Office of the
Saskatchewan Information
and Privacy Commissioner

# INVESTIGATION REPORT 239-2017

## Prince Albert Co-operative Health Centre Community Clinic

**March 27, 2018**

**Summary:** A patient and her spouse attended the Prince Albert Co-operative Health Centre Community Clinic (the Clinic) for lab services in relation to the patient's pregnancy. After attending the Clinic, the patient's spouse was notified of a social media post made by an employee of the Clinic that named the patient's spouse and referred to him getting someone pregnant. The spouse and the patient contacted the Clinic advising an employee at the Clinic had disclosed information about the patient's pregnancy to an outside party. The Information and Privacy Commissioner (IPC) found that a privacy breach had occurred and that the Clinic had not adequately investigated. The IPC recommended the Clinic complete its investigation, including interviewing the employee that made the social media post, consider appropriate disciplinary steps for the employee and implement additional policies and procedures.

## I BACKGROUND

[1] On August 30, 2017, a patient attended the Prince Albert Co-operative Health Centre Community Clinic (the Clinic) for lab service in relation to her pregnancy, accompanied by her spouse. On Friday, September 8, 2017, the Clinic contacted my office by phone indicating that the patient's spouse had notified the clinic of an alleged breach of privacy. The spouse indicated that an employee of the Clinic (the employee) had disclosed information about the patient's pregnancy to an outside party. The Clinic indicated it intended to conduct an investigation and meet with the patient and her spouse to obtain additional details about the complaint.

[2] In emails dated September 14 and 20, 2017, the Clinic emailed my office additional details regarding the breach of privacy complaint. The Clinic indicated the patient's spouse alleged the employee had disclosed information about the patient's pregnancy to an outside party without authority. The patient's spouse provided the Clinic with social media posts made by the employee making remarks about the spouse getting someone pregnant and alleging the spouse had told someone he would get her fired if she was to tell anyone about the pregnancy.

[3] During the Clinic's meeting with the patient and the spouse, the spouse also advised that he and the employee were related, but did not have a close relationship. In this meeting, the spouse also informed the Clinic that when the patient and spouse had attended the Clinic, the employee had also made comments about the spouse getting the patient pregnant and other comments of a personal nature.

[4] On September 29, 2017, the Clinic was notified of my office's intentions to undertake an investigation regarding this matter. In the notification, my office requested the Clinic provide my office with a copy of its internal investigation report as well as any policies or procedures related to this matter.

## II DISCUSSION OF THE ISSUES

### 1. Is *The Health Information Protection Act* (HIPA) engaged?

[5] HIPA is engaged when three elements are present: 1) a trustee, 2) personal health information, and 3) the trustee must have custody or control over the personal health information.

[6] The Clinic provided my office with a copy of an agreement between the Minister of Health and the Clinic regarding the delivery of primary health care services. The agreement indicates it will commence April 1, 2017 and will expire March 31, 2020, unless extended by mutual agreement of the parties. Clause 11.3 of this agreement provides the following:

> 11.3 The parties acknowledge that for the purposes of providing the services pursuant to this Agreement, the Clinic may be required to collect and use personal health information from its clients. The Clinic specifically acknowledges that it is a "trustee" within the meaning of *The Health Information Protection Act* and as such agrees to comply with that Act in the course of providing the services.

[7] Subsection 2(t)(xiv) of HIPA provides as follows:

> **2** In this Act:
>
> …
>
> (t) **"trustee"** means any of the following that have custody or control of personal health information:
>
> …
>
> (xiv) a person, other than an employee of a trustee, who or body that provides a health service pursuant to an agreement with another trustee;

[8] As such, I find that the Clinic qualifies as a trustee pursuant to subsection 2(t)(xiv) of HIPA. I find the first requirement is met.

[9] Subsection 2(m) of HIPA defined "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] In its internal investigation report, the Clinic indicated that the patient had attended the clinic for lab work related to her pregnancy. The Clinic indicated the employee had not performed the blood draw, but did process the patient's client lab order. This document would have included the following elements:

- Patient's name;
- Date of birth;
- Gender;
- Ordering physician;
- Name of clinic;
- Client phone number;
- Date of collection; and
- Test to be completed.

[11] It is the patient and spouse's allegation that the employee disclosed information about the patient's pregnancy based on this information, and as such, I find that this incident includes personal health information as defined at subsection 2(m) of HIPA.

[12] Simply because an individual or an organization qualifies as a trustee, it does not mean they would qualify as 'the' trustee of personal health information in every circumstance. In order to determine who 'the' trustee is, in other words the person or organization who has responsibility for the protection of the personal health information in question, the individual or organization must also have custody or control of the personal health information.

[13] As the Clinic collected the personal health information for the purposes of providing a health service, it would have custody and control of the personal health information. As such, the Clinic is 'the' trustee of the personal health information in question.

[14] I find that HIPA applies to this matter.

## 2. Did the Clinic respond appropriately to the privacy breach?

[15] The *IPC Guide to HIPA* (the HIPA Guide) includes privacy breach guidelines that are specifically geared to trustees. Appendix C in the resource recommends the following five steps for responding to a breach of privacy:

- Contain the breach,
- Notification,
- Investigate the breach,
- Prevent future breaches, and
- Privacy breach report.

[16] The clinic has indicated in its internal investigation report that it had reached the conclusion that a breach had not occurred. I will first consider the Clinic's investigation into the incident to consider how the clinic reached the conclusion that there was no breach of privacy.

### *Investigate the breach*

[17] The HIPA Guide provides:

> A privacy breach is often thought of as inappropriate sharing of personal health information. However, a privacy breach can occur in a number of different ways:
> …
>
> ***Use***: A privacy breach could occur when personal health information already in the possession or control of the trustee is used for reasons not consistent with the purpose for which they were collected…
>
> ***Disclosure***: A privacy breach could occur when an unauthorized disclosure of personal health information transpires…

[18] The Clinic advised it had reviewed video surveillance of the day the patient had attended the Clinic and confirmed the spouse and the employee had a conversation that lasted approximately 10 minutes. The Clinic did confirm based on the EMR chart/user audit the employee processed the patient's paperwork and therefore would have had knowledge of the type of lab test that was ordered. Finally, the Clinic had reviewed the screen shots of

the social media post made by the employee that the spouse alleged had revealed the patient was pregnant.

[19] The Clinic advised that based on a review of the social media post, it concluded a breach of privacy had not occurred.

[20] Based on the information provided in its internal investigation report, my office requested additional details about the Clinic's investigation into this matter. This included whether the Clinic had interviewed the employee and whether or not the Clinic was able to verify the nature of the conversation between the spouse and the employee, based on its surveillance records.

[21] The Clinic advised it had not interviewed the employee as the breach was not confirmed. It also indicated that the employee and the patient's spouse had multiple connections in the community and could have heard of the patient's pregnancy from another source. The Clinic also advised that while it was able to confirm the employee and the spouse had a conversation at the Clinic, the surveillance records did not contain audio so it could not confirm the nature of the conversation.

[22] Along with its internal investigation report, the Clinic provided my office with copies of the social media post made by the employee. The Clinic redacted the names and photos but identified who the parties were by labeling whether the post and comments were made by the employee, spouse or a third party. The Clinic advised that the patient's name was not used in the post or the resulting comments.

[23] The social media post includes the initial post made by the employee and the resulting comments on that post by the employee, the patient's spouse and other third parties. It appears the third parties that commented on the employee's social media post included people who were familiar with the patient's spouse and based on the nature of some of the comments, appear to be relatives of the spouse and the employee. The initial post made by the employee names the spouse and allegations that the spouse had threatened to get her

fired. The post and subsequent comments also includes statements by the employee about the spouse getting someone pregnant.

[24] Based on a review of the social media comments provided to my office, the employee was the only individual to make comments of this nature. These comments made by the employee clearly referenced the name of the patient's spouse. It is reasonable that those who viewed the social media post could reach the conclusion that the person the spouse is having a baby with is the patient. Especially since those who commented on the post appear to be familiar with the spouse and therefore likely know about his relationship with the patient.

[25] Based on the social media posts provided, no one else, including the spouse, made any comments that he was having another child. While the Clinic indicates that the Lab Assistant may have gained knowledge of the pregnancy through other sources, the Clinic did not interview the employee to allow the employee the opportunity to confirm or deny this.

[26] Regardless of whether the employee could have also learned the patient was pregnant through sources outside of the Clinic, it has been confirmed the employee would have known of the patient's pregnancy from her employment with the Clinic. It is an inappropriate practice for employees to post information that they would have knowledge of based on their employment with the trustee. Based on the social media post, I would conclude that a patient's personal health information was inappropriately disclosed as it is reasonable that the patient would be identifiable; therefore, a privacy breach has occurred.

[27] As well, the spouse alleged that when the patient and the spouse attended the Clinic for lab services, the employee made comments to the spouse about him getting another woman pregnant and other comment of a personal nature.

[28] As mentioned earlier the Clinic was not able to verify the nature of the conversation or confirm if the employee had made the comments the spouse alleged she had made as the

surveillance records do not include audio. As well, the Clinic did not interview the employee regarding this incident.

[29] An employee should not be disclosing personal health information collected for the purposes of accessing health services as a source of information to make comments of a personal nature. Disclosing the personal health information of the patient for the basis of a conversation of this nature is not an appropriate disclosure of personal health information, as such this would also constitute a privacy breach.

[30] While there are provisions in HIPA that provide trustees with the authority to use and disclose personal health information without the consent of the individual, using personal health information collected for health services to make comments of a personal nature, either in person or on social media, would not be one of those.

[31] As the Clinic has not interviewed the employee about this matter, I find that the Clinic has not adequately investigated this privacy breach complaint.

[32] I recommend the Clinic interview the employee to gain additional details regarding the incident to properly investigate and prevent future occurrences. In the future, the Clinic should conduct interviews with employees that are involved in the alleged breach of privacy at the time a complaint is received, as this would allow employees to more accurately recall details of the incident.

***Contain the breach***

[33] The Guide to HIPA provides that it is important to contain the breach immediately. In other words, ensure that personal health information is no longer at risk. This may involve:

- Stopping the unauthorized practice.
- Recovering the records.
- Shutting down the system that was breached.
- Revoking access to personal health information.
- Correcting weaknesses in physical security.

[34] While the Clinic has taken the position that no breach of privacy has occurred, it has not taken any steps to contain this privacy breach.

[35] When the Clinic interviews the employee regarding this incident, it should also ensure the employee stops the unauthorized practice of making social media posts and personal comments regarding personal health information they have access to based on their employment with the trustee.

[36] Once the clinic has conducted its interview with the employee and completed its investigation, the Clinic should also consider an appropriate level of disciplinary action for the employee.

***Notification***

[37] The HIPA Guide provides that notification should include the following:

- A description of the breach (a general description of what happened).
- A detailed description of the personal health information involved.
- Steps taken and planned to mitigate the harm and to prevent future breaches.
- If necessary, advice on actions the individuals can take to further mitigate the risk or harm and protect themselves.
- Contact information of an individual within your organization who can answer questions and provide further information.
- A notice that individuals have a right to complain to the IPC. Provide contact information.
- Recognition of the impacts of the breach on affected individuals and an apology.

[38] As the patient and her spouse were the ones to notify the Clinic of the breach of privacy complaint they are aware of the alleged breach of privacy incident. Once the Clinic has interviewed the employee and adequately investigated the incident, it should notify the individuals of its findings and what steps it has taken to prevent any future occurrences.

***Prevent future breaches***

[39] The most important part to responding to a privacy breach is to implement measures to prevent future breaches from occurring. A trustee should ask itself, what steps can be taken to prevent a similar privacy breach?

[40] Section 16 of HIPA provides a duty for a trustee to protect personal health information in its custody or control and establish policies and procedures to maintain administrative, technical and physical safeguards.

[41] In its internal investigation report, the Clinic identified steps it would take to prevent future privacy breaches. This included meeting with all lab staff to review the Clinic's privacy policies to ensure all employees are aware of their obligations to protect personal health information and its intentions to review and revise its internal privacy policies and procedures.

[42] The Clinic also provided all lab employees with a "letter of expectation" to serve as a reminder of its obligation to protect personal health information. The Clinic provided my office with a copy of this letter dated October 4, 2017 which included the following statement:

> Due to the sensitive nature of services and testing such as HIV, AIDS, pregnancy, etc., extreme caution must be used to ensure client privacy and health information remains confidential and must not be shared with anyone within or outside the organization. This includes ensuring non-lab staff or clients are not in the lab or at the desk for any purpose other than to receive lab services.
>
> All staff must comply with privacy and confidentiality legislation and policy. Potential breach of confidentiality or privacy includes incidents such as talking about clients during breaks, talk to family members or friends about a certain client or that you saw them at the clinic, posting a comment on social media, snooping on EMR, accessing your own EMR files, etc… Prince Albert is a small community and people can figure out who you are talking about even without stating their names and then privacy is breached.
>
> If a member of the public comes forth with allegations that a staff member has breached confidentiality, it is our legislated duty to follow up with an investigation and

disciplinary action including suspension and dismissal depending on the severity of the breach.

[43] The Clinic advised it would be revising its complaint form to reflect the steps for investigating a breach of privacy complaint as outlined in the HIPA Guide.

[44] As well, the Clinic advised it was in the process of reviewing its internal policy and procedure manual to reflect the Saskatchewan Medical Association's EMR Program Privacy and Security Policy and Procedure Manual in order to create a comprehensive privacy and confidentiality manual.

[45] I commend the Clinic for its review of its internal policies and procedures to create a comprehensive privacy manual. During its review of its policies and procedures, I would recommend the Clinic ensure its privacy manual includes policies or procedures that address the following:

- The use of social media by employees;
- Appropriate use and disclosure of personal health information by employees; and
- The Clinic's expectations of employees when dealing with patients with whom they have a personal relationship.

[46] I note that the Clinic also indicated it has an oath of confidentiality it has all staff review and sign on an annual basis. While the Clinic is reviewing its internal policies and procedures to create a comprehensive privacy and confidentiality manual, it should also consider reviewing the oath it has employees sign to ensure it speaks to the obligations under HIPA. My office's website has a sample confidentiality agreement for trustees that the Clinic may want to consider referring to as a template.

***Privacy breach report***

[47] Once the necessary information has been collected, it is recommended that the trustee prepare a privacy breach investigation report.

[48] The Clinic did provide my office with an internal investigation report outlining dates related to the complaint, steps it had taken based on the complaint and what its findings were. As such, I find the Clinic had completed a privacy breach report.

[49] My office provided the Clinic with a draft version of this investigation report. After reviewing the report, the Clinic responded advising it intended to follow all the recommendations outlined in this report.

## III FINDINGS

[50] I find that HIPA applies to the breach of privacy complaint.

[51] I find that a breach of privacy has occurred.

[52] I find that the Clinic has not adequately contained this privacy breach.

[53] I find that the Clinic did not adequately investigate the breach of privacy complaint.

## IV RECOMMENDATIONS

[54] I recommend that the Clinic interview the employee involved in the breach of privacy complaint and complete its internal investigation into the complaint.

[55] I recommend the Clinic consider appropriate disciplinary action for the employee involved in the breach of privacy incident.

[56] I recommend the Clinic notify the patient of the outcome of the investigation and steps taken to prevent future breaches of privacy.

[57] I recommend the Clinic develop policies and procedures as outlined at paragraph [45].

Dated at Regina, in the Province of Saskatchewan, this 27th day of March, 2018.

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