Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 077-2017

Sherbrooke Community Society Inc. operating as Sherbrooke Community Centre

November 3, 2017

Summary: Two employees of Sherbrooke Community Centre (Sherbrooke) disclosed personal health information to their union in relation to a concern as a result of an adverse event. The Commissioner found that Sherbrooke did not have adequate safeguards in place. He recommended Sherbrooke tailor its privacy policies and procedures, annual confidentiality agreements and enhances its training program. He also recommended Sherbrooke develop a procedure with the union for obtaining personal health information when concerns are raised.

I BACKGROUND

[1] The Saskatoon Regional Health Authority (SRHA) provides access and privacy services to Sherbrooke Community Centre (Sherbrooke), which includes support for responding to a privacy breach.

[2] On January 13, 2017, SRHA proactively reported a privacy breach that occurred at Sherbrooke. On January 11, 2017, two Sherbrooke employees photocopied six Adverse Event Management System (AEMS) reports and five weekly safety meeting records which contained personal health information and one of the patients provided it to their union for the purpose of investigating a concern with adverse events regarding a specific resident. The union is a separate organization from Sherbrooke.

[3] On April 18, 2017, my office provided notification to Sherbrooke of my intention to investigate the matter.

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] SRHA indicated that six AEMS reports were disclosed to the union. The AEMS reports contained the subject individual's full name, physician, provincial health services number and date of birth. Additionally, the form contained the full name, address and phone number of the subject individual's "key contact person". They also contained details of adverse events or near adverse events that occurred while Sherbrooke staff were providing care. There were also five weekly safety meeting reports that were provided to the union. Four of the sheets contain the patient's name and details of the adverse events.

[6] Subsections 2(m)(v) and (q) of HIPA defines registration information and personal health information as follows:

> **2** In this Act:
> …
> (m) "personal health information" means, with respect to an individual, whether living or deceased:
> …
> (ii) information with respect to any health service provided to the individual;
> …
> (v) registration information;
> …
> (q) "registration information" means information about an individual that is collected for the purpose of registering the individual for the provision of health services, and includes the individual's health services number and any other number assigned to the individual as part of a system of unique identifying numbers that is prescribed in the regulations;

[7] The information of the subject individual qualifies as registration information pursuant to subsection 2(q) of HIPA and personal health information pursuant to subsection 2(m)(v) of HIPA. The information in question also describes care provided to the patient. Therefore, it also qualifies as personal health information pursuant to subsection 2(m)(ii) of HIPA.

[8] Next, I must determine if Sherbrooke qualifies as a trustee. Trustee is defined in subsection 2(t) of HIPA. Subsection 2(t)(ii) of HIPA provides:

> 2 In this Act:
> …
> (t) **"trustee"** means any of the following that have custody or control of personal health information:
> …
> (ii) a regional health authority or a health care organization;

[9] Subsection 2(h.1) of HIPA provides:

> 2 In this Act:
> …
> (h.1) "health care organization" means a health care organization as defined in *The Regional Health Services Act*;

[10] Subsection 2(h) of *The Regional Health Services Act* defines health care organization and affiliate as follows:

> 2 In this Act:
>
> (a) "affiliate" means a person who, immediately before the coming into force of this section, is the operator of a hospital approved pursuant to *The Hospital Standards Act* or a not-for-profit special-care home licensed pursuant to *The Housing and Special-care Homes Act*, and includes any successor to that operator but does not include a regional health authority or a prescribed person;
> …
> (h) "health care organization" means:
>
> (i) an affiliate; or
>
> (ii) a prescribed person that receives funding from a regional health authority to provide health services;

[11] In addition, the *Saskatoon Health Region Annual Report 2016-2017* lists Sherbrook as an affiliate partner.

[12] Sherbrooke qualifies as a trustee pursuant to subsection 2(t)(ii) of HIPA because it qualifies as a health care organization pursuant to subsections 2(h.1) of HIPA and 2(h) of *The Regional Health Services Act*.

[13] Finally, the personal health information was in the custody of Sherbrooke at the time of the breach. All elements are present and HIPA is engaged.

2. Did Sherbrooke follow best practices in its response to this privacy breach?

[14] 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 Sherbrooke 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.

[15] I will use these steps to assess Sherbrooke's response to the breach.

Contain the Breach

[16] 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:

- Stopping the unauthorized practice;
- Recovering the records;

- Shutting down the system that has been breached;
- Revoking access privileges; or
- Correcting weaknesses in physical security.

[17] The SRHA reported that Sherbrooke retrieved the personal health information from the union and ensured no copies of the personal health information were kept. I am satisfied the breach was contained.

Notify affected individuals and/or appropriate organizations

[18] 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.

[19] The SHRA indicated that the affected individual's substitute decision maker was made aware of the incident.

[20] It is also best practice to proactively report privacy breaches to my office so that my office may offer advice and monitoring of the trustee's response to the incident. SRHA reported the incident to my office on behalf of Sherbrooke.

Investigate the breach

[21] 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.

[22] SRHA provided a copy of its Privacy Incident Overview report to my office. SRHA's report concluded that the Sherbrooke employees did not follow SRHA policies. It also indicated that some of the responsibility fell on the union for asking individual employees for copies of personal health information and not following the formal agreement with SRHA.

[23] I will first examine what safeguards were in place at the time of the breach. Section 16 of HIPA requires that trustees maintain administrative, technical and physical safeguards to protect personal health information. It provides:

> **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.

[24] One of the most important safeguards a trustee should have in place is written privacy policies and procedures. I note that, during the course of my investigation, my office has received mixed messages about Sherbrooke's policies and procedures. Initially, my office was informed that Sherbrooke follows SHRA policies. SRHA indicated that Sherbrooke provides a link to SRHA's privacy policies.

[25] SHRA then provided me with its letter of agreement with Sherbrooke dated February 18, 2017. The letter describes what access and privacy services SRHA will provide to Sherbrooke. SRHA's access and privacy officers are appointed as privacy officers for

Sherbrooke. The letter explicitly states that Sherbrooke "is the trustee of personal health information collected under *The Health Information and Protection Act*." Further, the letter states:

> The Affiliate must have policies and procedures in place to address privacy and confidentiality. These policies and procedures must outline the consequences to Affiliate employees if they have been found to have breached personal health information or personal information.

[26] However, my office was later informed that SRHA's policy has been in Sherbrooke's general Policy and Procedure manual since 2011. My office was provided with a copy. It is similar to the SRHA's policy and procedure with "SHEREBROOKE GENERAL POLICY MANUAL NUMBER: 50.05.1" typed in the upper margin. The policy states that its scope covers the SRHA and Affiliates.

[27] Privacy policies and procedures are a fundamental safeguard. I am not persuaded that simply adopting a different organization's privacy procedure without any tailoring satisfies the requirements of either HIPA or the letter of agreement. There are a number of reasons why.

[28] First, I note that SRHA's privacy policy indicates it was first approved on June 3, 2015. However, Sherbrooke appears to be working with a copy of the document dated April 2, 2012.

[29] Further, the following two excerpts from SRHA's privacy policy are obvious examples of why this practice is problematic:

> **1. PURPOSE**
> The purpose of this policy is to outline responsibilities to ensure our patients' personal health information (PHI) and Saskatoon Health Region (SHR) business information is protected during collection, use, disclosure, storage, and destruction. Information will be protected in accordance with *The Health Information Protection Act* (HIPA), *The Local Authority Freedom of Information and Protection Privacy Act* (LA FOIP) and other relevant legislation.

> **2. PRINCIPLES**
> **2.1 Accountability –** SHR is responsible for PHI and personal information (PI) under its control. SHR has designated a Privacy Officer who is accountable for compliance with the following principles.

[30] These excerpts make it seem like this policy applies only to personal health information in the control of SRHA. Alternatively, given the context of the situation, it could be interpreted by some that SRHA has control of personal health information that is in Sherbrooke's custody or control. I note that SRHA and Sherbrooke are different entities under HIPA. Also, SRHA's incident report that was originally submitted to my office explicitly noted that SRHA was the trustee with custody or control of the personal health information in question. It has since clarified its position that Sherbrooke is the trustee with custody and control of the personal health information in question.

[31] There is no document that signals to Sherbrooke employees that they must protect personal health information in Sherbrooke's custody and control.

[32] My office also asked if the two employees in question had received privacy training and whether the training covered secondary purposes such as those described in subsection 27(4) of HIPA. SRHA reported that each of the two employees had received privacy training every year since 2010, but not from SRHA. It provided me with two slide decks that were used in the training received by the employees. The most recent slide deck did not cover secondary purpose, or many of the topics that I would expect in privacy training related to HIPA. The older slide deck, last updated in 2012, did indicate that personal health information could be used or disclosed for the provision of services (care and treatment) or for the reason the personal health information was obtained with deemed consent and for limited purposes listed in HIPA and the Regulations without consent. The slide deck reminds individual to ask a supervisor, manager or privacy officer if ever in doubt. It also indicates that employees should follow their organization's policies and procedures.

[33] The situations where personal health information may be disclosed without consent, as referenced in the slide deck are mainly found in subsection 27(4) of HIPA which provides:

> 27(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

[34] In cases where disclosure is made without consent, trustees must take extra care to make sure all of the conditions described in the relevant clauses under subsection 27(4) of HIPA have been met. As such, it should be the role of employees of the trustee with proper training and authority to make such a decision and not rogue employees. My office has recently encountered a number of situations where employees of trustees have disclosed personal health information to unions or regulatory bodies without approval of the trustee organization (Investigation Report 021-2017, 067-2017 & 068-2017). Although the training provided to the two employees in question skimmed the topic, I recommend that Sherbrooke, and all trustees, emphasize these types of disclosures in their training.

[35] Sherbrooke also stated that their employees sign the same confidentiality agreement as SRHA employees. Again, the agreement that Sherbrooke employees sign applies to information in connection to duties and services performed for the SRHA. This would not apply to personal health information in Sherbrooke's custody or control.

[36] With respect to policies, procedures and the confidentiality agreement, I find Sherbrooke did not have adequate safeguards in place.

[37] SRHA also described a formal arrangement it had with the union where by the union would request personal health information from SRHA if required to address a concern. SRHA did not indicate whether the agreement specifically included personal health information from Sherbrooke. The goal of this agreement is to give SRHA, as the trustee of the personal health information, opportunity to decide whether disclosure is authorized by HIPA.

[38] The union does not qualify as a trustee pursuant to HIPA. The union does have an interest in protecting Sherbrooke employees by ensuring they do not violate HIPA. However, HIPA imposes the responsibility of protecting the personal health information on Sherbrooke. That did not occur in this case. I recommend Sherbrooke discuss with the union the procedure for obtaining personal health information when concerns are raised. If possible, this should be formalized into a memorandum of understanding. Nevertheless, subsection 16(c) requires Sherbrooke to ensure its employees comply with HIPA.

Plan for prevention

[39] 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.

[40] SRHA's report concluded that the best plan for prevention would be to work with the union to train union employees not to ask for personal health information directly from Sherbrooke employees. As noted, a memorandum of understanding between Sherbrooke and the union would be beneficial.

[41] However, Sherbrooke should have safeguards in place to ensure that it is complying with subsection 16(c) of HIPA as discussed above.

Write a privacy breach report

[42] SRHA completed a Privacy Incident Overview report on behalf of Sherbrooke.

[43] Our province is moving to a single health authority on December 4, 2017. I would hope that SRHA and Sherbrooke would bring these recommendations to the attention of the new authority. There will be a need for the new health authority to revisit all agreements

with affiliates in all the existing health regions. There is an opportunity to make the agreements consistent in terms of how affiliates work with the new health authority.

III FINDING

[44] I find that Sherbrooke did not have appropriate safeguards in place, as required by subsection 16(c) of HIPA.

IV RECOMMENDATIONS

[45] I recommend that Sherbrooke ensure it has adequate safeguards in place. This includes:

- tailoring privacy policies and procedures as discussed in this report;
- enhance its training program to provide special emphasis on disclosures pursuant to subsection 27(4) of HIPA; and
- a requirement that employees sign annual confidentiality agreements specific to Sherbrooke.

[46] I recommend Sherbrooke discuss with the union the procedure for obtaining personal health information when concerns are raised and formalize by way of a memorandum of understanding.

Dated at Regina, in the Province of Saskatchewan, this 3rd day of November, 2017.

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