



## **INVESTIGATION REPORT 170-2016**

### **Prince Albert Parkland Regional Health Authority (PAPRHA)**

**August 29, 2016**

**Summary:** A former nurse entered the Victoria Hospital with a locum physician and proceeded to provide care to patients. In the course of providing care, the former nurse accessed and made handwritten notes on two patients' charts. This former nurse also had the potential to access other patients' personal health information. The Office of the Information and Privacy Commissioner (IPC) made a number of recommendations, including forwarding this file to the Ministry of Justice, Public Prosecutions Division.

#### **I BACKGROUND**

- [1] On April 23, 2016 and April 24, 2016, a nurse who is a former employee of the Prince Albert Parkland Regional Health Authority (PAPRHA), arrived at the Victoria Hospital and entered the Obstetrics Unit with a locum physician at the Victoria Hospital. She proceeded to provide care to at least two patients.
- [2] In the course of providing care, PAPRHA determined that the nurse accessed two patients' charts and made handwritten notes into the charts. PAPRHA noted that the former nurse would have also had access to the patient assessment board, which contained information about 14 other patients.
- [3] On June 28, 2016, PAPRHA proactively reported this breach to my office. On June 30, 2016, my office notified PAPRHA that it would be monitoring the matter.

## II DISCUSSION OF THE ISSUES

[4] PAPERHA qualifies as a “trustee” as defined by subsection 2(t)(ii) of *The Health Information Protection Act* (HIPA).

### 1. Does the information at issue qualify as personal health information as defined by 2(m) of HIPA?

[5] Subsection 2(m) of HIPA defines “personal health information” as follows:

2(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;

[6] Based on email correspondence between my office and PAPERHA dated July 18, 2016, PAPERHA found the former nurse accessed and made notes on two patients’ charts. I find the information contained within patients’ charts would qualify as personal health information as defined by subsection 2(m) of HIPA.

[7] Further, PAPERHA reported that the nurse had access to the patient assessment board which contained patient names, number of children and pregnancies the patient has had, gestation information, reasons for treatment, and outcome of doctors’ visits. I find that such information also qualifies as personal health information as defined by subsection 2(m) of HIPA.

### 2. Did the PAPERHA follow best practices in its response to this privacy breach?

[8] In circumstances where there is no dispute that a privacy breach has occurred, my office’s focus will be determining whether the trustee has appropriately handled the privacy breach. In order to be satisfied, my office would need to be confident that PAPERHA took the privacy breach seriously and appropriately addressed it. My office’s resource, *Privacy Breach Guidelines* recommends four best practice steps to be taken by public bodies when responding to privacy breaches. These are:

1. Contain the breach,

2. notify affected individuals and/or appropriate organizations,
3. investigate the breach,
4. prevent future breaches.

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

**i. Contain the Breach**

[10] The first step in responding to a privacy breach is containing the breach, which means to stop the unauthorized practice when the trustee learns of it.

[11] In this particular situation, PAPERHA failed to stop the unauthorized access to the personal health information until the former nurse left the hospital on her own. In its internal investigation report, PAPERHA reported that the former nurse was "on and off the ward for much of the 2 days in question". Staff notified the Nurse in Charge and the Nursing Supervisor. The Nursing Supervisor did not come to the Obstetrics Unit because staff felt the situation was settled and did not want the situation to be escalated any further.

[12] In its internal investigation report, PAPERHA acknowledges that it did not follow its Management On-Call Policy. The policy is meant to provide staff with management support in difficult situations including where there may be a law or policy enforcement and an unusual presence.

[13] I find that PAPERHA did not make sufficient effort to follow its own Management On-Call Policy to stop and contain the unauthorized practice while it was occurring.

**ii. Notify affected individuals and/or appropriate organizations**

[14] Notifying an individual that their personal 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 hardship that may result

from the inappropriate access. Unless there is a compelling reason not to, trustees should always notify affected individuals.

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

[16] PAPERHA notified the two patients whose charts were accessed by the former nurse. The notification to these two patients include the following:

- A description of the breach,
- The types of personal health information accessed by the former nurse,
- The actions undertaken by the PAPERHA to address the breach,
- An apology,
- The contact information of the PAPERHA Privacy Officer,
- The contact information of my office.

[17] The notification, though, did not include the detail that the nurse had made handwritten notes on each of these patients' charts. This detail could be meaningful to the affected individuals in determining if they should take action, such as requesting a copy of their charts, so they can ensure accuracy and completeness of their personal health information. Therefore, I find that the notification to the two patients could have been strengthened to include more information.

[18] My office recommended to PAPERHA that it notify the two patients that the former nurse made handwritten notes on each of their charts and to provide them each with a copy of the handwritten notes. In a letter dated August 23, 2016, PAPERHA agreed to do so and that it would also include information about how to request to amend their personal health information under HIPA if they believe their personal health information to be inaccurate and/or incomplete.

[19] PAPERHA also notified the 14 individuals whose personal health information the nurse may have accessed in the patient assessment board. The notification contained the following:

- A description of the breach,

- The types of personal health information that may have been accessed by the former nurse,
- The actions undertaken by the PPRHA to address the breach,
- An apology,
- The contact information of the PPRHA Privacy Officer,
- The contact information of my office.

[20] In addition to the above notifications to affected individuals, the PPRHA notified the Saskatchewan Registered Nurses Association (SRNA) since the former nurse is still registered with the SRNA. I find that PPRHA's notification to the individuals whose personal health information was on the patient assessment board to be sufficient.

### **iii. Investigate the Breach**

[21] In the event of a privacy breach, the public body should conduct an internal investigation. The investigation should be documented in an internal privacy breach investigation report and include a root cause analysis. At the conclusion of its investigation, the public body should have a solid grasp of what occurred.

[22] In its investigation, PPRHA received written accounts of the events that occurred from employees, from the former nurse's lawyer, and from the locum physician.

[23] The handwritten accounts by employees who witnessed the former nurse accessing personal health information and treating patients state the former nurse arrived on the Obstetrics Unit with the locum physician. The former nurse invited a patient into an assessment room and proceeded to conduct an assessment on the patient. When approached by another nurse, the former nurse refused to leave and continued to conduct the assessment upon the patient. Employees reported that the former nurse declared "I don't fucking care" when the nurse in charge told her that she was not to do the assessment. Finally, an employee reported that the locum physician had advised her to sign off on the former nurse's assessment.

[24] The former nurse's account of the events contrasts with the employee's handwritten accounts. My office obtained a letter dated June 6, 2016 written by the former nurse's

lawyer to PAPERHA. The letter was in response to PAPERHA's letter dated May 20, 2016 which banned the nurse from PAPERHA health facilities except in certain circumstances (to be discussed later in this Investigation Report). The June 6, 2016 letter asserts that the nurses present at the Obstetrics Unit did not assist the patient when the patient presented herself at the nurses' desk. Therefore, the former nurse took the patient's chart, led the patient to the assessment room, and attached the patient to the monitor. Then, the former nurse went back to the nurses' desk and stated she believed the patient's membrane ruptured and then offered to ask the patient "the necessary questions". The letter states that at that point, the nurse-in-charge said "I don't think you can do that". The former nurse responded by stating she still had her license. The former nurse stated she believed the nurse-in-charge was referring to her license and was not preventing her from assisting the patient.

[25] The June 6, 2016 letter by the former nurse's lawyer stated the former nurse was quite surprised the nurse-in-charge failed to take control of the situation if the nurse-in-charge objected to the former nurse's actions. Further, the letter states the former nurse's "empathy kicked in and she assisted the patient when no one else wanted to." It goes on to state that the former nurse "believed that she was being of assistance to both the patient and the Health Region, and protecting the latter from liability as a result of the current staff's failure to act".

[26] In terms of the locum physician, PAPERHA contacted the locum physician by telephone on May 10, 2016. According to the telephone notes by the Senior Medical Officer who spoke to the locum physician, the Senior Medical Officer explained to the locum physician the situation, including how employees were reporting that the former nurse conducted assessments and had even written in patients' charts. The locum physician responded as follows:

- the former nurse was her friend and accompanied her,
- the locum physician asserted that the former nurse did not assess or make entries into patients' charts,
- that PAPERHA was informed incorrectly.

- [27] My office obtained a copy of a letter dated June 6, 2016 by the locum physician. The locum physician states that the former nurse “provided transfers” from the Saskatoon Airport to the Victoria Hospital. She stated that the patient presented herself at the nursing station and the former nurse addressed the patient’s concerns while the staff on duty “sat there”. She stated the former nurse had only put the patient on the monitor and filled out the admission form. She asserted that there was “no action or objections” from the staff present.
- [28] Based on my office’s review of the case notes by a Quality Improvement Consultant at PAPRHA, the Obstetrics Unit reviewed the charts of patients that were seen by the locum physician. Initially, my office’s understanding was that PAPRHA determined that the former nurse had written in two patients’ charts but did not sign her name but that PAPRHA had recognized the former nurse’s handwriting. However, in its letter dated August 23, 2016 to my office, PAPRHA asserted that there were four instances where the former nurse had signed her name in one of the charts.
- [29] Also, in an email dated July 20, 2016, PAPRHA provided my office with confirmation that the former nurse’s user account that would have given her access to clinical and network applications have been inactive since the former nurse’s date of termination.
- [30] Based on the above information, even though the account of event of the employees contrast with the accounts of the former nurse and the locum physician, I find the PAPRHA’s investigation allows us to have a good grasp of what occurred. That is, the former nurse accessed personal health information that was contained in paper records.
- [31] The Government of Saskatchewan recently strengthened the offense provisions under HIPA as a signal that it takes the unauthorized access and use of personal health information seriously. My office recommended to PAPRHA that if it had not sent its investigation file to the Ministry of Justice, Public Prosecutions Division yet, it should do so. This would allow prosecutors to further consider whether an offense has been committed by either the former nurse or the locum physician. In its letter dated August 23, 2016, PAPRHA stated it would not forward its investigation file to the Ministry of

Justice because one of the affected individuals had stated she wished to remain anonymous. PAPERHA said that a potential legal proceeding may necessitate the affected individual's involvements, which would be against her wishes. I understand the wishes of one individual but there is also another individual who has not expressed the same sentiment. Referring the matter to Public Prosecutions Division does not necessarily mean the information would be instantly public.

**iv. Prevent future breaches**

[32] The final step in responding to a privacy breach is to formulate a plan to avoid future breaches of a similar nature. Some changes that are needed may have revealed themselves to the public body during the investigation phase such as deficient policies or procedures, a weakness in the system, a lack of accountability measures or lack of training. This is an important step in addressing a privacy breach because a privacy breach cannot be undone but the public body can learn from it and improve.

[33] In terms of prevention, PAPERHA has taken steps to deal specifically with the former nurse and locum physician. It has also taken steps to train staff. Below is an analysis of both approaches.

**i. The former nurse and locum physician**

[34] A letter dated May 20, 2016 was sent to the former nurse. The letter states that the former nurse is not to attend any PAPERHA facilities unless 1) she is receiving a personal assessment or treatment by appointment or on an emergency basis, 2) she is there as a visitor or family member, or 3) she is hired as a private care attendant. PAPERHA also informed the nurse that it was going to notify the SRNA of the matter. In a letter dated August 23, 2016, PAPERHA informed my office that it has indeed forwarded the matter to the SRNA.

[35] While I find the contents of PAPERHA's letter to the former nurse to be appropriate, I note that the PAPERHA should have reminded the former nurse of subsection 64(1)(f) of HIPA,



which provides that no person shall obtain another person's personal health information by falsely representing that she is entitled to the information. Subsection 64(1)(f) of HIPA provides:

64(1) No person shall:

...

(f) obtain another person's personal health information by falsely representing that he or she is entitled to the information.

[36] I find that PAPERHA's letter to the former nurse could have been strengthened by referring to subsection 64(1) of HIPA.

[37] A letter dated June 24, 2016 was sent to the locum physician. The letter advises the locum physician that the former nurse is no longer a member of the nursing staff and reminds the locum physician that only active nursing staff should actually be involved with patients.

[38] While I find that the contents of the letter to the locum physician to be appropriate, I note that PAPERHA should have also reminded the locum physician of subsection 64(3.2) of HIPA, which provides that an individual who is in the service of a trustee may be guilty of an offence if she directs another person to access or use personal health information that is not reasonably required by that individual to carry out a purpose authorized by HIPA. Subsection 64(3.2) of HIPA provides:

64(3.2) An individual who is an employee of or in the service of a trustee and who wilfully accesses or uses or directs another person to access or use personal health information that is not reasonably required by that individual to carry out a purpose authorized pursuant to this Act is guilty of an offence and is liable on summary conviction to a fine of not more than \$50,000, to imprisonment for not more than one year or to both, whether or not the trustee has been prosecuted or convicted.

[39] I find that the contents of PAPERHA's letter to the locum physician could have been strengthened by referring to subsection 64(3.2) of HIPA. In its letter dated August 23, 2016 to my office, PAPERHA informed my office that it would write to the locum physician and remind her of subsection 64(3.2) of HIPA and the relevant bylaws of the College of Physicians and Surgeons of Saskatchewan (the College). It stated that

depending on the locum physician's response, it would consider forwarding its investigation file to the College.

**ii. Training for staff**

[40] On June 29, 2016, the Nursing Unit Manager of the Obstetrics Unit did a safety talk about the escalation of concerns during a huddle. The Nursing Unit Manager plans to continue to raise this topic at future huddles with staff on the Obstetrics Unit.

[41] All staff received information about escalating concerns through PPRHA's electronic communication tool called Basecamp.

[42] Finally, PPRHA is developing an initiative called "Stop the Line". This will become a process where any staff member can stop a procedure if he/she feels that if that procedure is negatively affecting patient safety or negatively impacting efficient operations. PPRHA plans to deliver training to staff for this Stop the Line initiative at the end of this summer or beginning of this fall.

[43] I find that the training that has been and will be delivered to staff to be appropriate.

[44] In addition, my office recommended that PPRHA ensure that all staff, including the Nursing Supervisor referred to in paragraph [11] and security staff, receive training on the Management On-Call Policy. In its letter dated August 23, 2016, PPRHA stated that it would revise its Management On-Call Policy to include privacy breaches as a possible reason to notify the manager on call. It stated that it would educate staff on the policy through "Safety Talk" and the education will include a de-identified scenario involving unauthorized access to personal health information.

**a. Other possible prevention steps**

[45] Although I find that PPRHA is taking steps to empower staff to speak up if they see something that negatively affects patient safety, I find it alarming that the former nurse was able to access personal health information so easily. This suggests that personal

health information can easily be accessed by any person and that PAPRHA's safeguards are inadequate. Section 16 of HIPA requires that trustees have safeguards to protect against unauthorized access to or use, disclosure or modification of personal health information:

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:

...  
(iii) unauthorized access to or use, disclosure or modification of the information;

[46] PAPRHA's internal privacy investigation report states that physical and technical safeguards are "not applicable" in this case. However, I recommend that PAPRHA revisit its physical and technical safeguards to ensure that patient personal health information is only accessed by those with a need-to-know.

### **III FINDINGS**

[47] I find that such information also qualifies as personal health information as defined by subsection 2(m) of HIPA.

[48] I find that PAPRHA did not make sufficient effort to stop and contain the unauthorized practice.

[49] I find that the initial notification to the two affected patients could have been strengthened to include more information.

[50] I find that PAPRHA's notification to the individuals whose personal health information was on the patient assessment board to be sufficient.

[51] I find that PAPRHA's investigation to be adequate.

[52] I find the contents of PAPRHA's letter to the former nurse could have been strengthened by referring to subsection 64(1) of HIPA.

- [53] I find that the contents of PAPERHA's first letter to the locum physician could have been strengthened by referring to subsection 64(3.2) of HIPA.
- [54] I find that the training that has been and will be delivered to staff to be appropriate.
- [55] I find that PAPERHA's safeguards to prevent unauthorized access to or use, disclosure or modification of the information to be inadequate.

#### **IV RECOMMENDATIONS**

- [56] I recommend that PAPERHA request the College of Physicians and Surgeons to consider discipline proceedings against the locum physician.
- [57] I recommend that PAPERHA forward this file to the Ministry of Justice, Public Prosecutions Division, to allow prosecutors to consider whether an offence has occurred and if charges should be laid under HIPA or any other statute.
- [58] I recommend that PAPERHA ensures that all staff, including the Nursing Supervisor referred to in paragraph [11] and security staff, receive training on the Management On-Call Policy.
- [59] I recommend that PAPERHA review all of its safeguards, not just its administrative safeguards, to prevent a similar privacy breach in the future. That is, to prevent any person without a need-to-know, access to a patients' chart.

Dated at Regina, in the Province of Saskatchewan, this 29th day of August, 2016.

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