Office of the
Saskatchewan Information
and Privacy Commissioner

# INVESTIGATION REPORT 007-2016

## Saskatoon Regional Health Authority

**June 2, 2016**

**Summary:** Saskatoon Regional Health Authority (SRHA) proactively reported to the Office of the Information and Privacy Commissioner (OIPC) that one of its employees had not followed the appropriate process and allowed an unauthorized research assistant to access personal health information. The Commissioner was satisfied with how SRHA addressed the breach. The Commissioner recommended SRHA report the employee for his conduct in this matter to his professional association.

## I BACKGROUND

[1] On July 23, 2015, Saskatoon Regional Health Authority (SRHA) received an internal email complaint from an employee (a psychologist) alleging that there was an inappropriate access of personal health information located in his office. The employee also copied my office on this email. The email stated:

> I am writing to you to report a breach of privacy under HIPPA. On or between June 24, 2015 at 3:20pm and July 12, 2015 at 12:00pm 18 patient records were stolen from my working office…This included patient names and clinical information about each of these eighteen patients. I believe that the person or persons who stole these files had zero need to know. Furthermore, I believe that the person or persons who stole this information were not clinicians that were actively professionally involved with any of these patients. I would like an investigation of this matter. I would also like to know the outcome.

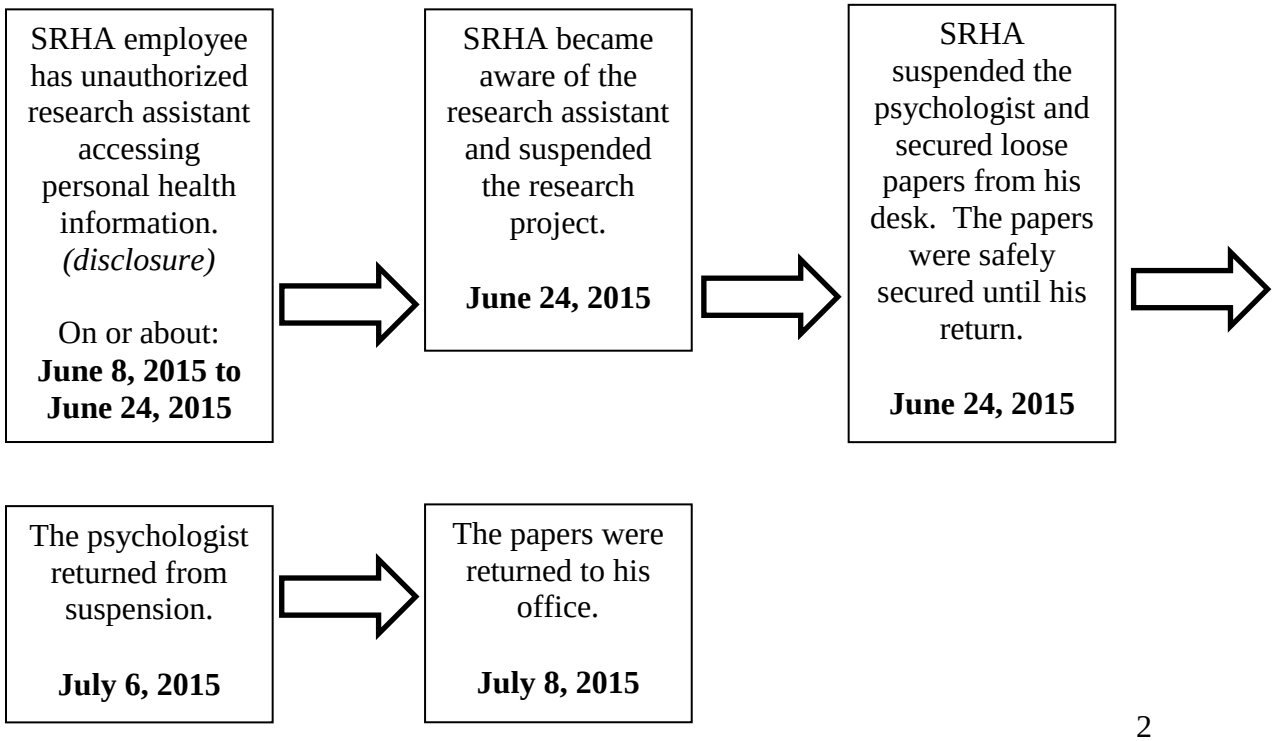
[2] On January 19, 2016, SRHA contacted my office to proactively report a privacy breach. It provided copies of two internal investigation reports related to the above complaint and

a second matter. According to SRHA, the first matter was not a privacy breach but the second matter was. SRHA indicated that the second matter was about the psychologist not following appropriate processes and allowing a research assistant to access SRHA clients, their charts and SRHA property.

[3] On January 20, 2016, my office provided notification to SRHA advising that my office would review its internal privacy breach investigation reports.

[4] On March 16, 2016, the psychologist with SRHA contacted my office. On March 18, 2016, my office spoke with him. He requested that my office issue a public report. There are other issues going on here, such as disagreement between the psychologist and SRHA on whether an agreement was signed, whether there was approval for the research assistant and general conflict between the psychologist and his superiors. However, my office has no jurisdiction to address such issues. These matters are best addressed through the grievance arbitration which SRHA advises is occurring. Therefore, my office can only address whether SRHA appropriately handled the privacy breach.

[5] Based on the information provided by SRHA, the following appears to be the flow of data involving this case:



## II DISCUSSION OF THE ISSUES

### 1. Who is the trustee?

[6] To answer this question, I must first determine whether *The Health Information Protection Act* (HIPA) is engaged on the facts in this case. This requires two things:

1. There must be personal health information involved as defined at subsection 2(m) of HIPA; and

2. There must be a trustee involved as defined at subsection 2(t) of HIPA.

[7] Subsection 2(m) of HIPA defines "personal health information" as follows:

> **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;
>
> (iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of 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;

[8] According to SRHA, the information involved was personal health information of the clients involved in a research project. The research project was regarding Fetal Alcohol Spectrum Disorder (FASD). This project was run out of the SRHA Mental Health and Addictions Outpatient Clinic. The personal health information involved would include

the fact that the individuals were involved in the research project and testing results which would constitute personal health information pursuant to subsection 2(m) of HIPA.

[9] In order for there to be a trustee that is required to comply with HIPA, the organization in question must have two things:

1. The organization must be listed at subsection 2(t) of HIPA; and
2. The organization must have custody and control of the personal health information involved.

[10] Subsection 2(t)(ii) of HIPA provides as follows:

> **2**(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;

[11] Subsection 2(t)(xii) of HIPA provides that employees of a trustee cannot be stand-alone trustees:

> **2**(t) **"trustee"** means any of the following that have custody or control of personal health information:
>
> …
>
> (xii) a person, **other than an employee of a trustee**, who is:
>
> (A) a health professional licensed or registered pursuant to an Act for which the minister is responsible; or
>
> (B) a member of a class of persons designated as health professionals in the regulations;
>
> [emphasis added]

[12] The psychologist is a paid employee of SRHA. Therefore, he would not be a stand-alone trustee under HIPA. However, SRHA is a stand-alone trustee pursuant to subsection 2(t)(ii) of HIPA.

[13] The psychologist argues that the principle investigator is the trustee with custody and control. SRHA advised that the principle investigator is not an employee of SRHA but

works out of a different location than where the client and their personal health information are located. Further, the clients register for the research project through SRHA's Mental Health and Addictions Central Intake and SRHA was paying its employees to conduct work on the research project (e.g. testing, interviewing and collecting personal health information from the clients). The psychologist was analyzing the testing data and providing results to the principle investigator at an off-site location.

[14] *Custody* is the physical possession of a record by the trustee. *Control* is a term used to indicate records that are not in the physical custody of the trustee but are still within the influence of the trustee via another mechanism (i.e. contracted services or a trustee's employees working remotely etc.). Control need only be considered if there is no custody by an organization.

[15] SRHA asserted in its investigation report dated September 24, 2015, that it had custody and control of the client files. SRHA asserted that the clients were registered through SRHA's Mental Health and Addictions Central Intake and seen in its Mental Health Outpatient Clinic. Further, the psychologist is a paid employee of SRHA.

[16] I find that SRHA is the trustee with custody of the client files. Therefore, it has the right to access, collect and subsequently use and/or disclose the personal health information in compliance with HIPA. As I have found SRHA has custody, I do not need to determine if it also had control.

**2. Did SRHA follow best practices in its response to the privacy breach?**

[17] As indicated, SRHA advised my office that there was an unauthorized disclosure of client personal health information when its employee allowed an unauthorized research assistant access to SRHA's clients. SRHA has acknowledged that this constituted a breach of the clients' privacy and proactively disclosed the breach to my office. Therefore, the focus is on whether SRHA appropriately handled the privacy breach. In order to be satisfied, my office would need to be confident that SRHA took the privacy breach seriously and appropriately addressed it. My office's resource, *Privacy Breach*

*Guidelines: Tips for Public Bodies/Trustees Dealing with Privacy Breaches* recommends four best practice steps be taken when responding to privacy breaches. These are:

1. Contain the breach;
2. Notify affected individuals and/or appropriate organizations;
3. Investigate the breach; and
4. Plan for prevention.

[18] I will weigh the appropriateness of SRHA's handling of the privacy breach against these four best practice steps.

***Best Practice Step 1: Contain the breach***

[19] 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.

[20] As the trustee with custody of the personal health information, SRHA has a duty under HIPA to protect the personal health information pursuant to Parts III and IV of HIPA. In particular, section 16 of HIPA requires SRHA to maintain administrative, technical and physical safeguards. These safeguards must protect against any reasonably anticipated threat or hazard to the security or integrity of the information; and the loss of, unauthorized access to, use or disclosure of the information. Section 16 provides as follows:

> **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.

[21] According to SRHA, when the psychologist was suspended, papers were left on his desk and the desk of the unauthorized research assistant. SRHA removed the papers to ensure that they were securely locked away from unauthorized access or loss for the duration of the psychologist's suspension pending investigation. Any other files remained locked in the psychologists office including laptops and files that may have held personal health information.

[22] In conclusion, I am satisfied that SRHA appropriately contained the breach.

***Best Practice Step 2: Notify affected individuals and/or appropriate organizations***

[23] Notifying an individual that their personal information or 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.

[24] In addition to notifying individuals, trustees may want to notify other organizations, for example, my office, law enforcement or other regulatory bodies that oversee particular professions.

[25] In this case, SRHA provided written notification to 18 affected individuals. The affected individuals were the clients involved in the research project. The notification letter alerted the clients that a research assistant was gathering information and interviewing clients for the purpose of an approved study. However, the research assistant had not obtained SRHA authorization to work on the study and had not signed an SRHA

confidentiality agreement. SRHA advised the clients that the study was permanently suspended and the research assistant was no longer associated with SRHA. Further, the employee who permitted the research assistant to assist had been disciplined.

[26] In addition to notifying affected individuals, SRHA alerted my office of the privacy breach.

[27] I am satisfied with the steps taken by SRHA.

***Best Practice Step 3: Investigate the breach***

[28] Once a 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. 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.

[29] According to SRHA's internal privacy breach investigation report, the research assistant was not hired by SRHA or the principal investigator hence she had no authority to meet with, collect personal health information or access client's records. The research assistant was the common law wife of the psychologist. SRHA advised that the research assistant was never approved by the manager, there was no written contract in place prior to her work commencing and she never signed a confidentiality agreement. There is currently grievance arbitration occurring with regards to the psychologist and SRHA related to this matter.

***Best Practice Step 4: Plan for prevention***

[30] The final 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.

[31] SRHA assesses its privacy breaches based on its procedure titled *Privacy and Confidentiality #7311-75-003*, which includes an appendix, titled, *Privacy Violations – Recommended Actions.* The appendix outlines three levels of privacy breaches from unintentional to intentional and malicious. SRHA assessed this privacy breach as a level 3 – intentional and malicious. SRHA's response to this breach with regards to the actions it took with the employee was in compliance with its procedures. SRHA suspended the psychologist for 30 days. In addition, the SRHA will not support a research project with this employee's involvement in the foreseeable future, and are confident this is an unusual circumstance that will not be repeated. The issue does not appear to be one that requires a broader prevention strategy by SRHA.

[32] I am satisfied with the preventative steps being taken by SRHA. In conclusion, I am satisfied overall with the steps taken by SRHA to address the privacy breach.

## III FINDINGS

[33] I find that there is personal health information involved.

[34] I find that SRHA is the trustee with custody of the personal health information involved in this matter.

[35] I find that SRHA took appropriate steps to address the privacy breach.

## IV RECOMMENDATION

[36] Provided it does not violate any law or agreement, I recommend that SRHA report the employee for his conduct in this matter to his professional association.

Dated at Regina, in the Province of Saskatchewan, this 2nd day of June, 2016.

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