Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 292-2018

Saskatoon Sexual Health

January 14, 2020

Summary: Saskatoon Sexual Health (SSH) proactively reported a privacy breach in which a password-protected laptop containing a file with client information was stolen. The Commissioner found that SSH is a "trustee" pursuant to *The Health Information Protection Act*, and was satisfied with how SSH managed the breach. The Commissioner recommended that SSH ensure its policies and procedures acknowledge HIPA as its guiding legislation, and that it make annual privacy training/refreshers available to its staff.

I BACKGROUND

[1] On November 19, 2018, Saskatoon Sexual Health (SSH) emailed my office to provide details of a privacy breach that had occurred on November 15, 2018. The privacy breach involved the theft of an office laptop that contained files, dated between January 1, 2016 and July 15, 2018, with personal information and personal health information of 156 SSH clients.

[2] On November 27, 2018, my office contacted SSH to ask it for further information to help determine if SSH is a trustee pursuant to *The Health Information Protection Act* (HIPA), to which SSH responded on November 29, 2018. On the same date, it also provided my office with the following documents:

- A copy of its Data Sharing Agreement with eHealth for "Non-trustee access" to the EHR viewer, which is "a secure website for Saskatchewan health care providers to access patient information regardless of where an individual presents for care"; and

- A copy of its agreement with the Ministry of Health (Medical Services Branch), dated September 2, 2016 (for a term up to March 31, 2019) for funding to provide physician services at SSH.

[3] On December 13, 2018, my office determined that it would open an investigation file and notified the SSH on the same date. On December 14, 2018, my office confirmed with SSH that the purpose of the investigation would be to determine if SSH, pursuant to HIPA, is a "trustee"; if so, this would help determine if my office has jurisdiction to conduct an investigation.

[4] On January 22, 2019, SSH provided my office with a copy of a legal opinion it had received from its solicitor regarding the "protocol you [SSH] followed after a break in incident at your office in Saskatoon on November 15, 2018". The report noted that with respect to the breach, the SSH followed a privacy breach protocol that is consistent with HIPA.

[5] To further my office's investigation, the following information was collected from SSH and other sources:

- May 6, 2019 – SSH provided my office with information on its connection to Action Canada, which describes itself as a "progressive, pro-choice charitable organization committed to advancing and upholding sexual reproductive health and rights in Canada and globally".

- May 10, 2019 – Information Services Corporation provided my office a copy of SSH's "Corporate Registry Profile Report" and a copy of a "Non-profit Corporations Act – Articles of Amendment" statement.

- November 20, 2019 – SSH provided my office with a copy of its "Articles of Incorporation" pursuant to *The Non-profit Corporations Act*. Included are an amendment dated June 1, 2006, recognizing a name change (effective September 1, 2006) from "Planned Parenthood Saskatoon Centre INC" to "Sexual Health Centre Saskatoon INC".

- December 9, 2019 – the Ministry of Health provided my office with a copy of SSH's Medical Laboratory License, issued pursuant to *The Medical Laboratory Licensing Act*.

II DISCUSSION OF THE ISSUES

1. Does HIPA apply?

[6] For HIPA to apply, there must be three elements present: 1) a trustee; 2) personal health information; and 3) the trustee must have custody or control over the personal health information. I must first determine if SSH qualifies as a trustee.

[7] With respect to the definition of "trustee", subsection 2(t)(viii) of HIPA provides:

> **2** In this Act:
>
> …
>
> (t) "trustee" means any of the following that have custody or control of personal health information:
>
> …
>
> (viii) a licensee as defined in *The Medical Laboratory Licensing Act, 1994*;

[8] As SSH is licensed by the Ministry of Health to provide on-site medical laboratory testing pursuant to *The Medical Laboratory Licensing Act*, *1994*, it is a trustee.

[9] With respect to "personal health information", HIPA provides:

> **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;
>
> …
>
> (iv) information that is collected:
>
> (A) in the course of providing health services to the individual; or
>
> …
>
> (v) registration information;

[10] Upon review of the information provided to my office by SSH, I note that the type of information breached contained the following data elements: client full name; personal health number; date of birth; home address; and treatment information. This constitutes personal health information pursuant to subsections 2(m)(ii), (iv) and (v); thus, personal health information is involved, and was in custody or control of SSH. I find that SSH is a trustee and that HIPA applies.

2. Did SSH respond appropriately to the privacy breach?

[11] Upon establishing that an organization is a trustee pursuant to HIPA and that a breach occurred, my office would normally shift towards analyzing how the organization managed the breach based on its submission and supporting documentation/evidence. Because there was some initial question as to whether or not SSH qualified as a trustee pursuant to HIPA, my office did not ask SSH to provide a formal submission. SSH, however, has willingly provided my office with enough detail and information on how they managed the breach for me to proceed with an analysis. I wish to thank it for its willingness and cooperation in this regard, and also for proactively reporting the breach to my office in the first place.

[12] My office recommends that trustee organizations take a systematic approach to investigating a breach following five best practice steps. These steps, which are outlined in my office's resource, *Privacy Breach Guidelines for Government Institutions and Local Authorities* (May, 2018), include:

1. Contain the breach;
2. Notify the affected individuals and/or appropriate organizations;
3. Investigate the breach;
4. Develop and implement a plan to prevent future breaches; and
5. Complete a report.

Contain the breach

[13] To contain a privacy breach means to prevent it from being ongoing. This is the first step an organization should undertake in managing a privacy breach. This includes taking actions such as recovering records, stopping the unauthorized practice or access, shutting down systems that have been compromised, revoking access privileges and correcting physical weaknesses in applications or software.

[14] The records in question were contained in a password-protected laptop owned by SSH that was stolen when the office was broken into. SSH stated to my office that the electronic records contained scanned copies of patient records that were in paper form. SSH kept the paper version of these documents in a locked cabinet at the back of the building; these were not disturbed during the break in. SSH reported the theft to the police, and advised my office that the "investigation was concluded and closed. No arrests or actions were taken. The laptop was never recovered". SSH also added that it was able to account for all records that were contained on the laptop.

[15] Even though the breach was not contained because the laptop was never recovered, I find that SSH has made reasonable efforts to contain the breach.

Notify the affected individuals and/or appropriate organizations

[16] Another important step in responding to a privacy breach is to notify the affected individuals. This is important for a number of reasons. Not only do individuals have a right to know, but they also have a need to know in order to protect themselves from potential harm that may result from the breach. Unless there are compelling reasons not to, trustees should always provide notification to affected individuals.

[17] SSH provided my office with a copy of the notification letter it provided to clients. Upon review, I note the letter contained information on what occurred, how individuals were affected, what steps the organization was taking to address the breach and prevent future breaches, that it was working with my office on assessing the breach and that individuals

had the right to contact my office, that individuals could contact the organization with concerns, and an apology for what had occurred. These are all elements that I suggest a trustee organization include in a notification, and am pleased to see that SSH included them.

[18] SSH further indicated to my office that because of the nature of the services it provides, some individuals did not want to receive a notification letter at their home. Instead, SSH either provided notice to the individual's private email, or if the client preferred, left it at the verbal notification. SSH began the process of notifying clients within a week of the breach. In follow up, SSH confirmed with my office that it had not received any complaints from the affected individuals regarding the information that was breached.

[19] I find that SSH has provided notification.

Investigate the breach

[20] To investigate a privacy breach is to understand what happened that led to the breach and to identify the root cause. This step helps an organization develop a plan to prevent the same or similar breaches from occurring.

[21] The Executive Director (ED) of SSH became aware of the break-in upon arriving at SSH's premises in the morning. The alarm had gone off twice earlier in the morning, and the police were dispatched for the first alarm. The ED was instructed by the alarm company to not go into the building alone, so the ED did not go into the building until arriving at the premises later on in the morning. Upon arriving, the ED noticed the back door was unlocked. At the time, nothing appeared out of place, but the ED was alerted by staff a short time later that two laptops were missing, one of which contained the client information. To address this, SSH had the building owners reinforce the locks, which is an obvious measure to take if the physical security of a premises is compromised.

[22] In addition, SSH later found that the individuals entered the space using an elevator that has access to the basement, which is normally locked. It was believed that due to human

error, access to the basement was left open. After the break-in, this access was locked off, which is also a helpful measure to take to ensure the physical security of a premises.

[23] It appears that the breach occurred because of an illegal entry to the building, during which the laptop with the personal health information was stolen. SSH did have a security system that alerted them to the entry, but also increased its other physical safeguards in response.

[24] I find that SSH investigated the breach.

Develop and implement a plan to prevent future breaches

[25] While a privacy breach cannot be undone, a trustee can learn from the experience and improve its practices as part of a prevention plan. During the course of an investigation, a trustee may learn about required changes, such as addressing deficient policies or procedures, updating or improving system weaknesses, implementing privacy training and introducing accountability measures.

[26] As I have noted in this Report, one measure SSH took was to increase its physical security. With respect to the personal health information stored on the laptop, SSH advised my office that the information was only intended to be on the laptop temporarily as part of a project to upload client files to a secure, externally-managed electronic medical record (EMR) server. SSH confirmed it has completed its migration process to the EMR, so there are no further client records stored on laptops. For information on increasing the security of mobile devices, I suggest that trustee organizations that store personal health information on them should review my office's resource, *Helpful Tips: Mobile Device Security*. Some tips include adding encryption in addition to having strong passwords, and keeping devices in a locked drawer or cabinet or having a security cable attached to them.

[27] I find that SSH has a plan to prevent future breaches.

[28] Through the materials and information that SSH has provided my office, SSH appears to observe many best practices with respect to having administrative and technical safeguards in place, for which I commend them. These include:

- allowing only clinical staff to access the EMR, and having information in the EMR further restricted by role (e.g. nurse or doctor) (i.e. "need to know" restrictions on information);
- having staff sign a confidentiality agreement in which they acknowledge their employment may be terminated if they violate the agreement; and
- having a formal confidentiality/privacy policy in place.

[29] I would recommend, however, that since SSH is a trustee pursuant to HIPA that its policies and procedures acknowledge HIPA as its guiding legislation, and that SSH makes available to all staff annual privacy training and/or refreshers. SSH noted that professionals who work within its organization are subject to the requirements of their professional licensing bodies. Although a licensing body may have an expectation of, or a regulatory requirement for, maintaining confidentiality, they would likely not provide specific training on HIPA to its members. The trustee, and not an outside agency, is responsible to ensure its employees, through organizational training, adhere to HIPA and are aware of the organization's responsibilities and obligations under HIPA.

Complete a report

[30] Documenting a trustee organization's investigation into a privacy breach is a method to ensure the organization follows through with its prevention plans.

[31] I find that the SSH has provided my office with the necessary information to enable my office to undertake and complete its analysis. I am satisfied with the information that SSH has provided to my office regarding this breach, and again commend it for its efforts to have in place many appropriate safeguards.

III FINDING

[32] I find that SSH is a trustee and that HIPA applies.

[33] I find that SSH has made reasonable efforts to contain the breach.

[34] I find that SSH has provided notification.

[35] I find that SSH investigated the breach.

[36] I find that SSH has a plan to prevent future breaches.

[37] I find that SSH has provided my office with the necessary information to enable my office to undertake and complete its analysis.

IV RECOMMENDATION

[38] I recommend that SSH ensures its policies and procedures acknowledge HIPA as its organization's guiding legislation, and that SSH makes available to all staff annual privacy training and/or refreshers.

Dated at Regina, in the Province of Saskatchewan, this 14th day of January, 2020.

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