas might have a logout period of two to three

minutes. (www.hippa.com). I also recommend that the SHA explore shortening the automatic log out period of SCM in this manner.

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

Write a privacy breach report

[35] The SHA has created a privacy breach report.

III FINDINGS

[36] I find that the Employee should have known that it was inappropriate to access Individual B's personal health information as the Employee did not have a need-to-know.

[37] I find that the Employee should have known to log out of the their user account when stepping away from the computer.

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

IV RECOMMENDATIONS

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

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

[41] I recommend that the SHA explore shortening the automatic log out period of SCM to less than ten minutes of inactivity.

[42] I recommend that the Employee receive privacy training before being 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