Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 306-2019

Dr. Noor Adams, Dr. Mark Cameron, Dr. Ashis Paul (Broad Street Medical Clinic)

September 15, 2020

Summary: The Broad Street Medical Clinic (the Clinic) proactively reported that one of its physicians lost his Dictaphone which contained the personal health information of 39 individuals. The Dictaphone was not recovered. The Commissioner found that the Clinic did not have adequate administrative, physical or technical safeguards in place to protect against loss or unauthorized disclosure of personal health information, including agreements that designate Dr. Adams, Dr. Cameron and Dr. Paul as the trustees of the personal health information. The Commissioner also found that the Clinic did not take appropriate steps to respond to the breach. He made several recommendations such as putting agreements in place that describe who has custody or control of personal health information, notifying affected individual and enhancing other safeguards.

I BACKGROUND

[1] On September 27, 2019, the Broad Street Medical Clinic (the Clinic) proactively reported a privacy breach to my office. It indicated that the Dictaphone of Dr. Noor Adams, one of the physicians and partners at the Clinic, was missing. It suspected that the device had been stolen. The Clinic estimated that it contained dictated notes of 39 patients that Dr. Adams saw on September 23, 2019.

[2] On October 3, 2019, my office requested that the Clinic provide documentation that establishes trusteeship of personal health information that is involved. Nothing was provided.

[3] On October 17, 2019, my office notified the Clinic that my office would be undertaking an investigation. My office asked the Clinic to provide the following information by November 18, 2019:

- documentation which clearly establishes trusteeship and responsibility for patient records at the Clinic at the time the breach occurred;
- the Clinic's internal investigation report which explains how our office's recommended steps for responding to a privacy breach were addressed;
- details of the breach; and
- copies of relevant documents including written privacy policies, procedures or agreements.

[4] My office did not receive the requested material from the Clinic by the deadline. Throughout the month of November and December 2019, my office provided reminders and guidance to the Clinic about what was required to move forward with the investigation. On January 23, 2020, the Clinic provided my office with an internal investigation report and details about the breach. My office did not receive further documentation that established trusteeship or copies of the Clinic's privacy policies or procedures.

[5] Through the months of May, June and July, my office sent reminders and further guidance as to the type of documentation my office required regarding trusteeship. My office also repeatedly asked for copies of the Clinic's privacy policies and procedures. The Clinic noted that Dr. Adams was not working during the COVID-19 pandemic and could not provide anything further during the pandemic. However, the Clinic remained open and other physicians and staff continued working. My office received nothing further.

II DISCUSSION OF THE ISSUES

1. Does HIPA apply in these circumstances and do I have jurisdiction?

[6] *The Health Information Protection Act* (HIPA) applies in full 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.

Is there personal health information?

[7] Personal health information is defined in subsection 2(m) of HIPA which provides:

> **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;

[8] Further, subsection 2(q) of HIPA defines registration information as follows:

> 2 In this Act:
>
> …
>
> (q) "registration information" means information about an individual that is collected for the purpose of registering the individual for the provision of health services, and includes the individual's health services number and any other number assigned to the individual as part of a system of unique identifying numbers that is prescribed in the regulations;

[9] The Clinic reported that the missing Dictaphone contained Dr. Noor Adam's dictated notes for 39 patients that he saw on Monday, September 23, 2019. The Clinic indicated that Dr.

Adams used the name of each patient to identify them in his notes on the Dictaphone. It noted that Dr. Adams' typist uses encounter sheets containing registration information for the purpose of identifying patients when transcribing the notes from the Dictaphone, so only names are used on the Dictaphone.

[10] The 39 patients were receiving a health service from Dr. Adams when they saw him on September 23, 2019. Therefore, the notes on the Dictaphone would qualify as personal health information pursuant to subsection 2(m)(ii) of HIPA. Further, the health service provided would relate to the patients' physical or mental health and would qualify as personal health information pursuant to subsection 2(m)(i) of HIPA. Finally, as described above, the patients' names were used to register the individuals for the purpose of a health service and would qualify as registration information pursuant to subsection 2(q) of HIPA. This would qualify as personal health information pursuant to subsection 2(m)(v) of HIPA.

Are there trustees?

[11] In its submission of January 23, 2020, the Clinic indicated that the Clinic has three physician partners: Dr. Mark Cameron, Dr. Noor Adams and Dr. Ashis Paul. The Clinic reported that there are also four associate physicians.

[12] Subsection 2(t) of HIPA defines trustee. In part, it provides:

> **2** In this Act:
>
> …
>
> (t) "trustee" means any of the following that have custody or control of personal health information:
>
> …
>
> (xii) a person, other than an employee of a trustee, who is:
>
> (A) a health professional licensed or registered pursuant to an Act for which the minister is responsible; or
>
> (B) a member of a class of persons designated as health professionals in the regulations;

[13] The three partners, Dr. Adams, Dr. Cameron and Dr. Paul, are each licenced pursuant to *The Medical Profession Act, 1981*, through the College of Physicians and Surgeons of Saskatchewan (CPSS) according to CPSS' website. They can qualify as trustees if they have custody or control of the personal health information in question.

Is personal health information in the custody and control of the trustees?

[14] In Investigation Report 398-2019, 399-3019, 417-2019, 005-2020, 019-2019, 021-2020, my office defined "custody" and "control".

[15] Custody is the physical possession of a record by a trustee, who has a measure of control.

[16] Control connotes authority. A record is under the control of a trustee when the trustee has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition. Custody is not a requirement.

[17] My office asked the Clinic for details of who the trustees with custody or control of the personal health information in question were.

[18] In its initial submission, the Clinic indicated that Dr. Adams, Dr. Cameron and Dr. Paul were the partners of the Clinic at the time of the breach. I accept this position.

[19] The Clinic suggested that custody and control of the personal health information was entrusted to each physician. The Clinic did not explain the reason for this shift. I do not accept this alternate explanation.

[20] My office asked the Clinic to provide documentation to which supported its understanding of custody and control. Nothing was provided. I view written agreements between health professionals that describe the trusteeship of personal health information as a fundamental safeguard that all trustees should have in place.

[21] I find that Dr. Adams, Dr. Cameron and Dr. Paul are trustees that have joint custody and control of the personal health information in question.

[22] I recommend that Dr. Adams, Dr. Cameron and Dr. Paul develop written agreements between themselves and other health professionals involved with the Clinic that explicitly address the issue of custody and control of personal health information.

2. Was there a privacy breach?

[23] The Clinic reported that Dr. Adams had dictated notes about 39 patients he saw on September 23, 2020 on to his Dictaphone. Dr. Adams left the Dictaphone on his desk in his office in the Clinic while he saw patients on September 24, 2020. At the end of the day on September 24, 2020, Dr. Adams could not locate the Dictaphone. Dr. Adams, the Clinic's office manager, reception staff and the cleaning staff searched the office. The cleaning staff also provided cleaning services in Dr. Adam's home. The cleaning staff were also asked to search Dr. Adams' home. The Clinic did not indicate if the typist, was involved in the search or if any employees were interviewed during the process of the Clinic's investigation.

[24] The Dictaphone was not found. The Clinic has indicated that it suspects that the Dictaphone was stolen, but is not certain.

[25] As the Dictaphone has not been recovered, we cannot be certain of what happened to it.

[26] Subsection 27(1) of HIPA provides:

> **27**(1) A trustee shall not disclose personal health information in the custody or control of the trustee except with the consent of the subject individual or in accordance with this section, section 28 or section 29.

[27] A disclosure is the exposure of personal health information to a separate entity, not a division or branch of the trustee in custody or control of that information.

[28] As it is not known what has happened to the Dictaphone, it is possible that the personal health information on the Dictaphone was exposed to a separate entity. There was no authority for the Clinic to disclose the personal health information in such a manner. Therefore, the loss of the Dictaphone constitutes a breach of privacy.

[29] This Report will also explore whether the Clinic had reasonable safeguards in place to protect against the loss or unauthorized disclosure of personal health information.

3. Did the Clinic respond to this privacy breach appropriately?

[30] My office suggests that trustees undertake the following four steps when responding to a privacy breach:

1. Contain the breach (as soon as possible);
2. Notify affected individuals (as soon as possible);
3. Investigate the breach; and
4. Plan for prevention.

[31] Below is an analysis of each of these steps.

Contain the Breach

[32] To contain the privacy breach is to ensure that the personal health information is no longer at risk. This may include recovering the record(s), revoking access to personal health information, and/or stopping the unauthorized practice.

[33] After it searched for the Dictaphone and could not locate it, the Clinic indicated that it contacted CPSS to obtain advice. It also contacted my office to obtain advice and proactively report the breach.

[34] In a letter to my office dated September 25, 2019, the Clinic indicated that it intended to report the incident to the Regina Police Service (RPS). However, in its investigation report, received in my office on January 23, 2020, the Clinic indicated that it did not report to the RPS as it wanted to ensure that it was theft. It did not indicate what evidence it was seeking

that would have triggered a call to police. Further, it did not explain why it continued to suspect that the Dictaphone was stolen.

[35] The Clinic indicated that Dr. Adams asserted that his office door was locked. However, the Clinic's report did not report any damage to the office door or any other signs of forced entry to the office. It did not indicate if it had to make any repair or take other steps in order to protect any other personal health information that might be stored in Dr. Adams' office.

[36] I am not satisfied that Dr. Adams, Dr. Cameron and Dr. Paul took reasonable steps to contain the breach.

Notify affected individuals

[37] It is best practice that a trustee notify the affected individuals when there has been a breach of privacy. Notifying affected individuals of the privacy breach is important so that they can determine how they have been impacted and take steps to protect themselves. An effective notification should include the following:

- a description of what happened;
- a detailed description of the personal information or personal health information that was involved;
- if known, a description of possible types of harm that may come to them as a result of the privacy breach;
- steps that the individuals can take to mitigate harm;
- steps the organization is taking to prevent similar privacy breaches in the future;
- the contact information of an individual within the organization who can answer questions and provide further information;
- a notice that individuals have a right to complain to my office and contact information; and
- where appropriate, recognition of the impacts of the breach on affected individuals and an apology.

[38] The Clinic indicated that it has not notified the 39 affected individuals. In its investigation report, the Clinic submitted that it did not want patients to fear that all their medical information had been compromised as it was only the diagnosis of that day that was

recorded. It indicated that this was the Clinic's "compelling rationale" for not notifying affected individuals.

[39] The Clinic also reported that it did not notify affected individuals because only the patients' names were used to identify the patients.

[40] I am not persuaded by the Clinic's reasons for not notifying affected individuals. A patient's name is enough to identify an individual. This puts all the affected individuals at risk of being identified by whoever finds the Dictaphone. Also, the guidance provided to the Clinic by my office indicates that, during notification, trustees should provide affected individuals with a detailed description of the personal information or personal health information that was involved. This would alleviate the Clinic's concerns that affected individuals would not know what personal health information was lost.

[41] I recommend that Dr. Adams, Dr. Cameron and Dr. Paul notify the 39 affected individuals of the breach as soon as possible. After receiving a draft of this Report, the Clinic indicated that it would notify the affected individuals.

Investigate the Breach

[42] Investigating the privacy breach to identify the root cause is key to understanding what happened and to prevent similar privacy breaches in the future. It is fundamental for trustees to review the administrative, physical and technical safeguards that were in place at the time of the breach to ensure that the personal health information was protected from reasonably anticipated threats pursuant to section 16 of HIPA which provides:

> **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:
>
> (a) protect the integrity, accuracy and confidentiality of the information;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the information;

(ii) loss of the information; or

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

(c) otherwise ensure compliance with this Act by its employees.

[43] Examples of common administrative, physical and technical safeguards can be found in Appendix B of my office's resource, *IPC Guide to HIPA.*

[44] Written privacy policies and procedures are very important administrative safeguards that inform all individuals employed by a trustee of how personal health information is to be protected. My office asked the Clinic for a copy of their written privacy policies and procedures multiple times. Nothing was provided. It does not appear that there were administrative safeguards in place. The Clinic indicated that it did have a clean desk policy, but did not indicate if this was a written policy.

[45] The Clinic also indicated that, as part of its written policies and procedures, it requires all staff and contractors to sign a Broad Street Clinic Confidentiality Policy and a Confidentiality Agreement for Employees. The Clinic did not provide those to my office for review. It also noted that these documents were forms written by CPSS or the Saskatchewan Medical Association. My office has said in previous reports, such as Investigation Report LA-2013-001, Investigation Report H-2014-001 and Investigation Report 351-2017, 031-2018, 143-2018, 144-2018, 145-2018 that is not enough for a trustee to adopt the policies of another organization. It must ensure policies and procedures are tailored to meet the unique and specific needs of the trustee. My office encourages trustees to alter any templates available to them and tailor them to the unique circumstance of their practice.

[46] I recommend that Dr. Adams, Dr. Cameron and Dr. Paul develop comprehensive written tailored privacy policies and procedures for the Clinic. After receiving a draft of this Report, the Clinic indicated that it would work on developing policies and procedures in the coming weeks.

[47] As noted, the Clinic indicated that Dr. Adams left the Dictaphone on his desk in his office at the Clinic. With respect to physical safeguards, the Clinic reported that Dr. Adams asserts that he locked his office. The Clinic did not report any signs that the lock on the office door was damaged or any other sign of forced entry to the office. One of the measures the Clinic is taking to prevent further breaches is to recommend to physicians to keep their office doors locked. Finally, the Clinic has not provided a written policy that demonstrates that such physical safeguards were in place.

[48] I recommend that Dr. Adams, Dr. Cameron and Dr. Paul ensure all personal health information is locked when it is not in the presence of one of its staff members. I recommend that Dr. Adams, Dr. Cameron and Dr. Paul include this in its written privacy policies and procedures.

[49] Finally, in its investigation report, the Clinic did not address any technical safeguards in place with respect to the Dictaphone; namely passwords. The Clinic did not indicate that the personal health information on the Dictaphone was protected by passwords or encryption. I am not satisfied that the personal health information was protected by technical safeguards.

[50] For information on increasing the security of mobile devices, I recommend that Dr. Adams, Dr. Cameron and Dr. Paul review my office's resource, *Helpful Tips: Mobile Device Security* and implement technical safeguards on all mobile devices. Some tips include adding encryption in addition to having strong passwords, and keeping devices in a locked drawer or cabinet or having a security cable attached to them.

[51] I have pointed out several deficiencies in the Clinic's administrative, physical and technical safeguards, I find that Dr. Adams, Dr. Cameron and Dr. Paul did not have adequate safeguards in place to protect the personal health information against reasonably anticipated threats or hazards to the security or integrity of the personal health information, loss of the personal health information or unauthorized disclosure of the personal health information pursuant to subsection 16(b) of HIPA.

Plan for prevention

[52] The Clinic indicated that its first action to prevent future breaches was to ensure that its hallway cameras were working. Cameras will not necessarily protect against the loss or unauthorized disclosure of personal health information, but might be helpful in recovering personal health information that is lost.

[53] The Clinic's second action was to notify all physicians in the Clinic to ensure that they were aware of the presumed theft. The Clinic advised the physicians to keep their office doors closed and the external doors to Physician offices locked at all times. I have also made recommendations regarding these physical safeguards.

[54] As a third preventative measure, the Clinic indicated that it advised all staff to watch the people in the hallways. In addition, I urge the Clinic to focus on administrative, physical and technical safeguards.

[55] Finally, the last preventative action that the Clinic reported was to "inform all new staff that security of patients and property are very important for everyone". Having written privacy policies and procedures and yearly training sessions are essential for promoting the protection of personal health information among staff members. I recommend that Dr. Adams, Dr. Cameron and Dr. Paul ensure its staff receive privacy training on an annual basis. After receiving a draft of this Report, the Clinic indicated it would comply with this recommendation.

[56] As discussed, I am not satisfied with Dr. Adams, Dr. Cameron and Dr. Paul's efforts to contain the breach, notify police or affected individuals, and investigate the breach or prevent future breaches. As such, I find Dr. Adams, Dr. Cameron and Dr. Paul did not adequately respond to this privacy breach.

[57] I recommend that Dr. Adams, Dr. Cameron and Dr. Paul review the procedures that the Clinic follows when responding to a privacy breach.

III FINDINGS

[58] I find that Dr. Adams, Dr. Cameron and Dr. Paul are trustees with joint custody and control of the personal health information in question.

[59] I find that the theft or loss of the Dictaphone constitutes a breach of privacy.

[60] I find that Dr. Adams, Dr. Cameron and Dr. Paul did not have adequate administrative, physical or technical safeguards in place to protect the personal health information against reasonably anticipated threats or hazards to the security or integrity of the personal health information, loss of the personal health information or unauthorized disclosure of the personal health information pursuant to subsection 16(b) of HIPA.

[61] I find Dr. Adams, Dr. Cameron and Dr. Paul did not adequately respond to this privacy breach.

IV RECOMMENDATIONS

[62] I recommend that Dr. Adams, Dr. Cameron and Dr. Paul develop written agreements between themselves and other health professionals involved with the Clinic that explicitly address the issue of custody and control of personal health information.

[63] I recommend that Dr. Adams, Dr. Cameron and Dr. Paul report any future suspected theft to the RPS as soon as potential criminal activity is identified.

[64] I recommend that Dr. Adams, Dr. Cameron and Dr. Paul notify the 39 affected individuals of the breach as soon as possible.

[65] I recommend that Dr. Adams, Dr. Cameron and Dr. Paul develop comprehensive and tailored written privacy policies and procedures for the Clinic.

[66] I recommend that Dr. Adams, Dr. Cameron and Dr. Paul ensure all personal health information is locked when it is not in the presence of one of its staff members. I recommend that Dr. Adams, Dr. Cameron and Dr. Paul include this in its written privacy policies and procedures.

[67] I recommend that Dr. Adams, Dr. Cameron and Dr. Paul review my office's resource, *Helpful Tips: Mobile Device Security* and implement technical safeguards on all mobile devices.

[68] I recommend that Dr. Adams, Dr. Cameron and Dr. Paul ensure their staff receive privacy training on an annual basis.

[69] I recommend that Dr. Adams, Dr. Cameron and Dr. Paul review the procedures that the Clinic follows when responding to a privacy breach.

Dated at Regina, in the Province of Saskatchewan, this 15th day of September, 2020.

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