



INVESTIGATION REPORT 030-2016

Regina Qu'Appelle Regional Health Authority

August 17, 2016

Summary: The Regina Qu'Appelle Regional Health Authority (RQRHA) proactively reported a privacy breach that involved an employee snooping into 97 electronic medical records of 35 individuals. The IPC found that RQRHA did not appropriately respond to the privacy breach and made a number of recommendations for RQRHA to consider in order to respond more appropriately to future privacy breaches.

I BACKGROUND

- [1] On February 25, 2016, the Regina Qu'Appelle Regional Health Authority (RQRHA) contacted my office to proactively report a privacy breach. RQRHA advised that “through a patient driven complaint, a [RQRHA] employee was identified as viewing medical records with no need to know constituting a breach of patient privacy under *The Health Information Protection Act* (HIPA). A broader audit identified approximately 49 instances of improper usage of the Laboratory Information System (LIS) databases. Further auditing is underway and the employee has been placed on administrative leave.”
- [2] The employee is a Medical Lab Assistant in the Phlebotomy unit of the Regina General Hospital. The employee inappropriately accessed personal health information such as Medical Record Number (MRN), patient name, lab orders and ordering physician of the employee's relatives and former spouse among others.

[3] On February 29, 2016, my office provided notification to RQRHA advising that my office would be monitoring the matter and requested RQRHA provide a copy of its internal privacy breach investigation report.

[4] On March 21, 2016, RQRHA provided my office with further details based on its investigation. At this time, RQRHA advised that after completing the audit on the patient driven complaint and finding instances of improper use of personal health information, RQRHA expanded the audit to review the employee's accesses over the past year. Based on that finalized audit, RQRHA advised that it found that the employee had in fact inappropriately viewed 97 medical records of 35 individuals.

II DISCUSSION OF THE ISSUES

[5] RQRHA is a "trustee" pursuant to subsection 2(t)(ii) of *The Health Information Protection Act* (HIPA).

1. Did RQRHA respond appropriately to the privacy breach?

[6] The *IPC Guide to HIPA* includes *Privacy Breach Guidelines* that are specifically geared to trustees and can be found at Appendix C in this resource and recommends the following for responding to a breach of privacy:

- Contain the Breach,
- Notification,
- Investigate the Breach, and
- Prevent Future Breaches

[7] I will consider each of these steps to determine if RQRHA adequately responded to the privacy breach.

i. Contain the breach

[8] After receiving a privacy breach complaint on October 15, 2015 and meeting with the employee and their union representative, RQRHA advised that it placed the snooping employee on a paid administrative leave on January 29, 2016 for one month. This however was over three months after the initial complaint was received leaving the employee with the ability to potentially continue to inappropriately access the medical records of individuals while further auditing took place.

[9] From reviewing RQRHA's investigation report, it is not clear if any other steps were taken prior to placing the employee on leave more than three months after the initial complaint.

ii. Notification

[10] The RQRHA advised that it initiated its investigation after receiving a complaint from an individual on October 15, 2015. Upon inspection of the FairWarning Audit reports, it found that the employee who the complainant was originally concerned about had not viewed the complainant's personal health information. However, the audit report did show another employee's actions as suspicious.

[11] RQRHA advised that on October 20, 2015, it was determined that the employee had viewed the complainant's personal health information five times on September 18, 2015 with no reasonable need-to-know, as the individual "was not receiving care in the hospital and had not been to the hospital outpatients".

[12] On November 2, 2015, RQRHA provided the complainant with the list of employees that had used and viewed her medical records, to determine if a connection existed.

[13] RQRHA also informed my office that it had advised its Labour Relations department and the employee's union regarding the inappropriate accesses. After a meeting with these parties on December 18, 2015, RQRHA agreed to expand the audit of the employee beyond the inappropriate accesses of the complainant's medical information. This audit found further inappropriate accesses by the employee. On January 29, 2016, another

meeting was held with these parties. Following this meeting, the employee was placed on paid administrative leave while a review of the employee's accesses for the past year was conducted to determine if there were any further inappropriate accesses.

[14] RQRHA also chose to proactively report the privacy breach to my office. My office appreciates public bodies proactively reporting and I encourage them to do so as soon as practical after learning of an incident.

[15] It is my understanding that RQRHA was hesitant to provide notification to affected individuals based on the nature of the employee's leave, as the employee had gone from paid administrative leave to a definite leave of absence. However, after a meeting with the employee on July 4, 2016, RQRHA made the decision to provide notification letters to the affected individuals regarding the inappropriate use of their personal health information. I would encourage RQRHA in the future to provide notification of the breach of personal health information to affected individuals as soon as it becomes aware of a breach.

iii. Investigate the breach

[16] RQRHA began their investigation after receiving a complaint from a citizen about concerns that an employee without a need-to-know was accessing their medical record. The employee initially suspected, was found to have not viewed the complainant's personal health information, however a different employee had. After confirming that the concern was valid, RQRHA expanded its investigation to include all accesses by the employee for the last year and found further inappropriate uses.

[17] I commend RQRHA for expanding its investigation to determine if there was a broader systemic issue with inappropriate accesses by the employee rather than simply investigating the concern received from the citizen.

[18] RQRHA advised it had also intended to interview the employee regarding these inappropriate uses of individuals' electronic medical records, however the employee is

currently off on definite leave of absence which has made this not possible because the CUPE Collective Agreement prevents them from doing so. It is my understanding that RQRHA will complete the interview upon the employee's return. Once RQRHA has the opportunity to interview the employee and determine what corrective measures would be appropriate, our office would request that RQRHA update our office with this information.

iv. Prevent future breaches

[19] RQRHA advised that currently the LIS audits are completed weekly but were limited to self-look up. It advised that as of September 5, 2016, the audit capabilities would be expanded to include same last name, multiple lookups of a last name and provide the ability to do deeper random audits. I would ask RQRHA to advise my office when these enhancements are implemented.

[20] RQRHA also advised that a LIS user access form was being drafted to complement the Confidentiality Agreement for all RQRHA employees. However, based on my review of this document it does not appear to contain any references to the employees' responsibilities under HIPA or the offences that could result from contravention of this Act.

[21] RQRHA also advised that it would be implementing privacy focused training for laboratory employees. However, RQRHA did not indicate in the information provided the frequency of this training.

[22] On July 27, 2016, my office provided RQRHA a copy of the draft investigation report regarding this matter.

[23] On August 4, 2016, RQRHA provided my office with further information regarding employee training. They provided a list regarding employees who had taken various E-quizzes. However, while quizzes such as biosafety and fire safety had been taken thus far in 2016, the HIPA column was blank for all employees, indicating the staff had not yet

taken the HIPA E-quiz. I would recommend that RQRHA establish a schedule for privacy focused training annually which must be taken by laboratory employees.

[24] In response to our draft report, RQRHA advised that “for Laboratory employees with user rights in to LIS, the Manager of Regulatory Affairs reviews confidentiality with all new employees”, including having the new employees sign a specific confidentiality agreement.

[25] RQRHA also advised that it would be providing a HIPA refresher for its employees, and that employees are required to complete the training annually. RQRHA advised on August 16, 2016, that this training was currently underway, and was expected to be completed by the end of August.

III FINDINGS

[26] I find that RQRHA did not properly contain the privacy breach in a timely fashion.

[27] I find that RQRHA did not provide notification to affected individuals in a timely manner.

[28] I find that RQRHA did not have adequate auditing practices in place at the time of the privacy breach.

[29] I find that RQRHA did not have an adequate schedule for regular privacy training for its staff.

IV RECOMMENDATIONS

[30] I recommend that RQRHA revise its procedures in responding to a privacy breach to include steps to minimize the risk of the individual continuing to inappropriately access personal health information while an investigation is occurring.

- [31] I recommend that RQRHA enhance its auditing practices of the LIS system and report its progress in this regard to my office in three months.
- [32] I recommend that RQRHA report the disciplinary measures for the employee due to this privacy breach to my office once RQRHA has the opportunity to interview the employee and make that determination.
- [33] I recommend that RQRHA's LIS user access form reference the employee's responsibilities under HIPA and the offence provisions.
- [34] I recommend RQRHA create a schedule and conduct annual privacy training for all employees with access to personal health information in the LIS system and also keep records of attendance.

Dated at Regina, in the Province of Saskatchewan, this 17th day of August, 2016.

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