Date: November 10, 2014

SASKATCHEWAN
INFORMATION AND PRIVACY COMMISSIONER

INVESTIGATION REPORT 088/2013

Regina Qu'Appelle Regional Health Authority

Summary: The Complainant made an access to information request to the Regina Qu'Appelle Regional Health Authority (RQRHA) for a record that lists who had viewed her personal health information stored electronically by RQRHA. She found that a doctor, who had no involvement in her care but with whom she had an acrimonious relationship, viewed her personal health information. The Commissioner found that *The Health Information Protection Act* did not authorize the doctor's viewing of the Complainant's personal health information. In the course of the investigation, RQRHA made changes to its approach to handling employee/practitioner snooping cases.

I BACKGROUND

[1] The Complainant, who is a nurse at the Regina Qu'Appelle Regional Health Authority (RQRHA), was in a motor vehicle accident. She was admitted into the Regina General Hospital as an inpatient. She became alarmed at the number of people who knew of her accident. Through an access to information request to RQRHA, she obtained a record that listed who had viewed her personal health information stored electronically by RQRHA. The record showed that a doctor at RQRHA (doctor), who had no involvement with her care, viewed her personal health information on September 10, 2012 in the Sunrise Clinical Manager system. Based on her letter dated May 14, 2013 to my office, the Complainant has an acrimonious relationship with the doctor, where they have strong difference of opinion on how to treat patients.

[2] The Complainant submitted privacy complaints to RQRHA and to the College of Physicians and Surgeons of Saskatchewan. In response to her complaint, RQRHA found that the

doctor's viewing of the Complainant's personal health information breached RQRHA policy and the RQRHA Confidentiality Agreement that the doctor signed when he began working at RQRHA. As a result, the doctor signed an Alternative Dispute Resolution (ADR) with RQRHA to resolve matters.

[3] In response to her complaint, the College of Physicians and Surgeons (College) had charged the doctor with unprofessional conduct. However, it withdrew the charge after hearing information regarding the incident, including the apology letter the doctor wrote to the Complainant as well as hearing the doctor's explanation for viewing her personal health information. The College, instead, sent a private letter to the doctor expressing its disapproval of the doctor viewing the Complainant's personal health information.

[4] In her letter dated May 14, 2013, the Complainant asserted she was not pleased with the outcome of her complaints to both RQRHA and the College.

[5] My office determined that RQRHA is the responsible trustee in this case since the doctor is engaged by RQRHA by contract. As such, my office sent a notification letter dated September 27, 2013 to RQRHA advising it would be undertaking an investigation pursuant to subsection 42(1)(c) and 52 of *The Health Information Protection Act* (HIPA).

II DISCUSSION OF THE ISSUES

[6] RQRHA is a trustee as defined by subsection 2(t) of HIPA.

1. Does HIPA apply?

[7] 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.

[8] First, the doctor viewed the Complainant's electronic medical file that contained information regarding the Complainant and the accident. Such information would qualify as personal health information as defined by subsections 2(m)(i), 2(m)(ii), 2(m)(iv), and 2(m)(v). Second, RQRHA would qualify as a trustee as defined by subsection 2(t)(ii). Finally, since the doctor

viewed the personal health information in RQRHA's electronic medical record system called Sunrise, the personal health information is in the custody or control of RQRHA. I find that HIPA applies.

2. Was there an unauthorized use of personal health information?

[9] Use is defined by subsection 2(u) of HIPA, which provides:

> **2** In this Act:
>
> ...
>
> (u) "use" includes reference to or manipulation of personal health information by the trustee that has custody or control of the information, but does not include disclosure to another person or trustee.

[10] Trustees should be using personal health information in accordance with section 26 of HIPA. In his apology letter to the Complainant, the doctor explained that he would normally visit acquaintances who have been admitted into the hospital to offer his support. However, because of their "complex" relationship, he did not feel comfortable visiting the Complainant. That led him to view her electronic medical file. Section 26 of HIPA does not authorize the use of personal health information for such a purpose. I find that this viewing of personal health information - a "use" of the Complainant's personal health information – is an unauthorized use.

3. Is RQRHA's approach in responding to employee/practitioner snooping cases adequate?

[11] As stated in the background section, the doctor signed an ADR agreement with RQRHA. The ADR agreement required the doctor send an apology letter to the Complainant, review RQRHA privacy policies and procedures, re-sign the RQRHA Confidentiality Agreement, re-sign the RQRHA Acknowledgement regarding Information System Security document, attend a privacy course developed by the Saskatchewan Medical Association (SMA), and receive a written reprimand. It also included an acknowledgement by the doctor that he breached the Complainant's privacy. Further, as a result of RQRHA's investigation, it monitored the doctor's activities in the electronic system for six months to prevent a similar incident.

[12] While I acknowledge the efforts RQRHA has undertaken to resolve matters with the doctor, the above isn't enough. This is the fourth case where my office has learned of an employee/practitioner snooping case in RQRHA. My office issued an investigation report in 2013 dealing with three employee/practitioner snooping cases in RQRHA. It reviewed RQRHA's policies, procedures, and training, which resulted in five recommendations to RQRHA. RQRHA agreed to comply with all but one recommendation - the merging of levels II and III of its Privacy Violations – Recommended Actions for Employees. This document outlines the disciplinary approach RQRHA undertakes in dealing with employees who violate patient privacy. Level II deals with privacy violations with a "non-malicious intent" while level III deals with privacy violations with a "malicious intent". RQRHA's non-compliance was because this document is used in other regional health authorities in the province and it felt it was important that there be a consistent disciplinary approach among regional health authorities. Any changes to the document would be contingent upon discussion with other regional health authorities.

[13] If a consistent disciplinary approach is desired, I need to look to the Prairie North Regional Health Authority (PNRHA) and its termination of an employee after it was discovered she had snooped through the personal health information of 99 persons. She had been a health region employee for 25 years with a clean disciplinary record. She asserted the non-malicious intent of "medical curiosity" and the "need to understand" the medical diagnosis of patients whose personal health information she snooped. Arbitrator William F.J. Hood, Q.C. upheld the decision to terminate this particular employee. He noted that the regional health authority "is reposed with a public trust to which it is held accountable. This trust is onerous….The task would be indeed onerous, if not impossible, for the [health region] to rebuild this trust with the community and its employees if the person that committed the breaches was reinstated" (*Health Sciences Association of Saskatchewan and Saskatchewan Association of Health Organizations* [2014] S.L.A.A No. 3).

[14] Trust is what is at stake if employee/practitioner snooping is allowed to persist, not only between the regional health authority and the public, but among employees/practitioners as well. The Complainant on the subject privacy breach is a nurse who now must work with a doctor who snooped into her personal health information. Further, two snooping cases discussed in Investigation Report H-2013-001 dealt with employees snooping into

coworkers' personal health information, one of which where the snooper even went as far as modifying his co-worker's personal health information. Snooping and the modification (or the potential to modify) personal health information can easily lead to dangerous situations where health care providers are relying on inaccurate information to treat patients.

[15] PNRHA approach was very strong in that it resulted in employee termination. Such disciplinary action sends the message to PNRHA employees/practitioner to resist snooping lest they risk termination. PNRHA's employee termination and the arbitration decision that upheld the termination is consistent with other arbitration decisions in other jurisdictions such as Ontario and British Columbia. In one case, the arbitrator stated that zero tolerance should be the norm and only in compelling cases should termination not be the result of unauthorized access (IPC Investigation Report H-2013-001 at [70]).

[16] My office's mandate does not include dictating the disciplinary action a regional health authority uses on its employees/practitioner. However, I must comment that that RQRHA's disciplinary action should be strong enough that it acts as a safeguard in protecting personal health information from snoopers. Four cases of employee/practitioner snooping should give RQRHA sufficient reason to revise its approach in responding to snoopers.

[17] A stronger approach by RQRHA would also be consistent with the direction suggested by the Saskatchewan's Health Records Protection Working Group's recommendation to the Deputy Minister of Health. It recommended that there be a specific snooping offense for employees (or those in service of a trustee) who inappropriately access personal health information be included in HIPA (*Health Records Protection Report*, April 2014).

[18] In the course of this investigation, my office made a number of recommendations that RQRHA agreed to comply with. These recommendations include:

- Monitoring employees who have snooped for a period of years instead of months;
- Reporting to the professional regulatory body to whom the employee/practitioner belongs once the snooping has been investigated and substantiated;
- Sending an alert from its FairWarning application to its Privacy Officer if the doctor accesses the personal health information of the Complainant in the future;

- Work with eHealth Saskatchewan (eHealth) so that eHealth can add the doctor to its auditing and monitoring program for any electronic system eHealth is a trustee for;

- Amend its policies so that employees/practitioners who have snooped will be audited and monitored by RQRHA and eHealth.

[19] My office had also made the recommendation that details of the disciplinary action taken against the employee snooped be disclosed to the affected individual(s) and to all regional health authority employees/practitioners. The disclosure of this information would provide closure to the affected individual(s) but also act as a deterrent to snooping by other employees/practitioners. RQRHA advised it would only provide a non-nominal summary will be made known to all regional health authority employees/practitioners.

III FINDINGS

[20] I find that HIPA applies.

[21] I find that there was an unauthorized use of personal health information.

[22] I find that RQRHA's approach has been strengthened by complying with my office's recommendations.

[23] I find that RQRHA's approach in responding to employee snooping case remains inadequate.

IV RECOMMENDATION

[24] I recommend that RQRHA amend its policies so that details of disciplinary action taken against an employee who snooped is disclosed to affected individual(s) and to regional health authority employees/practitioners.

Dated at Regina, in the Province of Saskatchewan, this 10th day of November, 2014.

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