Date: November 25, 2014

SASKATCHEWAN
INFORMATION AND PRIVACY COMMISSIONER

INVESTIGATION REPORT 038/2014

Sunrise Regional Health Authority

Summary: Sunrise Regional Health Authority (Sunrise) was unable to locate the paper chart containing personal health information of one of its employees. The chart was specific to its Women's Wellness Centre (WWC) location. The Commissioner found that the WWC did not have sufficient safeguards in place to protect the chart against reasonably anticipated loss as required by subsection 16(1)(b)(ii) of *The Health Information Protection Act* (HIPA). He recommended that Sunrise update its policies and procedures so they provide clear direction. He also recommended Sunrise introduce a new policy and procedure regarding employees accessing their own personal health information under the custody or control of the region.

I BACKGROUND

[1] An employee of Sunrise Regional Health Authority (Sunrise) discovered the complainant's chart was missing when she went to locate it on July 17, 2013. This chart was a paper file and specific to Sunrise's Women's Wellness Centre (WWC) location. Sunrise's Privacy Officer was informed on July 19, 2013 and a search was performed on July 31, 2013.

[2] Sunrise notified the complainant of the loss of the chart via letter on August 13, 2013. The complainant then made a written complaint dated February 15, 2014 to my office. This office notified Sunrise and the Complainant of our intention to undertake a review on April 10, 2014. We received two submissions from Sunrise.

II DISCUSSION OF THE ISSUES

1. Does HIPA apply?

[3] *The Health Information Protection Act* (HIPA) applies 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] The complainant's chart contained records which qualified as personal health information pursuant to subsection 2(m) of HIPA. Sunrise qualifies as a trustee pursuant to subsection 2(t)(ii) of HIPA. The complainant's chart was located in Sunrise's WWC. As such, it was in the custody and under the control of Sunrise and HIPA applies.

[5] In her letter, the complainant also objected to the fact that so many people knew her chart was missing once the search began. The fact that her chart was missing would not qualify as personal health information and is not at issue in this investigation.

2. Does the loss of the complainant's personal health information constitute a breach of HIPA?

[6] Subsection 16(b)(ii) of HIPA places a duty on trustees to protect personal health information against reasonably anticipated loss. Subsection 16(b)(iii) of HIPA also places a duty to protect personal health information against reasonably anticipated unauthorized access to, use, disclosure or modification.

[7] It is this office's mandate to carry out investigations with respect to personal health information to assist trustees in complying with HIPA. As such, this investigation will focus on Sunrise's safeguards and whether they comply with section 16 of HIPA to reasonably protect personal health information against anticipated loss access to, use, disclosure or modification.

[8] Both parties have presented theories as to what occurred to the chart containing the complainant's personal health information. However, there is not enough evidence to come to a conclusion. Again, an analysis of Sunrise's safeguards will be performed to determine if the complainant's personal health information was reasonably protected against loss.

[9] The first step is to examine the safeguards that were in place at the time the complainant's personal health information was lost. With its submissions, Sunrise provided three relevant policies and procedures: *Patient/Client Record Control*, *Lost or Stolen Client Records or other Personal Health Information* and *Protecting Client Records During Transportation.*

[10] The *Patient/Client Record Control* policy and procedure is most relevant as it describes how personal health information is to be secured.

[11] Our office asked in a letter dated June 19, 2014 whether the WWC had a system of tracking patient records when they were in use. In reply, it referred to the *Patient/Client Record Control* policy and procedure. Steps 3 and 4 of the procedure require the following:

> 3. A system for controlling charge out and return of patient/client records will be in effect both during normal business hours and in after hour emergency situations, when users are expected to provide emergency care.
> 4. For each patient/client record retrieved and leaving the permanent filing area, an adequate system, either manual or computerized will be in place to monitor the location of the record and allow for its retrieval if necessary. The system will include:
>
> 4.1. Chart number (if chart numbers are used)
> 4.2. Patient/client name
> 4.3. Date removed
> 4.4. Destination or to whom
> 4.5. Date patient/client record returned

[12] Sunrise's submissions did not refer to any specific tracking system that may have been in place in the WWC or what the tracking system indicated with respect to the complainant's file.

[13] Further, the *Patient/Client Record Control* policy also indicates that "Health information while in active use must be in the immediate care and control of designated persons or areas." It also states "Control of the patient/client record is a duty and designated staff is responsible for tracking the location of the record at all times." Sunrise's submission did not indicate who the "designated staff" was and what their role in tracking the record in question was.

[14] Given the lack of information provided regarding crucial record control in this case, it appears that the *Patient/Client Record Control* policy was not being followed at the WWC. There has been no indication that any method of tracking patient files was in place as per Sunrise's policy. Our office has stated in the past that having a policy is not sufficient; it must be followed in practice.

[15] Further, the policy is vague. It should provide meaningful direction to staff. To strengthen this policy Sunrise should make the following changes:

- Define key terms such as "permanent filing area", "designated staff", "charge out system".
- Specifically indicate that each repository of patient files (ie. the WWC files) should have a tracking system that fits its needs.
- Assign an individual to be in charge of monitoring patient files for each repository. The policy should mention specific job titles.
- The language of the policy should reflect terminology found in HIPA (ie. personal health information, etc.)

[16] Throughout the course of this investigation, we have learned other practices of the WWC that may have contributed to this lost personal health information and require comment.

[17] Most notably, the employees of the WWC have free access to their own personal health information. Our office has commented in previous reports about the perils of allowing employees to have this free access. We have characterized this as an unauthorized use of personal health information. Employee personal health information is under the custody and control of the trustee, not the employee. Although consent would not be an issue, the employee would only have this free access by virtue of the fact they are an employee. The trustee has a duty to preserve the integrity of personal health information pursuant to section 16 of HIPA and it must protect against potential modifications made by

employees. Further, section 38 of HIPA contemplates situations where individuals could be refused access to their own personal health information. Further, employee personal health information could be intermingled with personal health information of others. Free access could lead to privacy breaches. Policies and procedures are required to guard against all of these issues.

[18] As such, Sunrise should establish a policy restricting employee access to their own personal health information and require that access only be gained through the HIPA procedure.

[19] Secondly, the complainant made allegations about her co-workers accessing her personal health information even though this is not the focus of this investigation. Our office has seen many cases of employees snooping in coworkers' personal health information over the years. In the case of WWC, where there is a smaller staff and paper files are still maintained, we made the suggestion that additional safeguards be put on employee personal health information files. This would include keeping these files in a locked cabinet controlled by a staff person in a position of authority. This would also assist in ensuring that employees do not have free access to their personal health information. However, in the course of this investigation, Sunrise informed us that the WWC has been amalgamated into a new Integrated Primary Health Care Centre. Also, that patient charts were being uploaded in to an Electronic Medical Record (EMR). As such, charts of the employees of the Integrated Primary Health Care Centre should be uploaded to the EMR as soon as possible.

[20] Finally, Sunrise provided a copy of an e-mail dated August 8, 2013 from the Director of Primary Health Care to various Sunrise employees. It states: "Effective immediately client charts will not be removed from the WWC unless authorized by the Director of Primary Health Care and the Region's Privacy Officer." It is unclear what the practice was before this e-mail. Sunrise has a policy entitled *Protecting Client Records During Transportation* which instructs employees on how to take care when taking personal health information off premise. This policy and procedure, however, does not provide guidance on when it is appropriate to take personal health information off premise. The

only direction given by the policy is as follows: “Only authorized Sunrise Health Region staffs are permitted to remove client information from the original storage area. This access must be required in order to provide care or other health-related services ("need-to-know" basis).” The policy does not indicate which staff are “authorized” and how authorization occurs. Sunrise should rewrite this policy more specific and meaningful.

III FINDINGS

[21] I find that Sunrise, in particular the WWC, did not have sufficient safeguards in place to guard against the reasonably anticipated loss of the complainant’s personal health information.

IV RECOMMENDATIONS

[22] I recommend that:

[23] Sunrise change its policies and procedures so that they provide more direction and are more meaningful for employees as described in this draft report.

[24] Sunrise ensure the Integrated Primary Health Care Centre follows all privacy related policies and procedures.

[25] Sunrise establish a policy and procedure regarding employee access to their own personal health information.

[26] Sunrise transfer personal health information of the employees of the Integrated Primary Health Care Centre from paper form to the Electronic Medical Record as soon as possible.

Dated at Regina, in the Province of Saskatchewan, this 25th day of November, 2014.

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