Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 204-2015 & 015-2016

Prince Albert Parkland Regional Health Authority

April 5, 2016

Summary: Prince Albert Parkland Regional Health Authority (PAPRHA) proactively reported to the Office of the Information Privacy Commissioner (OIPC) that one of its employees had inappropriately accessed the personal health information in the Picture Archiving Communications System (PACS). A number of preventative measures were taken by PAPRHA. The Commissioner was satisfied with how PAPRHA addressed the privacy breach. In addition, one of the affected individuals in the privacy breach complained to the OIPC that the same employee breached his daughter's privacy by testing urine samples in the laboratory at PAPRHA. However, upon investigation, the Commissioner found that *The Health Information Protection Act* (HIPA) was not engaged so the matter could not be addressed under HIPA.

I BACKGROUND

[1] On September 21, 2015, Prince Albert Parkland Regional Health Authority (PAPRHA) received a complaint from an individual alleging that his personal health information was inappropriately accessed by his ex-wife who worked for the health region. PAPRHA investigated the allegation and responded to the Complainant by way of letter dated November 5, 2015 indicating that it had determined that the Complainant's privacy had been breached.

[2] On November 10, 2015, PAPRHA contacted my office to proactively report the privacy breach. According to PAPRHA, the ex-wife is a Combined Laboratory and X-Ray Technologist (CLXT). She had inappropriately accessed the personal health information of her ex-husband and daughter in the Picture Archiving and Communications System

(PACS) between 2012 and 2014. Through an audit of PACS, PAPRHA found that the employee had accessed PACS five times without a legitimate business purpose; two times to look at her ex-husband's personal health information and three times to look at her daughter's. The CLXT works in the Department of Diagnostic Imaging in a hospital laboratory.

[3] On November 16, 2015, my office provided notification to PAPRHA advising that my office would be monitoring as PAPRHA investigated and requested that PAPRHA provide a copy of its internal privacy breach investigation report once completed.

[4] On December 8, 2015, my office received PAPRHA's internal privacy breach investigation report.

[5] On January 31, 2016, my office received a complaint directly from the ex-husband alleging that his ex-wife also took urine samples from his daughter and ran tests on them at the laboratory she works in. The Complainant provided my office with a copy of his original complaint to PAPRHA and its response to him.

[6] On February 2, 2016, my office provided notification to PAPRHA advising that my office would be conducting an investigation into the matter and requested that PAPRHA provide a copy of its internal privacy breach investigation report on the second issue. It was decided that both issues would be addressed in this Investigation Report.

[7] On February 23, 2016, my office received PAPRHA's internal privacy breach investigation report on the second issue. Its report indicated that its investigation found that the incident did not constitute a privacy breach under *The Health Information Protection Act* (HIPA).

II DISCUSSION OF THE ISSUES

1. Is there personal health information involved in this matter?

[8] In order for HIPA to be engaged on the facts in this case, two things must exist:

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.

[9] 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;

[10] PACS is designed for the storage, retrieval and display of diagnostic images including x-rays, computerized tomography (CT), ultrasounds, magnetic resonance imaging (MRI), positron emission tomography (PET), nuclear medicine and bone densitometry.

[11] Based on the investigation reports received from PAPRHA, the type of information involved for the first issue included the Complainant's health services number, type of diagnostic imaging exam information and clinical results. The same type of information was accessed in PACS for the Complainant's daughter. Based on the type of information

involved, it is clear that there would be personal health information involved pursuant to subsections 2(m)(i), (ii), (iv) and (v) of HIPA.

[12] In addition, the information involved for issue two is the results of a urine screen conducted on the Complainant's daughter. The results would constitute personal health information involved pursuant to subsections 2(m)(i) and (iii) of HIPA.

2. Is there a trustee involved?

[13] 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.

[14] 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;

[15] PAPRHA is a regional health authority. However, we must determine whether it has custody and/or control of the personal health information involved in this case.

[16] *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.

[17] For the first issue, the PAPRHA employee accessed PACS to view personal health information about the Complainant and the daughter. This personal health information

exists within a system accessible to the region and it has the right to access, collect and subsequently use and/or disclose personal health information from it in compliance with HIPA. Therefore, it is clear that PAPRHA has custody of the personal health information it accesses within PACS.

[18] For the second issue, the employee brought her daughter's urine sample into work and tested it. In its investigation report, PAPRHA indicated that the urine sample was tested using Chemstrips and not an analyzer. The results were not entered into the Laboratory Information System (LIS), or any other PAPRHA health record. Therefore, PAPRHA asserted that it did not have custody or control of the personal health information.

[19] On February 24, 2016, I contacted PAPRHA and confirmed that no record of any kind was created as a result of the employee testing the urine sample. PAPRHA confirmed that there was no record because of the use of the Chemstrips. Chemstrips are a standard urine test strip that is immersed for a period of time then extracted. The strip itself indicates the results. PAPRHA indicated that the Chemstrip would have been disposed of in the biohazard bin which is picked-up and disposed of twice daily.

[20] Based on what has been provided by PAPRHA, it does not appear that PAPRHA has custody or control of any personal health information involving the Complainant's daughter as it relates to the urine samples or the results of testing them. Therefore, HIPA would not apply. The collection and testing of the daughter's urine samples without a physician's order is a matter of professional conduct (or misconduct) and not a privacy matter under HIPA. My office has no jurisdiction over matters of professional conduct. Therefore, this Investigation Report will only address the first issue.

3. Did PAPRHA follow best practices in its response to the privacy breach?

[21] As indicated, the employee inappropriately accessed the personal health information of her ex-husband and daughter in PACS without a legitimate business purpose. PAPRHA has acknowledged that this constituted a breach of the Complainant's privacy and that of his daughter's. Therefore, there is no dispute on whether there was a privacy breach or

not. Therefore, the focus is on whether PAPRHA appropriately handled the privacy breach. In order to be satisfied, my office would need to be confident that PAPRHA 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.

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

Best Practice Step 1: Contain the breach

[23] 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.

[24] According to PAPRHA, upon learning that the privacy breach had occurred, it provided a written warning to the employee that any such future conduct may result in termination. In addition, the employee attended privacy in-service training and reviewed and re-signed PAPRHA's employee confidentiality pledge. The employee's PACS views will also be randomly audited for the next six months. I find that the breach was appropriately contained by PAPRHA.

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

[25] 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.

[26] 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.

[27] In this case, PAPRHA provided written notification to the Complainant. In addition, it alerted my office of the privacy breach. I am satisfied with the steps taken by PAPRHA to notify the Complainant.

Best Practice Step 3: Investigate the breach

[28] Once the breach has been contained and appropriate notification has occurred, the public body 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] PAPRHA assesses its privacy breaches based on its procedure titled *Privacy: Reporting and Investigating Privacy Breaches #10-10-25P*, which includes an appendix, titled, *Privacy Violations – Recommended Actions for Employers.* The appendix outlines three levels of privacy breaches from unintentional to intentional and malicious. PAPRHA assessed this privacy breach as a level II – intentional but non-malicious. PAPRHA's

response to this breach with regards to the actions it took with the employee was consistent with this appendix.

[30] According to PAPRHA's internal privacy breach investigation report, upon receiving the complaint, it ran audits of PACS, LIS and its Radiology Information System (RIS). RIS does not log "view events" so it cannot be audited for this. However, it does log data alterations such as deletions or additions. The audit revealed no data alterations in RIS. The audits also revealed no unauthorized views in LIS. However, the audit of PACS showed that the employee had inappropriately accessed the Complainant's personal health information on two occasions and the daughter's on three:

- April 21, 2013 (Complainant's record);
- February 7, 2014 (Complainant's record);
- December 14, 2012 (Daughter's record);
- January 12, 2013 (Daughter's record); and
- December 15, 2014 (Daughter's record).

Best Practice Step 4: Plan for prevention

[31] 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.

[32] PAPRHA outlined a number of preventative measures in its internal privacy breach investigation report including:

- Training:
    - Currently, all new employees attend privacy in-service training as part of their orientation;

  - All staff in the Diagnostic Imaging Department at the hospital will receive privacy in-service training again by March 2016;
  - General HIPA and electronic health records privacy training will be delivered on a more regular basis – i.e. monthly at the hospital; and
  - PAPRHA is exploring how to make privacy education more accessible (i.e. on-line training).

- Agreements
  - All staff sign a *Confidentiality Pledge* at the time of hire.
- Policies in place:
  - *Confidentiality Policy #10-10-13; and*
  - *Privacy: Reporting and Investigating Privacy Breaches Policy #10-10-25*
- Procedures in place:
  - *Privacy: Reporting and Investigating Privacy Breaches Procedure #10-10-25 P*.
- Auditing
  - PACS is currently audited monthly;
  - A Work Standard is in place that outlines the audit process; and
  - PAPRHA is working on a policy by the end of March 2016.
- *PACS User Agreements* with employees
  - PAPRHA does not currently use one but the goal is to have one developed by April 30, 2016 and have all employees sign it by September 30, 2016.

[33] I am satisfied with the preventative steps being taken by PAPRHA to prevent similar breaches of this type from occurring again. In conclusion, I am satisfied with the steps taken by PAPRHA to address the privacy breach related to the first issue.

III FINDINGS

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

[35] I find that for the first issue, PAPRHA is the trustee with custody and control of the personal health information contained in PACS.

[36] I find that for the second issue, PAPRHA is not a trustee with custody and control of the personal health information related to the urine screen testing.

[37] I am satisfied with the steps taken by PAPRHA to address the privacy breach related to the first issue.

IV RECOMMENDATIONS

[38] There are no recommendations to be made at this time as I am satisfied with the efforts made by PAPRHA in these circumstances.

Dated at Regina, in the Province of Saskatchewan, this 5th day of April, 2016.

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