Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 225-2016

Dr. Mahmud

November 28, 2016

Summary: Patient files were being stored in the waiting area of the Northgate Medi Clinic (Clinic), easily accessible to any person who entered the Clinic. The Office of the Information and Privacy Commissioner (IPC) found this matter to be a privacy breach. The IPC made several recommendations, including developing policies and procedures on how to protect and manage personal health information.

I BACKGROUND

[1] In August 2016, an individual reported to my office that boxes of patient files at the Northgate Medi Clinic (Clinic) were being stored in the patient waiting area. These boxes were easily accessible to any person who entered the Clinic.

[2] On September 2, 2016, my office attended the Clinic. It observed that along the east side of the waiting area of the Clinic contained the following:

- 51 open boxes of records stored on wooden shelves along the east wall of the Clinic;
- 1 four drawer cabinet – locked/jammed;
- 1 two drawer cabinet – unlocked and full of records;
- 1 four drawer cabinet – unlocked and full of records;
- 1 three drawer cabinet – unlocked and empty.

[3] My office noted that patient names on some of the records, especially those stored in the open boxes along the top shelf against the east wall of the Clinic could be easily read by a passerby.

[4] My office also observed that the attention of individuals in the waiting area would be drawn towards the direction of the patient records. First, a television set displaying general information, such as health tips, was installed on the wall adjacent to the 51 open boxes of patient records. Also, a rack of magazines was place right up against the cabinets. Finally, a sign indicating there should be no food or drinks in the waiting area was taped on one of the cabinets containing patient records.

[5] During my office's attendance at the Clinic on September 2, 2016 and in an email dated September 29, 2016, Dr. Mahmud and his staff asserted the records in the waiting area were placed there by the previous owners of the clinic. My office obtained a copy of the Bill of Sale indicating that Dr. Mahmud had purchased the Clinic in September 2013. Therefore, the records have been in the waiting area since September 2013. If the patient files had been placed in the waiting area by the previous owners, then the patient files have conceivably been in the waiting area since September 2013.

II DISCUSSION OF THE ISSUES

1. Is HIPA engaged?

[6] 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.

[7] First, Dr. Mahmud qualifies as a trustee as defined by subsection 2(t)(xiii) of *The Health Information Protection Act* (HIPA). Second, based on my office's observations, the patient files that were in the waiting area contained personal health information as defined by subsection 2(m) of HIPA. Third, based on the Bill of Sale, Dr. Mahmud

assumed responsibility for the patient files when he purchased the Clinic in September 2013. Therefore, I find that HIPA is engaged.

2. Did the trustee have appropriate safeguards?

[8] Section 16 of HIPA provides that trustees must establish appropriate safeguards. It 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.

[9] Since the records were in the waiting area and easily accessible to any person who entered the Clinic, I find that the trustee did not have appropriate safeguards. Furthermore, since only one staff member is on duty at one time with Dr. Mahmud, the records would have been left unattended if he or she left the front desk.

[10] Since the trustee did not have appropriate safeguards pursuant to section 16 of HIPA, I find that this matter qualifies as a privacy breach.

3. Did the trustee respond appropriately to the privacy breach?

[11] Where there is a privacy breach, my office's focus is determining whether the trustee has appropriately handled the privacy breach. My office's resource, *IPC Guide to HIPA*, recommends four best practice steps be taken by a trustee when responding to a privacy breach. These are:

1. Contain the breach;
2. Notify affected individuals and/or appropriate organizations;
3. Investigate the breach; and
4. Plan for prevention.

[12] I will use the above four steps to assess the trustee's response to the privacy breach.

[13] First, to contain the breach, the trustee indicated to my office that as of October 2, 2016 all the records had been moved from the waiting area to a backroom that is inaccessible to patients. I find that the trustee has contained the breach.

[14] Second, the trustee initially had not provided notice of the privacy breach to the affected individuals. I note the patient records could have contained outdated contact information for the hundreds or even thousands of affected individuals. Therefore, it may not be practical or feasible to contact each and every affected individual. My office recommended to the trustee that it post a notice at his Clinic that would notify any individual who visited the Clinic prior to September 2013 may have been affected by this privacy breach. In an email dated November 21, 2016, the trustee's office advised my office that the trustee has posted a notice of the privacy breach.

[15] Third, in terms of investigating this breach, my office looks to see if the trustee has identified the root cause of the privacy breach. The trustee asserted that this privacy breach was a result of the previous owners of the clinic placing the records in the waiting area. The trustee did not identify the root cause of this privacy breach. Even though the previous owners of the clinic placed the records in the waiting area, the trustee is responsible for safeguarding the personal health information. He left the patient records in the waiting area for nearly three years until my office prompted him to apply appropriate safeguards. Therefore, I find that the trustee did not investigate this privacy breach thoroughly.

[16] Fourth, in terms of preventing similar breaches in the future, the trustee indicated he reviewed the patient files and noted that the records are "very outdated". As such, he would be shredding the patient files that indicate that patient's last visit was at least seven years ago. He stated that he would retain files on youth until one year past their 18th birthday. I recommend that the trustee retain files on youth until at least two years past their 18th birthday or six years after the date the youth was last seen, whichever is the later date. This is in accordance with the College of Physicians and Surgeons of Saskatchewan's (the College) bylaws. The College's Bylaw 23.1 provides as follows:

> A member shall retain the records required by this regulation for six years after the date of the last entry in the record. Records of pediatric patients shall be retained until 2 years past the age of majority or 6 years after the date last seen, whichever may be the later date.

[17] In an email dated November 21, 2016, the trustee's office advised my office that it is continuing its efforts to go through all the records to determine what they can shred or not. It advised that going through the records is taking a long time. I can appreciate that the task of going through the records is time-consuming. I commend the trustee and his staff for their efforts in reviewing the records. I recommend they continue with their efforts.

[18] Further, in terms of preventing similar privacy breaches, the trustee outlined the Clinic's current policies and procedures to safeguard personal health information. My office reviewed these safeguards and it found them to be appropriate.

[19] The trustee also stated that he is contacting the College of Physicians and Surgeons of Saskatchewan, the Ministry of Health, and the Saskatchewan Medical Association for resources on how to protect personal health information. He stated that he will require staff to read the resources, and sign that they will follow the rules and guidelines.

[20] I find that the trustee contacting these three organizations for guidance is appropriate. I recommend that the trustee use the resources he receives from these organizations to develop policies and procedures that match the needs of his Clinic. I recommend that these policies and procedures be developed within three months of receiving this Investigation Report.

[21] I also recommend that the trustee appoint a staff member to be the Privacy Officer for the Clinic. The Privacy Officer should be responsible for developing privacy policies and procedures, and ensuring all staff members are trained on these privacy policies and procedures. He or she should also be responsible for establishing appropriate retention and disposition schedules for personal health information, and ensuring the secure destruction of personal health information once the retention period has been met, in accordance with section 17 of HIPA.

IV FINDINGS

[22] I find that HIPA is engaged.

[23] I find that the trustee did not have appropriate safeguards.

[24] I find that the trustee contained the privacy breach.

[25] I find that that the trustee has made reasonable efforts to notify affected individuals.

[26] I find that the trustee did not investigate the privacy breach thoroughly.

[27] I find that the trustee is undertaking appropriate steps to prevent a similar privacy breach in the future.

V RECOMMENDATIONS

[28] I recommend that the trustee continue his efforts to retain and destroy patient records pursuant to the College of Physicians and Surgeons of Saskatchewan Bylaw 23.1.

[29] I recommend the trustee follow through with contacting the College of Physicians and Surgeons of Saskatchewan, the Ministry of Health, and the Saskatchewan Medical Association for resources on how to protection personal health information.

[30] I recommend that the trustee develop policies and procedures on how to protect and manage personal health information within three months of receiving this Investigation Report.

[31] I recommend that the trustee appoint a staff member to be the Privacy Officer for the Clinic, as described in paragraph [21].

Dated at Regina, in the Province of Saskatchewan, this 28th day of November, 2016.

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