SASKATCHEWAN

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

INVESTIGATION REPORT H-2011-001

Dr. Teik Im Ooi, carrying on business as Dr. Teik Im Ooi Medical Professional Corporation, Albert Park Medical Clinic, Albert Park Medical Centre and/or Albert Park Family Medical Centre

JULY 14, 2011

TABLE OF CONTENTS

SASKATCHEWAN

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

INVESTIGATION REPORT H-2011-001

Dr. Teik Im Ooi, carrying on business as Dr. Teik Im Ooi Medical Professional Corporation, Albert Park Medical Clinic, Albert Park Medical Centre and/or Albert Park Family Medical Centre

I. EXECUTIVE SUMMARY

[1] On March 23, 2011 the Office of the Information and Privacy Commissioner (OIPC) was alerted to a large volume of patient files in a recycling bin in south Regina. This was located on the corner of a shopping centre parking lot near an office building.

[2] Our investigation determined that there were 180,169 pieces of personal health information (phi) (including approximately 2,682 patient files) in the recycling bin. These records belonged to Albert Park Family Medical Centre (hereinafter referred to as APFMC) located in Gold Square. The responsible trustee was Dr. Teik Im Ooi.

[3] It was determined that the patient records were thrown into the recycling bin by two employees of a contracted maintenance company for Golden Mile Shopping Centre (a building adjacent to Gold Square). We determined that the patient records had been moved from APFMC for storage on the second floor of Gold Square beginning in 2005. By 2007, approximately 150 boxes of patient records had accumulated there. This was the first of five different moves of the patient records that involved two different buildings and four different storage rooms or areas over a period of almost six years. For all intents and purposes, APFMC appeared to have lost track of the records when they

were moved from their original location at APFMC in 2005. At that point, there was no record or catalogue of the contents of the boxes. In addition, the boxes were not marked in any sequential fashion to be able to trace their subsequent moves. There was little to no involvement by APFMC in four of the five moves and no supervision by APFMC of the moves nor any inspection of the off-site storage spaces. There was no written agreement between Dr. Ooi and third parties who acted as information management service providers (IMSP). It was determined that from 2007 until March 23, 2011 the large volume of patient phi was unprotected from many persons who would have had no legitimate 'need-to-know' that patient information. This included workmen, labourers, staff of Golden Mile Shopping Centre, and a large crowd of more than 3,600 persons who toured the basement where the patient files were stored in an unlocked space during the last three weeks of October 2010.

[4] Although, as noted above, approximately 150 boxes of patient records were moved from APFMC for storage purposes between 2005 and 2007, the discovery of files in the recycling bin leaves unaccounted approximately 125 of those boxes of patient records. More than three weeks into our investigation APFMC advanced a theory that the missing 125 boxes had been moved back to APFMC at some point in 2007. Despite our further investigation, there is no reliable evidence that confirms this theory nor particulars of how such a move happened or who undertook the move. In any event, without an inventory of the box contents before they left APFMC and identification tags or numbers to allow tracing of the files, there is still the problem of a much larger number of patient files that left APFMC and did not end up in the recycling bin on March 23, 2011.

[5] The Commissioner found that Dr. Ooi failed to meet the requirements of section 16 of *The Health Information Protection Act* (HIPA) by the failure to have written policies and procedures to adequately safeguard patients' phi. Further, Dr. Ooi failed to take the steps required by section 17 of HIPA to ensure that the patients' phi was stored in a way that could be retrievable, readable and usable and to ensure that records were destroyed in a manner that protects the privacy of the affected patients. Dr. Ooi failed to put in place agreements and mechanisms required by section 18 in dealings with the IMSPs who provided storage, transportation and destruction of phi.

[6] The Commissioner made 11 recommendations including:

1. That Dr. Ooi provide notification to affected patients, past and present of APFMC consistent with our office's *Privacy Breach Guidelines*.

2. That for those patients related to the 2,682 files involved in this breach, a letter in a form satisfactory to our office, be mailed to each patient explaining what has happened, what corrective action will be taken to prevent a reoccurrence of the breach and advising them that they have the right to contact our office if they are dissatisfied with the action taken by Dr. Ooi and APFMC.

3. That a newspaper advertisement be published in the Regina *Leader-Post* on two successive weeks that provides the information described in 2 above.

4. That Dr. Ooi provide our office, within 30 days, comprehensive written policies and procedures for the administrative and physical safeguards contemplated by sections 16, 17 and 18 of HIPA.

5. That Dr. Ooi enter into formal written agreements with all existing IMSPs within 30 days and provide our office with copies.

6. That Dr. Ooi undertake, within 60 days, an intensive training program for all staff at any of her clinics in the city of Regina with respect to HIPA with particular emphasis on those requirements that go beyond simply a confidentiality requirement.

7. That Dr. Ooi ensure that each member of APFMC staff execute a confidentiality undertaking that includes an acknowledgement that breach of HIPA and APFMC privacy policies and procedures may be grounds for dismissal with cause.

8. That Dr. Ooi provide our office, within 60 days, a written plan that outlines how she intends to address the large volume of un-catalogued patient files currently being stored at Transcona Medical Clinic. The written plan should include what is contemplated for the retention and destruction of the records.

9. That the College of Physicians and Surgeons of Saskatchewan implement a mandatory requirement for a comprehensive HIPA training program and monitor attendance of its members.

10. That the Ministry of Health complete a comprehensive HIPA manual that provides detailed, concrete and practical information to all trustees and the public on compliance with all provisions of HIPA with particular emphasis on sections 16, 17 and 18.

11. That the Minister of Justice consider commencing a prosecution pursuant to section 64 of HIPA in respect to multiple breaches documented in this Investigation Report.

II. BACKGROUND

A. Content of the Boxes

[7] Before we consider the details of our investigation that followed the discovery of large volumes of patient personal health information (phi) in a recycling bin behind Golden Mile Shopping Centre, it may be useful to first describe exactly what we found on March 23, 2011. The following table describes both the number and the type of information that we seized.

Box	Total Number of Items of PHI (approximate)	Content of the Boxes
1(a), 1(b), 2, 3(a), 3(b), 5	87,974	Daily Activity Reports from APFMC containing SK Health Services Number (hereinafter referred to as HSN) patient name, agency involved with client, diagnosis code, patient address\patient phone number. The information was repeated on a label attached to the back of the Daily Activity Reports.
4	78,578	Practitioner Reports containing the patient's name, HSN, diagnosis code, claim number, fee code, and fee charged per service.
6(a), 6(b)	10,348	Workers' Compensation Board (WCB) related materials including: Payment Lists, Invoices, Practitioners Progress Reports, Resub lists, patient labels, letters to patients, and billing letters that included: HSN, copies of out of province health cards, address, treatment-diagnosis. Doctor information including earnings, patients treated, fee per service and rejected\resubmitted claims.
7	1,595	One time patient files related to individual visits.
8, 9, 10, 11, 12, 13, 14, 15	463	Comprehensive patient files.
16	41	28 comprehensive patient files, 12 lab result packages, and one letter.
17	N\A	Pharmacy invoice sheets: July 1996; June, August, September, October, November and December of 1997; expired stock February, March, April and May of 1997. This box did not contain any phi.
18(a), 18(b), 18(c)	581	Comprehensive patient files.
19	569	One box of miscellaneous medical records including partial charts, test results, and patient visit sheets.
20	20	An envelope of loose medical material of three identified individuals, one miscellaneous envelope, one letter from doctor discussing file disposal, one plastic bag with 15 comprehensive patient files.
Total=25 Boxes	Total=180,169	

i. Box Content Description

Seizure and Security

[8] Files and other documents containing patient phi that had been in the recycling bin on March 23, 2011, were seized and secured by our office. An additional large box of similar records was provided to us when it was discovered in Room #19 of the basement of Golden Mile Shopping Centre on March 25, 2011. The documents were stored in a locked room at our office and access was limited to those tasked with the investigation. The documents were sorted, catalogued and analyzed.

[9] Some of the files and loose papers were already in distinctive green and white 'Grand and Toy' brand boxes marked with the name 'Albert Park', some with date ranges of June 2, 2001 to August 10, 2001. Other green and white boxes had such markings as 'Results', and had white stickers with 'Albert Park' written in pen. Boxes with the same color, brand and markings were identified and photographed by my staff on visits to Albert Park Family Medical Clinic (APFMC).

[10] The boxes were examined in our office on three occasions by APFMC staff. On each of those occasions APFMC staff acknowledged that the records we seized belonged to APFMC. As noted in the box content schedule prepared by our office, 180,169 pieces of phi were involved.

Box Content: Boxes 1-6 (Total of nine boxes)

[11] These nine boxes included 176,900 pieces of phi found on Daily Activity Reports, Medical Practitioner Reports and WCB claim related material. Many of these reports included a diagnostic code used to identify specific ailments that were treated.

[12] From our investigation, we found that the diagnostic codes are from the *International Classification of Diseases* (ICD) from the World Health Organization (WHO).[1] My staff was able to generally match the diagnostic codes with those on a random sample of the Daily Activity Reports. APFMC staff confirmed that the diagnostic code is a universal code and is available from the WHO.

[13] In any event, the diagnostic codes are in a public document and are readily available to anyone with access to the internet.

Box Content: Boxes 7-20 (Total of 15 boxes)

[14] Boxes 7-20 (excluding box 17 as it did not contain phi) contained 3,269 pieces of phi detailed below. Of these 3,269 items: 1,595 items were one time patient files related to individual visits, 1,087 were comprehensive patient files, and 587 were items of miscellaneous patient information.

[15] The contents of the boxes could be generally described to contain the medical history and detailed payment schedules of patients who attended, or had physicians who worked for APFMC. These boxes included descriptions of patients' cancer treatments, mental health disorders, comprehensive documentation of a harassment complaint, detailed laboratory reports, x-ray results, electrocardiography results, infectious disease reports, sexually transmitted disease results, pregnancy results and doctor counseling notes. Test results and full copies of medical service cards from Alberta, Manitoba, British Columbia and Saskatchewan were included. We also found mammograms, operative reports, psychological assessments, dermatology results, results from ultrasound tests of a patient's uterus and cytology results.

B. Tracking the Boxes

[16] As a result of the investigation it appears that the patient records discovered in the recycling bin on March 23, 2011 were subject to five previous moves. The circumstances

[1] *International Classification of Diseases*, World Health Organization, available at: http://www.who.int/classifications/icd/en/.

surrounding those five moves and the roles of the key individuals will be discussed in later portions of this Report. The focus of this section is on the transactions that took place with these boxes and their contents.

[17] The narrative that follows flows backward from the discovery of the records in the recycling bin to the original location in APFMC in 2005 (see diagram *Tracking the Boxes from End Point to Source* on page 11 of this Report).

1. Basement Room #19

[18] On March 23, 2011, patient records that contained phi were discovered in the recycling bin on the southeast corner of Golden Mile Shopping Centre parking lot. The dimensions of the recycling bin were approximately 24 feet in length, 98 inches wide and 89 inches high. Our office was alerted at approximately 4:50 p.m., attended the scene, and took immediate steps to secure the records. In addition, 581 patient files were found in Room #19 of Golden Mile Shopping Centre on March 25, 2011.

[19] We learned later on March 31, 2011, that two employees of a contracted maintenance company had moved what they described as approximately 25 boxes of files from Room #19 in the basement of Golden Mile Shopping Centre (see Schedule 1) to the recycling bin previously described. No inventory of the boxes was taken before the move to the recycling bin. Under the direction of the maintenance supervisor employed by the owner of Golden Mile Shopping Centre, the boxes were carried from the basement Room #19, up a steep flight of narrow stairs to the door. Travelling by tractor and cart from the northwest corner of the mall that adjoins Rae Street to the southeast corner of the parking lot which adjoins 25th Avenue, the boxes were moved on the morning of March 23, 2011, and tossed into the recycling bin. They were first seen in the recycling bin by a witness at noon on the same day. When the boxes of files were tossed into the bin, the boxes were not sealed in any way. As a result, most of the records had fallen out of the boxes and were loose in the recycling bin when seized by the Office of the Information and Privacy Commissioner (OIPC).

[20] Previous to being discarded in the recycling bin, the boxes of records were stored in unlocked Room #19 of Golden Mile Shopping Centre basement. Basement Room #19 was a dimly lit room that was approximately 8x20 feet. The space was enclosed on all sides and accessible through the door from which entry is gained from the hallway. This room was apparently unlocked from the time the boxes were moved into Room #19 until they were moved out on March 23, 2011.

2. Basement Common Area

[21] Before the move to Room #19, the boxes were located in a common or open area of the basement of Golden Mile Shopping Centre (see Schedule 1). The common area is down a hallway north of storage Room #19. This common area was an open area accessible to anyone who entered the basement. The basement common area was not secured in any fashion other than by a locked door at the top of the stairs leading out of the building. In this space, the boxes and their contents would have been exposed to anyone who had business of any kind in the basement of the shopping centre. At this stage, the boxes were not sealed in any way and the contents could be easily accessed.

[22] The boxes had been moved to this space in the winter of 2007 by persons unknown, but presumably by staff of the landlord, the owner of Golden Mile Shopping Centre. We could not confirm how long the boxes remained in the common area.

[23] This basement was the location for a 'haunted house' event that took place between October 7th and October 31st, 2010. The event drew 150-200 people per day. This is estimated to be 3,600-4,800 persons passing through the basement from the northwest exit, south through the common basement area, down the hall passage, and exiting up the staircase and through the entrance door that opens onto the parking space adjacent to Rae Street.

3. Basement Room #5

[24] Prior to their storage in the basement common area, the records were stored in Room #5 of Golden Mile Shopping Centre basement. Room #5 is immediately adjacent to Room #19, on the east side of the passage way that separates the various storage rooms leading to the basement common area (see Schedule 1). At this point, the boxes of records were not sealed in any way.

[25] There was a lease for Room #5 between the owner of Gold Square and the owner of Golden Mile Shopping Centre. The lease term on this space was from February 15, 2007 to August 31, 2007. Subsequent to August 31, 2007, the lease was continued on a month-to-month basis until it was agreed between the parties that it would terminate on March 31, 2011.

[26] Initially Room #5 was locked. In the winter of 2007, as a result of a water leak in the basement, Golden Mile Shopping Centre staff broke the lock to the room, and the records were moved to the common area.

4. Second Floor

[27] Prior to the boxes moving to Room #5, the boxes were stored on the second floor of Gold Square, located at 3992 Albert Street (see Schedule 2). This was in a locked room. The records had been moved by employees of the owner of Gold Square and the contracted construction company to the basement storage Room #5 between the last two weeks of February and the first three weeks of March 2007. At the time of the move, the boxes were not sealed in any way.

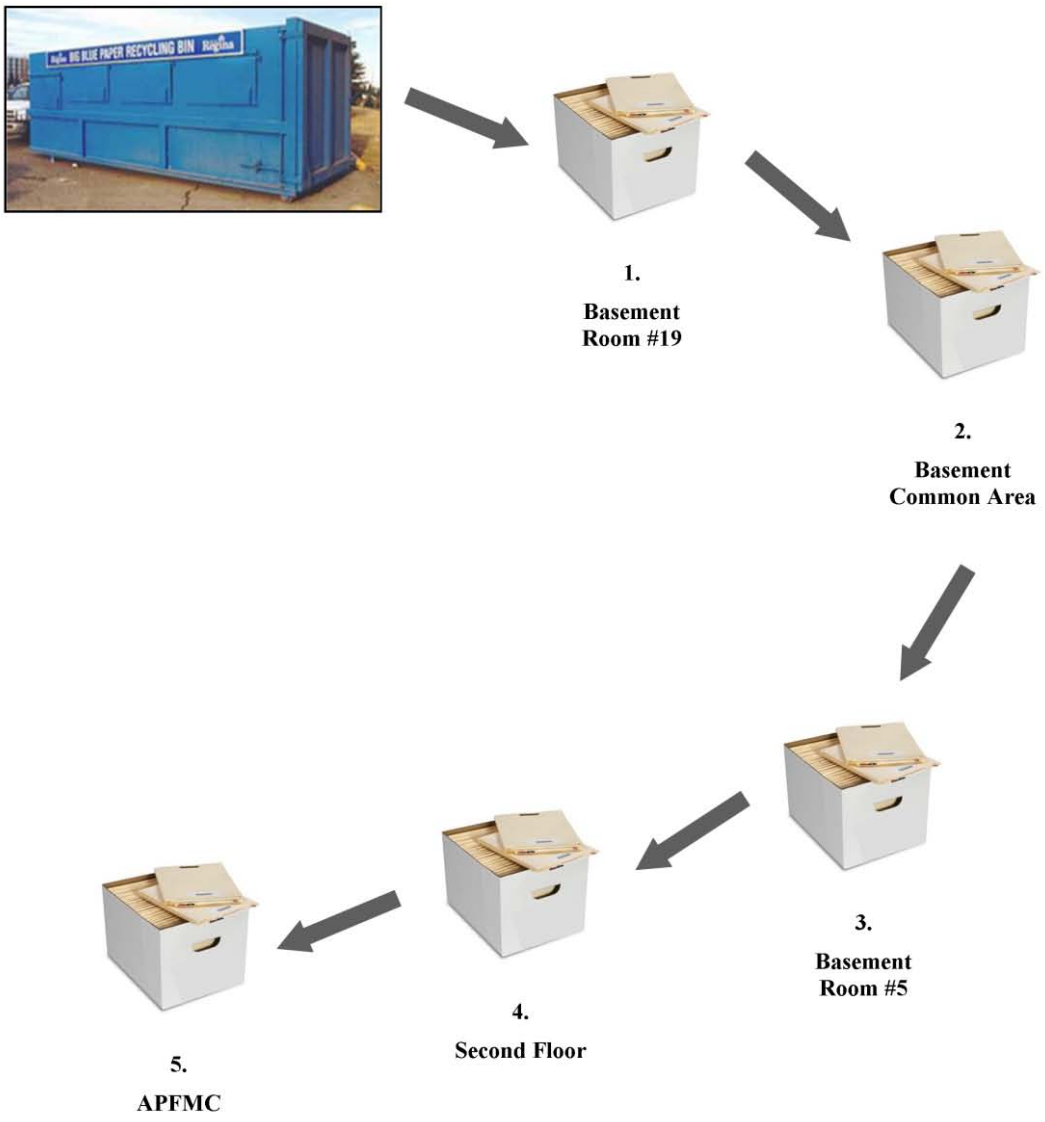
[28] We were advised that the boxes of records from the second floor were loaded into a van and driven to the basement door of Golden Mile Shopping Centre, transported by hand down the stairs, and placed in Room #5. Approximately 150 boxes were moved. It took six workers approximately four hours to move the boxes. No one from APFMC supervised or was present for the move.

[29] The boxes stored on the second floor of Gold Square had been moved there between 2005 and 2007.

5. APFMC

[30] Prior to their move to the second floor, the records were housed on the main floor of APFMC (see Schedule 2). Between 2005 and 2007, records were moved by staff, family members and friends to the second floor. At this point, the boxes of records were not sealed in any way. Also in August 2006, children of the owner of APFMC were hired to cull and move patient records. The children, aged 20 and 15 at the time, and their friends, assisted with culling and moving patient records to the second floor for storage.

i. Tracking the Boxes from End Point to Source



C. The Investigation

i. Authority

[31] The authority for our investigation into this matter is found in sections 42, 52 and 53 of *The Health Information Protection Act* (HIPA).[2]

> **42**(1) A person may apply to the Commissioner for a review of the matter where:
>
> ...
>
> (c) the person believes that there has been a contravention of this Act.
>
> …
>
> **52** The commissioner may:
>
> (a) offer comment on the implications for personal health information of proposed legislative schemes or programs of trustees;
>
> (b) after hearing a trustee, recommend that the trustee:
>
> (i) cease or modify a specified practice of collecting, using or disclosing information that contravenes this Act; and
>
> (ii) destroy collections of personal health information collected in contravention of this Act;
>
> (c) in appropriate circumstances, comment on the collection of personal health information in a manner other than directly from the individual to whom it relates;
>
> (d) from time to time, carry out investigations with respect to personal health information in the custody or control of trustees to ensure compliance with this Act;
>
> (e) comment on the implications for protection of personal health information of any aspect of the collection, storage, use or transfer of personal health information.
>
> …
>
> **53** The commissioner may:
>
> (a) engage in or commission research into matters affecting the carrying out of the purposes of this Act;
>
> (b) conduct public education programs and provide information concerning this
>
> Act and the commissioner's role and activities;
>
> (c) receive representations concerning the operation of this Act.

[2] *The Health Information Protection Act*, S.S. 1999, c. H-0.021.

[32] We provided formal notification in accordance with Parts VI and VII of HIPA to Dr. Ooi by way of letter dated March 28, 2011.

ii. Description of APFMC

[33] APFMC, a medical clinic, occupies more than 5,200 square feet on the main floor of Gold Square at 3992 Albert Street. The building is located on the south end of the block between Parliament Avenue and 25th Avenue in Regina, Saskatchewan. There is a pharmacy owned and operated by a pharmacist (hereinafter referred to as the Pharmacist), immediately adjacent to APFMC. Separate from Gold Square, and immediately to the northwest of Gold Square but in the same block is a shopping centre – Golden Mile Shopping Centre.

[34] The clinic is very busy. It would normally have approximately 14 physicians, including specialists working in the clinic. It has an x-ray facility. It has extended hours during the week and is open on weekends. To convenience patients, there are a number of specialists who would practice out of the clinic for one day every two weeks. The hospital emergency units would often transfer patients from the hospital to APFMC when they are overwhelmed and filled to capacity. It is estimated that close to 100 different physicians may have worked at APFMC at one time or another.

[35] At all material times, there was a large volume of patient records on APFMC premises. We have learned that health records were not shredded since the opening of APFMC in 1993 until approximately 2010. An additional storage room was built to the north of the pharmacy but accessible from APFMC for file storage (see Schedule 2). This was done in early 2007 by the contracted construction company

[36] The City of Regina maintains a large blue recycling bin that is located on the south end of Gold Square.

iii. Investigation Process

[37] Three staff from my office undertook this investigation over a four month period that commenced March 23, 2011, and continued to the issuance of this Report. In total, 43 individuals were interviewed, and eight of these individuals were interviewed multiple times. Our office interviewed ten employees of APFMC and four employees of the pharmacy. Through these interviews, we were able to identify 11 key individuals that worked for six separate companies (see Schedule 3), determined that two of these six companies had obligations under HIPA, and at least three were potentially functioning as information management service providers (IMSP).

[38] The process was documented through 72 photographs tagged with the time, date, and location. Most of the photographs were of storage facilities, medical clinic filing systems and assorted records.

[39] Also, my staff attended, on numerous occasions, off-site locations throughout Regina. These locations were determined to be involved in the storage of patient records belonging to APFMC.

[40] Further, we verified registration information of relevant trustees with the College of Physicians and Surgeons of Saskatchewan (CPSS) and the Saskatchewan College of Pharmacists (SCP).

[41] Upon our arrival at the scene on March 23, 2011, we seized a large volume of patient files and assorted papers containing phi which totaled approximately 25 boxes. Some of the material was still contained in original boxes, while other material was loose.

[42] Also on March 23, 2011, we spoke with an APFMC staff person who was uncertain if the records belonged to APFMC. In order to determine which trustee last had custody or control of the patient records we interviewed a number of other medical professionals whose offices were located in the vicinity of the recycling bin. This included a physical therapy clinic, five medical clinics, a medical laboratory clinic, and a radiology clinic.

[43] To determine when the records were discarded, we spoke to two witnesses from the community who saw the patient records in the recycling bin on March 23, 2011. The patient records were first seen in the recycling bin around 12:00 p.m. on Wednesday March 23, 2011. The timeline was verified by the City of Regina, and a private disposal company who indicated that the recycling bin had last been emptied at 12:00 p.m. the previous day.

[44] We conducted 16 corporation and land title searches through the Information Services Corporation of Saskatchewan.

[45] My staff attended two other medical clinics owned by the trustee and reviewed internal policies, procedures and record management practices. Early in the investigation, we determined that APFMC utilized multiple off-site facilities to store inactive patient records.

[46] We determined that APFMC utilized a storage space on the second floor of the Gold Square from approximately 2005 to 2007. APFMC stored approximately 150 boxes of patient records and furniture in the storage space. The space was accessible to a number of individuals not employed by the medical clinic. This included the Pharmacist, his maintenance person and a property manager for the Gold Square. As well, the space was accessible to construction workers who had been contracted to renovate the second floor in 2007 and realtors who were showing the space for lease to potential tenants in 2007.

III. ANALYSIS

A. Does HIPA Apply?

[47] HIPA is only engaged if three elements exist: (i.) there must be a trustee within the meaning of section 2(t); (ii.) there must also be phi within the meaning of section 2(m); and (iii.) the phi must be in the custody or control of the trustee. I will consider each element sequentially.

i. Who is the Trustee(s)?

[48] The definition of trustee is found in section 2(t) of HIPA.

> (t) "trustee" means any of the following that have custody or control of personal health information:
>
> (i) a government institution;
>
> (ii) a regional health authority or a health care organization;
>
> (iii) a person who operates a special-care home as defined in The Housing and Special-care Homes Act;
>
> (iv) a licensee as defined in The Personal Care Homes Act;
>
> (v) a person who operates a facility as defined in The Mental Health Services Act;
>
> (vi) a licensee as defined in The Health Facilities Licensing Act;
>
> (vii) an operator as defined in The Ambulance Act;
>
> (viii) a licensee as defined in The Medical Laboratory Licensing Act, 1994;
>
> (ix) a proprietor as defined in The Pharmacy Act, 1996;
>
> (x) a community clinic:
>
> (A) as defined in section 263 of The Co-operatives Act, 1996;
>
> (B) within the meaning of section 9 of The Mutual Medical and Hospital Benefit Associations Act; or
>
> (C) incorporated or continued pursuant to The Non-profit Corporations Act, 1995;
>
> (xi) the Saskatchewan Cancer Foundation;
>
> (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;
>
> (xiii) a health professional body that regulates members of a health profession pursuant to an Act;
>
> (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;
>
> (xv) any other prescribed person, body or class of persons or bodies;

[49] For HIPA to be engaged, the trustee must not only fall within one of the enumerated sub clauses in section 2(t), but must also have custody or control of the phi.

[50] Who is the appropriate trustee in this case?

[51] I have already described the records in the recycling bin as ones that relate to patients who were treated at APFMC in the past or records concerning patients treated by physicians who were associated with APFMC.

[52] Dr. Ooi has acknowledged that she is the trustee for purposes of HIPA and had effective custody and control of phi of patients, past and present, of APFMC. She qualifies as a trustee pursuant to section 2(t) of HIPA as a health professional licensed or registered pursuant to *The Medical Profession Act, 1981*.[3]

a. Role of Professional Corporation

[53] There is some evidence that Dr. Ooi carries on the practice of medicine at APFMC through her professional corporation. Dr. Teik Im Ooi Medical Professional Corporation was incorporated in this province effective July 11, 2008. Dr. Ooi is the sole director and shareholder of that professional corporation.

[54] In my view, the existence of the professional corporation does not affect Dr. Ooi's personal responsibility as a trustee for purposes of HIPA. The enabling legislation for medical professional corporations is *The Medical Profession Act, 1981*.[4]

[55] Section 37.8 provides as follows:

> **37.8**(1) The relationship of a person registered under this Act to a professional corporation does not affect the application of this Act or the bylaws to the person.
>
> (2) The liability of a person registered under this Act to a patient who receives services from the person is not affected by the fact that services were provided to the patient by the person as an employee of, or on behalf of, a professional corporation.

[3] *The Medical Profession Act, 1981*, S.S. 1981, c. M-10.1.
[4] Ibid.

[56] Section 37.9 provides as follows:

> **37.9**(1) Nothing in this Part affects any law applicable to the confidential, ethical or fiduciary relationships between a person registered under this Act and a patient who receives services from the person.
>
> (2) The relationship between a professional corporation and a patient who receives services from the professional corporation is subject to all applicable laws relating to the confidential, ethical and fiduciary relationships between the person registered under this Act who provides the services in the name of the professional corporation and the patient.
>
> (3) All rights and obligations pertaining to communications made to, or information received by, a person registered under this Act apply to the shareholders, directors, officers and employees of a professional corporation.

b. Trade Names

[57] I find that the trustee carried on business and continues to carry on business under the names *Dr. Teik Im Ooi Medical Professional Corporation, Albert Park Medical Clinic, Albert Park Medical Centre* and/or *Albert Park Family Medical Centre*. I will refer to the clinic or the business as APFMC.

c. How long has Dr. Ooi been the trustee of APFMC?

[58] Dr. Ooi has practiced medicine in Saskatchewan for almost 25 years. From 1986 to 1993, she practiced on a full time basis at Albert Park Medical Clinic at 4040 Albert Street, Regina. The clinic moved in early 1993 to 3992 Albert Street, Regina, where Dr. Ooi continued her practice. Although she has also worked at other clinics in Regina in which she had an ownership interest, she has worked primarily at APFMC.

[59] Dr. Ooi has asserted that until about 2008 when the only remaining partner voluntarily withdrew from the practice at APFMC, it was that partner who made the business decisions and her role was almost exclusively the clinical work with patients.

[60] In my view there are two separate issues that arise from this assertion which warrant analysis:

1. When did Dr. Ooi become a trustee of APFMC? And
2. What was Dr. Ooi's role with respect to patient records at APFMC?

1. When did Dr. Ooi become a trustee of APFMC?

[61] When APFMC started business at 3992 Albert Street (Gold Square) in 1993 there were four physicians who were equal partners. One of the partners was Dr. Ooi. By March 2003, two of the partners had left the practice. This left two remaining partners which included Dr. Ooi.

[62] This arrangement continued until Dr. Ooi entered into a *Partnership Dissolution Agreement* with her remaining partner on April 30, 2010. The effect of this was to make Dr. Ooi the sole legal and beneficial owner of all partnership assets effective April 1, 2010.

[63] Up until April 1, 2010, Dr. Ooi would have been a trustee for all purposes of HIPA with custody and control of the assets of APFMC jointly with the former partner. This arrangement would have continued from March 2003 until April 1, 2010. Neither would have had exclusive custody and control of the assets. The assets would include the patient phi in patient records of APFMC.

[64] Whatever arrangement was made for a division of tasks between the two partners and co-trustees would not operate to negate the custody or control of Dr. Ooi in terms of the patient records. I note that *The Partnership Act* provides as follows:

> **7** Every partner is an agent of the firm and his other partners for the purpose of the business of the partnership; and the acts of every partner who does any act for carrying on in the usual way business of the kind carried on by the firm of which he is a member, bind the firm and his partners, unless the partner so acting has in fact no authority to act for the firm in the particular matter, and the person with whom he is dealing either knows that he has no authority, or does not know or believe him to be a partner.[5]

[5] *The Partnership Act*, S.S. 1978, c. P-3.

[65] In practical terms, her former partner could not legally have walked away with the patient records without her consent. Any decisions he would have made with respect to the patient records, including arrangement with third parties for storage or destruction of patient records, would have been binding on Dr. Ooi consistent with *The Partnership Act*. This would be so whether she knew much or little about his arrangements for patient records. As a partner, if she chose to defer to her partner in terms of patient records and related decisions as she apparently has done, she is nonetheless liable for the consequences of bad decisions made by her former business partner.

[66] In short, Dr. Ooi was a custodian of the patient records at APFMC from the time the practice started at Gold Square in 1993 with three co-custodians. From March 2003, Dr. Ooi continued as a trustee[6] jointly with a single partner. Effective April 1, 2010, Dr. Ooi became the sole and exclusive trustee.

2. What was Dr. Ooi's role with respect to patient records at APFMC?

[67] Apart from the question of her legal responsibility as a co-trustee of the phi prior to April 1, 2010, her role in the decisions made by APFMC about patient files and records warrants consideration. In other words, what did Dr. Ooi actually know or what should she have known about the transactions involving the phi of patients?

[68] Dr. Ooi advised that until 2008, her former partner was effectively the 'managing partner' at APFMC. Nonetheless, Dr. Ooi was in APFMC on a full time basis working with the professional and non-professional staff since the clinic moved in 1993.

[69] I determined that Dr. Ooi would have been familiar with the volume of patient records in APFMC since she practiced in the clinic on a full-time basis steadily from 1986. This would have started at the original medical clinic at 4040 Albert Street, Regina.

[6] The term "trustee" would be appropriate commencing September 1, 2003 when *The Health Information Protection Act* came into force.

[70] I have learned that prior to 2010 APFMC patient records were not shredded on an ongoing basis but were archived on-site. Dr. Ooi would work amidst this large volume of patient files on a daily basis. It was Dr. Ooi who, according to the former Nurse/Office Manager, approved the move starting in 2005 of patient records from APFMC to the second floor storage room.

[71] The former Nurse/Office Manager advised that:

> [E]ven though he [Dr. Ooi's former partner] was a partner he wasn't here very often. He worked in the other clinic so I didn't really see him very often. I would be more apt to run something by Dr. Ooi and again it would be a verbal thing. I remember when we were using the space upstairs and I mentioned to her that we can't store things up there anymore, things meaning files and a few pieces of hardware but [the Pharmacist] and [Gold Square head landlord] are going to find us a place and then when we did I said we have a secure place in Golden Mile Shopping Centre, with two locks, no one can get in.

[72] The former Nurse/Office Manager would update Dr. Ooi on developments with respect to movement of patient records off-site. She specifically advised Dr. Ooi that patient records were moved to the second floor and then when they needed to be moved from the second floor to the basement of Golden Mile Shopping Centre.

[73] Dr. Ooi told me that she worked primarily at APFMC and was at the clinic most days. If that is so, she could not have been unaware of the month long construction in 2007 at APFMC which resulted in additional storage space for APFMC records.

[74] In November 2009, Dr. Ooi would have learned from her former Nurse/Office Manager that the Pharmacist next door to APFMC had signed a lease for storage of 250 boxes of APFMC patient records at an off-site location operated by a commercial storage facility in Regina. Her former partner had already left the practice so she would have been the only partner available to give instruction to the former Nurse/Office Manager.

[75] The former Nurse/Office Manager advised me that she would go to Dr. Ooi regarding off-site storage and for most issues that arose at APFMC because Dr. Ooi's former partner was busy at other clinics they jointly owned and was not often at APFMC. This was the case even before he withdrew from the practice of medicine.

[76] It was Dr. Ooi who hired the full time Office Manager for APFMC in April 2010. It was Dr. Ooi who was consulted in December 2010 as to whether or not to extend the lease for the storage of records at the commercial storage facility.

[77] I note that in the recent Report HR10-18 from Brian Beamish, Assistant Commissioner in the Office of the Information and Privacy Commissioner of Ontario, he addressed responsibility in the lifecycle of health records. He stated:

> Similarly, custodians who are taking over an established business cannot assume that their predecessor has fully complied with the requirements of the *Act*. It is imperative that custodians who become new business owners ensure that records of personal health information coming into their possession are catalogued accurately and then either securely stored or securely disposed of in accordance with relevant legislation, standards of practice and standards of professional conduct.[7]

[78] In the circumstances of APFMC, Dr. Ooi had a responsibility to learn of any arrangements made by her present and former partners with respect to off-site storage of patient records and to initiate any action required to ensure compliance with HIPA.

[79] I find, therefore, that not only was Dr. Ooi a co-trustee under HIPA for the period from March 2003 until April 1, 2010, but she was also involved in making decisions with respect to patient records throughout that same period.

[80] I find that Dr. Ooi would therefore be responsible for compliance by APFMC with the provisions of HIPA and would be the trustee at the material times with custody of the records of APFMC. Hereafter, I will simply refer to the trustee as Dr. Ooi.

ii. Is there Personal Health Information?

[81] The definition of phi is found in section 2(m) of HIPA. That provides as follows:

> (m) "personal health information" means, with respect to an individual, whether living or deceased:

[7] Information and Privacy Commissioner/Ontario, Report File No. HR10–18, at p. 8, available at: http://www.ipc.on.ca/images/Findings/HR10-18.pdf.

(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;

[82] Earlier in this Report, there is a detailed inventory of the materials seized from the recycling bin on March 23, 2011. As noted in the inventory, the materials include 2,682 patient files with various types of phi. There are also many other pieces of phi found in Medical Practitioner Reports, Daily Activity Reports and WCB claim related material. All of this information qualifies as phi.

[83] APFMC has asserted that billing records of a physician(s) are not subject to the same file recording requirements as medical charts. I acknowledge that the CPSS may treat different forms of records differently. That distinction however, has no significance when applying HIPA. HIPA defines phi broadly. From the perspective of a patient, I think that whether one's phi is found in a billing record or in a separate file folder makes no difference to the concern and prejudice which attaches to phi that ends up in a recycling bin.

[84] In total, the records seized contain approximately 180,169 items of phi including the approximate 2,682 patient files.

iii. Is the Personal Health Information in the Custody or Control of the Trustee?

[85] All of the records were for patients treated at APFMC or for patients of physicians who at one time or another worked at APFMC. Dr. Ooi has acknowledged that the records involved in this investigation were in her custody or under her control. She recently entered into an "Asset Purchase Agreement" for the sale of her practice at APFMC which describes these records as records in her control.

[86] I therefore find that HIPA is engaged on these facts and applies to Dr. Ooi and all of the records described above.

[87] In the course of this investigation, Dr. Ooi stressed that of the 180,169 pieces of phi, many of the included 1,087 comprehensive patient files had been brought into the clinic by a couple of physicians who had relocated their practices to APFMC. Those physicians subsequently left APFMC. Her view was that she should have a much diminished responsibility under HIPA since those files did not originate in APFMC. The short answer to that contention is that Dr. Ooi and her partners had a choice when physicians joined the clinic. They could have refused to accept trustee responsibility for those files and refused to store and deal with those records. On the evidence, Dr. Ooi and her partners manifested an intention to accept trustee responsibility for all of those files. They were moved and stored with other APFMC patient files. Significantly, when those physicians left the clinic they were not required to take their files with them. I find that for purposes of this investigation and Report, those patient files that were brought into APFMC by those other physicians became phi in the custody of Dr. Ooi.

B. The Most Relevant HIPA Provisions

[88] This investigation concerns a number of specific provisions of HIPA. These include sections 2(j), 9, 10, 16, 17, 18, 22 and 23. Those sections provide as follows:

> **2**(j) "**information management service provider**" means a person who or body that processes, stores, archives or destroys records of a trustee containing personal health information or that provides information management or information technology services to a trustee with respect to records of the trustee containing personal health information, and includes a trustee that carries out any of those activities on behalf of another trustee, but does not include a trustee that carries out any of those activities on its own behalf;
>
> …
>
> **9**(1) An individual has the right to be informed about the anticipated uses and disclosures of the individual's personal health information.
>
> (2) When a trustee is collecting personal health information from the subject individual, the trustee must take reasonable steps to inform the individual of the anticipated use and disclosure of the information by the trustee.
>
> (3) A trustee must establish policies and procedures to promote knowledge and awareness of the rights extended to individuals by this Act, including the right to request access to

their personal health information and to request amendment of that personal health information.

10(1) A trustee must take reasonable steps to ensure that the trustee is able to inform an individual about any disclosures of that individual's personal health information made without the individual's consent after the coming into force of this section.

(2) This section does not apply to the disclosure of personal health information for the purposes or in the circumstances set out in subsection 27(2).

…

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.

17(1) Not yet proclaimed.

(2) A trustee must ensure that:

(a) personal health information stored in any format is retrievable, readable and useable for the purpose for which it was collected for the full retention period of the information established in the policy mentioned in subsection (1);

and

(b) personal health information is destroyed in a manner that protects the privacy of the subject individual.

18(1) A trustee may provide personal health information to an information management service provider:

(a) for the purpose of having the information management service provider process, store, archive or destroy the personal health information for the trustee;

(b) to enable the information management service provider to provide the trustee with information management or information technology services;

(c) for the purpose of having the information management service provider take custody and control of the personal health information pursuant to section 22 when the trustee ceases to be a trustee; or

(d) for the purpose of combining records containing personal health information.

(2) Not yet proclaimed.

(3) An information management service provider shall not use, disclose, obtain access to, process, store, archive, modify or destroy personal health information received from a trustee except for the purposes set out in subsection (1).

(4) Not yet proclaimed.

(5) If a trustee is also an information management service provider and has received personal health information from another trustee in accordance with subsection (1), the trustee receiving the information is deemed to be an information management service provider for the purposes of that personal health information and does not have any of the rights and duties of a trustee with respect to that information.

…

22(1) Where a trustee ceases to be a trustee with respect to any records containing personal health information, the duties imposed by this Act on a trustee with respect to personal health information in the custody or control of the trustee continue to apply to the former trustee until the former trustee transfers custody and control of the personal health information to another trustee or to an information management service provider that is a designated archive.

(2) Where a former trustee fails to carry out the duties continued pursuant to subsection (1), the minister may appoint a person or body to act in place of the former trustee until custody and control of the personal health information is transferred to another trustee or to an information management service provider that is a designated archive.

(3) Where a trustee dies, the duties imposed by this Act on a trustee with respect to personal health information in the custody or control of the trustee become the duties of the personal representative of the trustee and continue to apply to the personal representative until the personal representative transfers custody and control of the personal health information to another trustee or to an information management service provider that is a designated archive.

23(1) A trustee shall collect, use or disclose only the personal health information that is reasonably necessary for the purpose for which it is being collected, used or disclosed.

(2) A trustee must establish policies and procedures to restrict access by the trustee's employees to an individual's personal health information that is not required by the employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.

(3) **Repealed.** 2003, c.25, s.13.

(4) A trustee must, where practicable, use or disclose only de-identified personal health information if it will serve the purpose.

[89] With respect to section 22, the related provision in *The Health Information Protection Regulations*[8] is section 4 that provides as follows:

> **4**(1) For the purposes of section 22 of the Act, the following are designated archives:
>
> (a) affiliates;
>
> (b) the Department of Health;
>
> (c) health professional bodies that regulate members of a health profession pursuant to an Act;
>
> (d) regional health authorities;
>
> (e) Saskatchewan Archives Board;
>
> (f) Saskatchewan Health Information Network;
>
> (g) University of Regina Archives;
>
> (h) University of Saskatchewan Archives.
>
> (2) Nothing in this section requires a designated archive to accept personal health information from a trustee.

[90] I view section 16 as one of the most important provisions in HIPA. Section 16 and our expectations in terms of compliance are outlined in some detail in our Investigation Report H-2005-002 from pages 78-112.[9]

C. Did the Trustee Have Policies and Procedures as Required by Section 16?

[91] HIPA prescribes that the trustee must establish policies and procedures to maintain administrative, technical and physical safeguards. These safeguards must protect the integrity, accuracy and confidentiality of the information. They must also protect against any reasonably anticipated threat or hazard to the security or integrity of the information; and the loss of, unauthorized access to, use or disclosure of the information.

[92] My office has seven years of experience overseeing the compliance efforts of Saskatchewan trustees with HIPA. Based on this experience, I suggest that, in considering the reasonably

[8] *The Health Information Protection Regulations*, S.S. 2005, c. H-0.021 Reg 1.
[9] Saskatchewan Office of the Information and Privacy Commissioner [hereinafter SK OIPC] Investigation Report H-2005-002, available at: http://www.oipc.sk.ca/reviews.htm.

anticipated threats or hazards, it is exceedingly unlikely that a medical clinic will be in compliance with HIPA requirements without:

(a) A specifically tasked privacy officer with a clear mandate and appropriate training;

(b) Extensive training of staff in HIPA requirements and provisions;

(c) Comprehensive, clear and practical written policies and procedures that are reinforced through leadership and training of staff;

(d) Written contracts with IMSP's that specifically address the requirements of section 17 and 18 of HIPA;

(e) Audit of use and disclosures of the phi; and

(f) Effective enforcement action to follow any breach.

[93] If a trustee fails to achieve satisfactory compliance with HIPA requirements, there is a greatly increased risk that patients' phi will fail to be protected from exposure to others who would have no legitimate need-to-know that phi without the consent of the patients. There is also a heightened risk that patient confidence in their health providers will be undermined and that this will negatively impact health outcomes. Such a lack of confidence could compromise the effectiveness of the electronic health record system now being rolled out in this province. These risks are a concern to the Canadian Medical Association (CMA). The CMA underscores the importance of privacy when it states:

1. Privacy, confidentiality and trust are cornerstones of the patient-doctor relationship.

   Health information is highly sensitive and is confided or collected under circumstances of vulnerability and trust. Trust plays a central role in the provision of health care and treatment; fulfillment of physicians' fiduciary obligations enables open and honest communications and fosters patients' willingness to share personal health information.[10]

[94] I note as well that the CPSS has addressed this issue in its Privacy Toolkit available on its website. This includes the following:

[10] *Principles for the Protection of Patients' Personal Health Information*, Canadian Medical Association, 2011, at p. 1-2, available at: http://policybase.cma.ca/dbtw-wpd/Policypdf/PD11-03.pdf.

> Health information is one of the most sensitive forms of personal information. Health information is collected primarily for reasons connected with patient care. Health information may be used for a number of other reasons including financial reimbursement, medical education, research, social services, quality assurance, risk management, public health regulation, litigation, and commercial purposes.
>
> Privacy is a major concern for physicians. The increased availability of patient records in electronic format has led to concerns about the potential misuse of personal information for purposes other than direct patient care. Without confidence that their privacy will be maintained, patients may refrain from disclosing critical information, may refuse to provide their consent to use personal health information for research purposes, or may simply not seek treatment.
>
> A 1999 Canadian Medical Association (CMA) survey found that 11% of the public held back information from a health-care provider due to concerns about whom it would be shared with or what purposes it would be used for. Wrongful release of information to third parties also may result in harm to the patient. The Supreme Court of Canada has recognized that Section 7 of the Canadian Charter of Rights and Freedoms includes the right to be free of the psychological stress resulting from the unauthorized disclosure of one's personal health information.
>
> ***The Saskatchewan Health Information Protection Act***
>
> The Saskatchewan Health Information Protection Act was proclaimed in September 2003 and governs the collection, use and disclosure of personal health information in the province. The Act defines and places obligations on health information "trustees", which include government, regional health authorities, health professionals including physicians and professional regulatory bodies. The HIPA applies to personal health information in any form, including both paper and electronic records.[11]

[95] Also the CPSS advised its members as follows:

> Physicians traditionally have been cognizant of the duty to maintain patient confidentiality and to create complete and accurate medical records. New legislation imposes some external controls to ensure that personal information is managed appropriately. The SMA and the College of Physicians and Surgeons of Saskatchewan recommend that all physicians familiarize themselves and their staff with their responsibilities to maintain medical records in compliance with emerging legislation governing personal privacy and freedom of information.[12]

[11] *Privacy in Saskatchewan Health Care: An Overview*, College of Physicians and Surgeons of Saskatchewan, available at: http://www.quadrant.net/cpss/privacy/privacy/background_materials.htm#Overview.
[12] *A Guide to Compliance with Privacy Legislation*, College of Physicians and Surgeons of Saskatchewan, available at: http://www.quadrant.net/cpss/privacy/privacy/guide.htm.

[96] In this regard, I also refer to the numerous HIPA deficiencies documented and discussed in two relatively recent Reports issued by this office: Investigation Report H-2010-001 (L & M Pharmacy Inc., Sunrise Regional Health Authority and Ministry of Health)[13] and the *Report on Systemic Issues with Faxing Personal Health Information*.[14]

[97] I next consider the extent to which Dr. Ooi is compliant with each of the three kinds of safeguards contemplated by section 16 of HIPA. In my Investigation Report H-2005-002 I stated:

> HIPA does not particularize the kinds of safeguards required to discharge the section 16 obligation.
>
> Our office views *Guidelines for the Protection of Health Information* produced by Canada's Health Informatics Association as the relevant standard or best practice for Saskatchewan trustee organizations.[15]

[98] The Canadian Health Informatics Association (COACH) Guidelines I referred to in that Report were those issued in 2004 which state:

> Specifically, the Guidelines have three major objectives:
>
> - To assist health organizations in minimizing the risk of unauthorized collection, use, disclosure, modification or destruction of their clients' health information;
> - To assist health organizations, especially health delivery organizations, in maximizing the integrity, availability and confidentiality of their clients' health information, and the efficacy of administering authorized access; and
> - To assist health organizations in protecting the privacy of users and providers.[16]

[99] COACH has consistently recommended, since at least 2004, a standard set of recommendations for privacy compliance when it comes to phi. There is a 2010 version of this document from COACH.

---

[13] SK OIPC Investigation Report H-2010-001.
[14] *Report on Systemic Issues with Faxing Personal Health Information*, SK OIPC, available at: http://www.oipc.sk.ca/What's%20New/FINAL-%20Report%20on%20Misdirected%20Faxes%20-%20NOV%2023,%202010.pdf.
[15] Supra note 9 at p. 97.
[16] *Guidelines for the Protection of Health Information*, Canada's Health Informatics Association, 2004, at p. 10.

[100] In addition, our office has from time to time supplemented the COACH guidelines and provided specific advice to the Ministry of Health and to trustees that we recommend as a means of complying with HIPA. This is done through published Investigation and Review Reports, tools on our website, presentations to trustee organizations as well as our monthly e-newsletter, the Saskatchewan FOIP FOLIO, and our Annual Reports. All of this material is available at our website: www.oipc.sk.ca.

D. Did the Trustee Comply with Section 16?

i. Administrative Safeguards

[101] To begin to answer this question, it is necessary to consider what those administrative safeguards would be and what is contemplated by section 16 of HIPA.

1. Designate a Privacy Officer

[102] The first in a list of seven Privacy Best Practices in the COACH *2010 Guidelines for the Protection of Health Information Special Edition* (COACH Guidelines) is to identify a privacy officer.

> Identify an individual in your practice who will be responsible for implementing privacy policies and procedures, managing privacy breaches and being the contact for privacy inquiries and complaints.[17]

[103] Item #6 of the CPSS *Checklist for Compliance with HIPA* (CPSS Checklist) states as follows:

> 6. The office must designate an individual (ideally a physician) to act as Privacy Officer to oversee management of personal information.
>
> - The Privacy Officer should be familiar with the obligations under HIPA.
> - This individual should develop and implement the privacy policies for the clinic and provide clinic staff with advice regarding HIPA compliance.

[17] *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records - 2010 Guidelines for the Protection of Health Information Special Edition*, Canada's Health Informatics Association, 2010, at p. 8.

- All employees should know who this person is.[18]

[104] This would be particularly important in a busy clinic with approximately 40 staff.

[105] Although not an explicit requirement in HIPA, over the last seven years our office has promoted this consistently as a best practice with trustees and trustee organizations. It would be very difficult to achieve a robust HIPA compliance regime in a trustee organization without an identified leader with that responsibility. Obviously, the privacy officer would need to be very familiar with HIPA as well as applicable requirements of the CPSS and recommendations of the Saskatchewan Medical Association (SMA).

[106] Prior to March 23, 2011, there was no designated privacy officer for APFMC. When staff were questioned about whom they would go to if they had questions or concerns concerning privacy or if a patient had questions or concerns about what was happening to their phi, there were plenty of conflicting responses. Some staff assumed that the former Nurse/Office Manager would be the appropriate person. The former Nurse/Office Manager minimized her role and clearly did not see herself as the privacy officer. Others assumed this would be raised with one of the intake staff or receptionists with a referral to the former Nurse/Office Manager if necessary. Others thought it would the clinic's Medical Director. Others assumed it would be one of the clinic owners, namely Dr. Ooi or her former partner. Some staff assumed that insofar as old medical records were concerned, the privacy officer would be the Pharmacist working next door given his very active role in off-site storage of patient records. Not only was all of this quite opaque to any patient but it was also very unclear to the staff who worked there. Although none of the staff of APFMC that we interviewed were familiar with HIPA, we were advised that for a period of time there was a registered nurse who worked at both APFMC and a large regional health authority (RHA) who apparently shared certain information she had learned at the RHA with some of APFMC staff. We understand that when this registered nurse left APFMC, there was no longer anyone in the clinic who understood HIPA. This is consistent with our discovery of a one page summary of HIPA that was

[18] *Checklist for Compliance with HIPA*, College of Physicians and Surgeons of Saskatchewan, at p. 2, available at: http://www.quadrant.net/cpss/privacy/privacy/checklist.htm.

included in APFMC policy binder that appears to have come from the RHA and was designed for RHA staff.

[107] In this case, Dr. Ooi described the former Nurse/Office Manager for APFMC from 2003 until 2010 as the person responsible for health records, managing access requests and correction requests. When we interviewed the former Nurse/Office Manager, she confirmed that it was her responsibility to orient new staff to confidentiality requirements. The former Nurse/Office Manager also oversaw the work of all clinic staff other than the physicians. Yet, it became immediately apparent she had virtually no knowledge of HIPA. She advised that she was completely unfamiliar with sections 9, 16, 17 and 18 of HIPA. She had no formal training with respect to HIPA and she provided no HIPA training to APFMC staff. She advised that she had no discussions with Dr. Ooi with respect to HIPA. She stated that HIPA training in her view was not needed since:

> [T]he confidentiality/privacy issues are just reinforced verbally and by posting information for staff.

[108] When I asked the former Nurse/Office Manager about her responsibilities for safekeeping and storage of patient files she responded:

> Well, I've always, because I'm a registered nurse, I've always known the importance of the safekeeping of people's information, so I don't think I really had to become aware of anything in addition to what I already knew. And with respect to other staff members, I mean it's reinforced all the time that confidentiality is important.

[109] When asked about specific training on HIPA her response was:

> Not specific training, no. But I would have to say that would've been deemed unnecessary. As a registered nurse I received two publications monthly, one from the SRNA [Saskatchewan Registered Nurses Association] and one from the Canadian Medical Association and very often they have information in them about the confidentiality issues. And as I mentioned as a registered nurse it's part of my life to maintain confidentiality. I don't need training about what to say outside of work and how important people's privacy is.

[110] The fact that the former Nurse/Office Manager didn't know the requirements of HIPA, yet saw no need to acquire a good working knowledge of this 2003 provincial law, actually mirrors the

attitude of the other key health care professionals we considered in this investigation. Both Dr. Ooi and the Pharmacist exhibited the same deficient understanding of the purpose, scope and requirements of HIPA. All three of these key players in this investigation conflated privacy with confidentiality and made what have proven to be very inaccurate assumptions about their responsibilities to their patients. As noted elsewhere in this Report, confidentiality is just a part of the privacy obligations created for trustees by HIPA.

[111] We interviewed a member of APFMC staff who worked in the clinic for many years and later became the full time Office Manager in April of 2010. She took over all of the record management responsibilities assigned to the former Nurse/Office Manager. She had no familiarity with HIPA and its requirements. She had received no instruction or orientation to HIPA. It appears that Dr. Ooi did not think to even bring HIPA to the new Office Manager's attention.

[112] Not only did the trustee fail to designate a privacy officer, but the fragmentation and confusion over decisions and responsibility relating to records stored off the premises of APFMC was a major data loss just waiting to happen. In the end, really no one was clearly responsible for records and files stored off-site. What was troubling was that in speaking to many different health care professionals, we found there was too little, if any at all, attention focused on the prejudice to patients resulting from the records in the recycling bin. Although many staff we interviewed would be quick to assert the importance of patient confidentiality, virtually everything that happened to approximately 150 boxes of patient records evidenced an alarmingly casual approach to patient records and the interests of those patients.

2. Create a Privacy Policy

[113] COACH recommends the following:

> Develop a privacy policy based on the requirements of your applicable privacy legislation as they pertain to collecting, using and disclosing personal and/or personal health

> information, including consent requirements, individual access to information and correction and security safeguards.[19]

[114] Our office has in the past urged trustees to create written policies and procedures.

[115] COACH has identified a number of reasons why a trustee should reduce its policies to written form. I note the following observation in the COACH Guidelines:

> The primary objectives of privacy and security policies are to:
>
> - Prevent and detect malicious activities from occurring
> - Assist in understanding the potential security exposures and risk
> - Educate, communicate and promote security responsibilities to all stakeholders
> - Comply with legislative, privacy and contractual requirements
> - Identify consequences of security policy violations
>
> If you do not have a documented policy, it will be difficult for you to communicate your privacy and security practices to patients, the public and external stakeholders or partners. On the other hand, if you do have a policy in place, you are clearly demonstrating that you have done your due diligence with respect to privacy and security. This is crucial if your practice is ever subject to a privacy audit, complaint, privacy breach or security incident.[20]

[116] Every Saskatchewan trustee should have a privacy policy that addresses the following:

- Accountability for phi;
- Purpose for collecting phi;
- Consent for collecting, using and disclosing phi;
- Accuracy and correction of phi;
- Retention and destruction of phi;
- Privacy breach management;
- Use and disclosure audits;
- Use and disclosure control;
- Individual access to information;
- Privacy complaint management; and
- Enforcement mechanisms.

[19] Supra note 17 at p. 8.
[20] Ibid. at p. 9.

[117] The short answer is that in terms of written policies and procedures, what does exist at APFMC is lamentably weak. All that APFMC could produce when asked about section 16 was a single binder described by staff as the Policy Manual. This was kept in the staff room of APFMC. Some of APFMC staff we spoke with were completely unfamiliar with this manual. With it was a Communications Binder that was intended to be a means of sharing information with staff from time to time. Some staff were aware of these two resources. We were told that these were not only available to all staff in the clinic, but that staff were also encouraged to periodically check these resources. APFMC provided us with what is purported to be a true copy of the Policy Manual.

[118] The only reference to HIPA in the Policy Manual is a single sheet entitled [name of health region] *Health Region – The Health Information Protection Act (HIPA) Summary*. The single page is a very skeletal and general overview with the following headings:

> What is Personal Health Information?
> Who is a Trustee?
> Rights of Individual
> Important to remember

[119] The only contact information is a note at the bottom of the sheet as follows:

> For more information:
> - See the [name of health region] Privacy Office website (click on [health region] intranet/Departments/Privacy Office).
> - Contact the HIPA Education Coordinators, [name and phone numbers for two health region trainers].

[120] As noted earlier in the Report, we were told by several staff in our interviews that there had been an employee who had also worked at an RHA until June 2010, and had brought some materials with her from the RHA with respect to HIPA training. This employee was a registered nurse and was apparently responsible for keeping the Policy Manual up to date.

[121] I assume that this is the source of this document in the Policy Manual. None of the ten APFMC staff members we interviewed could recall any other written policies or procedures related explicitly to HIPA compliance.

[122] This document was presumably intended to be merely an initial introduction to HIPA. It is insufficient to enable health care professionals and support staff to develop a comfortable understanding of what they can do and must not do with phi. It is simply too general to achieve that goal. The reference "for more information" would be useless to a non-medical staff person in APFMC since they would not have access to the RHA's Intranet. Given the wealth of material and information available to Saskatchewan health trustees, such a weak effort is inexcusable.

[123] The other relevant item in the Policy Manual is the *Record Retention* piece. This apparently was created by the Canadian Medical Protective Association (CMPA) in March 2003. Since it appears to have been written for a national audience there is no reference to HIPA. Under the heading *Storage and disposal*, it states:

> It is required that clinical records be kept not only intact but also in a safe and secure place. If at all possible, they should be kept under the physician's or estate's control. The records are the property of the physician or the estate, and in the event of later medico-legal difficulty, it will be the physician or estate who will need the record without delay.
>
> When clinical records no longer need to be retained, they should be destroyed by burning or shredding. They should not simply be thrown out with the garbage where they may fall into the wrong hands. This has indeed occurred with very unhappy results. However, before destroying any records it would be very wise to make a list of the names of those patients.
>
> As a general practice you are advised **not** to let the **original** files out of your control.
>
> [emphasis in original]
>
> [This last sentence as it appeared in the copy we were provided was represented to be a true copy. We note that this sentence was circled by pen or pencil by hand.]

[124] The other items in the Policy Manual dealt with topics such as: Job Descriptions, Dress Code, Abuse/Harassment, Documentation, Oral Hygiene, Incident Reporting, Employee

Performance, Nursing Standards 2000, Telephone Advice, Immunizations/Illnesses, Nursing Articles (2), Visual Acuity, Internal Memos, and PT/NR Tracking. Of interest is that most of the materials with respect to these other headings are detailed and granular. Much of the material is much older than 2003 when HIPA came into force. For example, the *Standards and Foundation Competencies for the Practice of Registered Nurses* (the Standards) has an effective date of 2000. In this regard, I note the recommendation from COACH that a best practice for privacy security policy is that they be reviewed and updated regularly (at least annually). In any event, the Standards document makes no explicit mention of privacy or confidentiality of patients and the nurses' obligations in that respect.

[125] Notwithstanding the above noted admonition in the CMPA piece in the Policy Manual, no record was made of the names of patients whose files were included in the boxes sent from the second floor of Gold Square to the basement of Golden Mile Shopping Centre. There was no kind of index to allow APFMC to have any idea of which patients' information was in the off-site storage.

[126] In the Policy Manual, there is an undated section on *Documentation* which makes no reference to HIPA. In fact, some of the material in this section is dated 1997. It appears that all of the material in this section predated HIPA since the only consent discussed relates to treatment and not to patient phi. Most of the material is focused on documenting consent for treatment. There is no mention of consent with respect to collection, use or disclosure in a HIPA context. The policy is described as follows:

> **POLICY: DOCUMENTATION**
>
> Documentation is an essential part of safe and effective patient care. It is therefore necessary to have a system in place whereby all members of the Albert Park Family Medical Centre interdisciplinary team effectively record all the care given and the patient's response. Documentation facilitates communication, accountability, evaluation of services and research.
>
> PROCEDURE:
>
> 1. Entries are legible, written in ink, dated and signed/initialed (including the job description of the writer).

2. Entries will describe assessment, interventions, client responses and outcomes and health teaching.
3. Entries are written by staff who performed the service.
4. Entries are concise, accurate and relevant without subjective terms.
5. Client records are confidential.

[127] There is a section on job descriptions. In the Receptionist Job Description the ninth item out of 13 enumerated duties says:

> It is very important to protect the patient's privacy - shred all information with names on, including old messages, labels, etc.

[128] Dr. Ooi never attended any workshops or training sessions with respect to HIPA. She was not familiar with HIPA resources available at the CPSS, SMA, the Ministry of Health or our office.

[129] Dr. Ooi, the new Office Manager and the former Nurse/Office Manager all confirmed that there are no other written policies and procedures. APFMC never utilized any of the materials available on the CPSS or SMA website. These include on the CPSS website, a Privacy Toolkit. The elements of that Privacy Toolkit are as follows:

1) Privacy in the Health Care System: An Overview
2) A Guide to Compliance with Privacy Legislation
3) Five Principles for Protecting Patient Information
4) Checklist for Compliance with HIPA
5) Guide to Ensuring the Security of Patient Records
6) Guide to Ensuring the Accuracy of Patient Records
7) CMA/SMA Privacy Poster
8) Patient Brochure
9) Confidentiality Agreement for Employees
10) Confidentiality Agreement between Medical Practice and Service Provider
11) Confidentiality Agreement between Medical Practice and File Storage Facility
12) Confidentiality Agreement between Medical Practice and File Destruction Facility
13) Patient's Request for Access to Health Information

14) Patient's Request for Amendment of Personal Information
15) Links to Privacy Resources[21]

[130] Virtually the same materials, or at least most of them, are also available on the website of the SMA.

[131] In this regard, I refer Dr. Ooi to my statement in my Investigation Report H-2010-001 about privacy material and tools on the website of the regulatory college, the CPSS. In that case, I was considering a pharmacist who indicated that he was unaware of certain privacy resources and tools available on the website of the SCP. I stated in that Report:

> My view is that whether or not [the Pharmacist] specifically recalls reading each of these documents, he must be taken to have constructive knowledge of each of them. They are publications of his College, they are readily available on the College website and as a pharmacist he has a responsibility to make himself familiar with the policies, procedures that his regulatory College is mandated to create.[22]

[132] I apply the same reasoning in this case and am of the view that Dr. Ooi had constructive knowledge of the resources available to her on the website of the CPSS.

[133] This clinic has never utilized any of the materials developed by COACH or by CPSS.

[134] Dr. Ooi asserts that, despite the absence of written policies and procedures, HIPA does not require written policies and procedures. She claims that there is a general understanding among her staff about confidentiality and that should be sufficient. Unfortunately, this inaccurate and naïve view was not unique to Dr. Ooi. It was also shared by her former Nurse/Office Manager, her new Office Manager and the Pharmacist, whom she utilized as an IMSP in arranging for transportation and storage of a large quantity of her patient records.

[21] *Privacy Tool Kit*, College of Physicians and Surgeons of Saskatchewan, available at: http://www.quadrant.net/cpss/privacy/privacy/index.htm.
[22] Supra note 13 at [71].

3. Privacy Procedures

[135] The COACH recommendation is as follows:

> Establish privacy procedures to serve as an extension of your privacy policy. Procedures should provide you and your staff with consistent steps for managing 1) complaints, breaches of privacy and security incidents; 2) individual access to and correction of personal health information; and 3) consent.[23]

[136] In order to satisfy HIPA, the procedures required by any trustee would need to be more comprehensive. Such procedures must also address collection, use and disclosure practices as well as steps taken to respect the general duties in sections 9, 10, 16, and 23 of HIPA. CPSS offers a number of useful forms and checklists in its online Privacy Toolkit.

[137] The complete absence of any procedures for off-site storage of APFMC patient records became evident in many ways.

[138] The former Nurse/Office Manager, at no time prior to the appointment of a new full time Office Manager for APFMC on April 15, 2010, ever viewed the storage area for patient records in the basement of Golden Mile Shopping Centre. No one from APFMC supervised or was even present for the move of 150 boxes from the second floor to the basement storage Room #5. No inventory was taken of the patient files or the boxes before they were transported to Golden Mile Shopping Centre basement. No one from APFMC apparently had any awareness that the landlord of Golden Mile Shopping Centre decided to cut off the lock to Room #5 in the winter of 2007 and move out the 150 boxes to the open, common area in the basement while repairs were undertaken. No one from APFMC today has any personal knowledge as to what happened to approximately 125 boxes that were moved to the basement and are still unaccounted for. No one from APFMC was aware that the boxes of records had been in an unlocked room for the last three years before 25 boxes were tossed in the recycling bin.

[23] Supra note 17 at p. 8.

[139] In addition, off-site storage at the commercial storage facility for other patient records (approximately 250 boxes) was arranged by the Pharmacist. The Pharmacist signed the contract, had the only key and made arrangements whereby he or someone tasked by him would go to the rented storage space in east Regina to retrieve files when required by APFMC. The files in this storage space were not subject to an adequate system for identification and retrieval. I was told of one occasion when an incorrect box was retrieved by the pharmacy maintenance person even though he was following the explicit instruction of APFMC. APFMC later realized the required file was on-site and not at the commercial storage facility.

[140] As an additional safeguard, the Ontario Information and Privacy Commissioner suggests that a trustee should consider a provision in their record destruction policies that employees must obtain internal authorizations prior to the destruction of phi.[24] The trustee could develop a process to authorize the destruction of batches of records on a single authorization. The authorization should include a signature field for sign-off and the level of authorization required.

[141] Dr. Ooi had a remarkably relaxed view of the 'need-to-know' requirement of section 23 of HIPA. Sometimes described as the limiting use and disclosure rule, section 23 provides as follows:

> 23(1) A trustee shall collect, use or disclose only the personal health information that is reasonably necessary for the purpose for which it is being collected, used or disclosed.
>
> (2) A trustee must establish policies and procedures to restrict access by the trustee's employees to an individual's personal health information that is not required by the employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.

4. Agreements

[142] The COACH recommendation is as follows:

[24] *Get Rid of it Securely to Keep it Private - Best Practices for the Secure Destruction of Personal Health Information*, Information and Privacy Commissioner/Ontario, October 2009, at p. 9, available at: http://www.privacybydesign.ca/content/uploads/2009/10/naid.pdf.

> Enter into agreements before sharing any personal health information with a third party. Agreements protect you and your practice by establishing the terms and conditions of providing personal health information that you may receive from or share with others, including centralized databases and other healthcare providers. Agreements can also establish accountability between you and electronic service providers, including network providers.[25]

[143] The CPSS Checklist addresses this in the fourth bullet under #5 which indicates that:

> If an information manager (computer support person, off-site storage company, etc.), has access to patient information, a written agreement should be in place whereby the information manager agrees to ensure confidentiality and limit access to the records.[26]

[144] The CPSS, in its Privacy Toolkit, offers a number of sample contracts including:

- Confidentiality Agreement between Medical Practice and Service Provider
- Confidentiality Agreement between Medical Practice and File Storage Facility
- Confidentiality Agreement between Medical Practice and File Destruction Facility[27]

[145] APFMC had no written agreements with third parties to deal with the provision of service for file storage or file destruction. In accordance with the CPSS, confidentiality agreements should have been considered by APFMC for at least some of the following:

- The Pharmacist;
- The pharmacy maintenance person;
- The other pharmacy staff who had access to the second floor storage room;
- Labourers hired by the Pharmacist to move APFMC records;
- The commercial storage facility;
- The owner of Gold Square;
- Property manager of Gold Square;
- Owner of Golden Mile Shopping Centre and staff who had access to the basement storage room;
- The contracted maintenance company;
- The contracted construction company and staff;

[25] Supra note 17 at p. 8.
[26] Supra note 18 at p. 2.
[27] Supra note 21.

- Realtors and potential tenants that were viewing the second floor storage room for potential lease;
- Contractors doing renovations in the basement of Golden Mile Shopping Centre from 2007 to March 23, 2011;
- Dr Ooi's children and their friends; and
- The staff that set up the 'haunted house' display in the fall of 2010.

[146] Dr. Ooi needed to have taken the steps recommended by the CPSS and COACH to minimize the risk of a breach such as the exposure of the patient records to the estimated 3,600-4,800 persons viewing the Halloween 'haunted house' in the basement of Golden Mile Shopping Centre.

[147] The problem with not having such agreements is all too evident in this investigation. Insofar as the key individuals involved in handling the boxes of patient files and records are concerned, there is no clear accountability for the 180,169 items of patient phi that ended up in the recycling bin. We encountered conflicting expectations and confused understanding of roles and responsibilities of those involved. That confusion contributed directly to the privacy breach discussed in this Report. The kind of agreement(s) contemplated by sections 16, 17 and 18, the CPSS/SMA Privacy Toolkit and the COACH Guidelines would likely have prevented that confusion.

5. Privacy Awareness and Education Program

[148] In *A Guide to Compliance with Privacy Legislation*, the CPSS has stated:

> The SMA and the CPSS recommend that all physicians familiarize themselves and their staff with their responsibilities to maintain medical records in compliance with emerging legislation governing personal privacy and freedom of information.[28]

[149] Our office has consistently stressed, for the last seven years, the importance of providing all staff of trustee organizations with practical, accessible, concrete and granular information about what they must do to comply with HIPA in the course of collection, use, disclosure of phi, as well as access to and correction of that phi. Unlike Alberta, Ontario and

[28] Supra note 12.

Newfoundland, no detailed manual has been prepared by our Ministry of Health to assist all trustees and their employees to navigate what can be a somewhat complicated law. Too much of the early education material produced and used by trustees amounted to little more than repeating the general wording in the statute itself when what trustees needed were checklists, decision trees, case studies, template letters, forms and charts. We have urged trustees to focus initially on the four predictable problem areas of security, access, consent and disclosure.

[150] Despite the recommendation of both the CPSS and the SMA, APFMC staff received no adequate HIPA training to enable them to have a comfortable understanding of what they can do and what they must not do. Yet, how else could a trustee be satisfied that all staff are aware of the privacy protection practices that a trustee has implemented and of their individual accountabilities in complying with privacy policies and procedures? We interviewed ten members of APFMC staff and although they seemed familiar with the general concept of confidentiality, they were quite unfamiliar with the additional requirements created by the Legislative Assembly in 2003 with the proclamation of HIPA. We determined that no staff of APFMC were ever required to provide a confidentiality acknowledgement. Dr. Ooi herself had no HIPA training, formal or informal.

[151] Dr. Ooi rated her familiarity with HIPA as between poor and adequate:

> I had some knowledge but I didn't put it under the HIPA context.

[152] She acknowledged that she was relying on the general confidentiality culture that she would be familiar with as a physician.

[153] Having spent four hours speaking with Dr. Ooi, I have no hesitation in concluding that she was completely unfamiliar with HIPA and simply relied on a generalized understanding of confidentiality. Confidentiality is a useful part of privacy but only a part. I discussed with Dr. Ooi the differences between the two terms, which are addressed in our Investigation Report H-2005-002[29] and in the *Glossary of Common Terms – HIPA*.[30]

[29] Supra note 9.

6. Consent/Communication with Patients

[154] The advice from COACH is as follows:

> Identify the consent requirements that apply in your jurisdiction. (Your professional college can help you with this matter.) While implied consent allows the collection, use and disclosure of personal health information in healthcare delivery within the circle of care, best practice suggests, and in some cases, legislation requires, that you make your patients aware of your privacy practices. Therefore, you should provide patients with the following information:
>
> 1. The purposes for which you collect their personal information
> 2. How the information will be used
> 3. With whom the information will be shared
> 4. When the consent of patients will be sought
> 5. How patients can request access to and correction of their personal health information
> 6. How you manage privacy breaches and security incidents
> 7. How patients can register a complaint about your privacy practices or a suspected breach of their privacy
>
> The best method for informing your patients is by posting a patient privacy notice or providing a handout. [31]

[155] On the evidence, there was no express consent provided by patients for the movement of records. I find there would have been no implicit consent for the movement of the patient records in such a way that they would be exposed to the long list of persons who had no need-to-know this phi. Consent for what happened to the patient records, as documented in this Report could not be reasonably inferred from patients presenting for diagnosis, treatment or care.

[156] In its discussion of communicating information about privacy policies and procedures to patients COACH advises that:

> The best method for informing your patients is by posting a patient privacy notice or providing a handout.[32]

---

[30] *Glossary of Common Terms – HIPA*, SK OIPC, available at: http://www.oipc.sk.ca/Resources/HIPA%20Glossary%20-%20Blue%20Box.pdf.
[31] Supra note 17, at p. 8.

[157] Sections 9 and 10 of HIPA have not been addressed by Dr. Ooi. Despite the emphasis placed on these provisions in our Investigation Report H-2005-002, there have been no posters conspicuous to patients in the reception room or hallways of the clinic. There were no brochures or written material for patients or staff that describe even in general terms the rights of patients under HIPA and how that law has substantially added to the traditional understanding of confidentiality. A patient could attend at the clinic, receive a medical service and depart without even the existence of HIPA being brought to their attention by anyone or anything.

7. Security Protections

[158] The advice from COACH is as follows:

> Ensure that reasonable and appropriate physical, administrative and technical safeguards are in place to protect personal information. Safeguards will ensure the integrity, confidentiality and availability of personal information and protect it from being improperly accessed, altered or destroyed. [33]

[159] The advice from CPSS in the document entitled, *Five Principles for Protecting Patient Information* is as follows:

> [P]hysicians have a duty to keep records secure against unauthorized use or disclosure, and to maintain and retain records for an appropriate length of time.[34]

[160] Also in the same CPSS document is the statement that "physicians have a duty to control disclosure of information in the record".[35]

[161] A number of items in the CPSS' *Checklist for Compliance with HIPA* are relevant to this investigation. This includes the note at #5 that "All personal information (registration data,

[32] Ibid. at p. 8.
[33] Ibid. at p. 8.
[34] *Five Principles for Protecting Patient Information*, College of Physicians and Surgeons of Saskatchewan, available at: http://www.quadrant.net/cpss/privacy/privacy/principals.htm.
[35] Ibid.

billing data, health records, staff/employee records, etc.) should be kept appropriately secure."[36]

[162] Also in the same Checklist the fourth bullet under #5 indicates that "[i]f an information manager (computer support person, off-site storage company, etc.), has access to patient information, a written agreement should be in place whereby the information manager agrees to ensure confidentiality and limit access to the records."[37]

[163] Certainly, one of the problems in this case was the number of times that boxes of patient records and phi were moved. A major shortcoming was the failure of Dr. Ooi to have taken an inventory of the patient records before they left APFMC premises. This would have allowed a further inventory to be taken after each of the next three moves to ensure all records were accounted for. This would have also avoided the troubling uncertainty as to the disposition of some 125 boxes of patient records that the trustee cannot satisfactorily account for today. I don't know how else a trustee can be confident that records do not go missing as happened in this case. The failure to undertake an inventory of the patient phi before it was transferred from APFMC premises meant a failure to safeguard phi and represents a breach of section 16 of HIPA.

[164] Another helpful resource is the book titled, *The Personal Health Information Protection Act - Implementing Best Privacy Practices*. This includes the following:

> Enforcing Contractual Privacy Provisions
>
> Health information custodians' responsibilities do not end after signing a contract with an agent. Rather, custodians should monitor whether their agents are meeting the privacy requirements in their contracts. Effective monitoring entails setting dates for agents to report on their compliance, visiting agents' sites to evaluate privacy protection, meeting with agents regularly to discuss how current procedures are working and develop ways to remedy any issues, and notifying agents of any changes in the custodian's own information practices that agents will be asked to adopt.

[36] Supra note 18 at p. 2.
[37] Ibid. at p. 2.

> All privacy requirements in a health information custodian's contracts with its agents should be strictly enforced. If agents refuse or fail to resolve discovered problems, court action or ending the contract may be the custodian's only options.[38]

[165] I adopt these suggestions which should apply to Saskatchewan trustees who utilize the services of a contractor or IMSP. I find these suggestions are consistent with sections 16, 17 and 18 of HIPA.

[166] I find that in a host of ways, Dr. Ooi failed to ensure reasonable and appropriate physical and administrative safeguards to protect the phi seized from the recycling bin on March 23, 2011.

[167] This item is also considered in more detail later in this Report in the context of the analysis of sections 17 and 18 of HIPA.

ii. Summary of Section 16 Administrative Safeguards

[168] In assessing what was done by Dr. Ooi in this case against the privacy best practices promoted by the CPSS, SMA and COACH, and assessing the compliance or non-compliance with HIPA by Dr. Ooi, I have determined the following:

- Dr. Ooi had no privacy officer and no single individual with clear responsibility for HIPA compliance. APFMC had a fragmented and diffuse set of conflicting responsibilities among too many staff.
- Dr. Ooi failed to have written privacy policies or indeed any privacy policy for the collection, use, disclosure, access to and correction of phi of patients.
- Dr. Ooi failed to have written procedures or any clear procedures for the transport and storage of patient records once they left the premises on the main floor of Gold Square.
- Dr. Ooi failed to provide privacy awareness and education programs to new hires or in-service training for existing employees beyond some very general information about confidentiality independent of HIPA.
- Dr. Ooi failed to provide patients with any information about their HIPA rights and processes including how APFMC manages privacy breaches and security incidents.

[38] *The Personal Health Information Protection Act - Implementing Best Privacy Practices*, Scott, Graham. et al., LexisNexis Butterworths: Ontario, 2005, at p. 97.

- Dr. Ooi failed to undertake adequate security arrangements for the 150 boxes of patient records that were transported from the second floor of Gold Square to the basement of Golden Mile Shopping Centre.

- Dr. Ooi failed to have any written agreements as contemplated by the Privacy Toolkit produced by CPSS and the COACH Guidelines before turning over or exposing to third parties unsealed boxes of phi of patients including:
  - The Pharmacist, his staff, both professional and non-professional, and two day labourers;
  - Dr. Ooi's children aged 20 and 15 years and at least two of their friends who were tasked with culling patient files in the summer of 2006;
  - Realtors and prospective tenants who viewed the second floor storage area;
  - The Gold Square landlord and his staff;
  - The contracted construction company employees who moved the records from the second floor location to the basement of Golden Mile Shopping Centre;
  - The staff and contractors of Golden Mile Shopping Centre;
  - Whoever moved approximately 125 boxes of patient records to places unknown;
  - The persons who created the 'haunted house' display in the basement of Golden Mile Shopping Centre;
  - The estimated 3,600 to 4,800 persons who paid admission to tour the 'haunted house' in the basement of Golden Mile Shopping Centre between October 7, 2010 and October 31, 2010;
  - The workers who ultimately moved 25 boxes from the basement to the recycling bin from which my office seized the records; and
  - Any persons who attended at the recycling bin during the day of March 23, 2011, where the records of patients were on clear display to anyone who looked into the recycling bin prior to 4:50pm when our office seized them.

[169] This meant that Dr. Ooi had effectively failed to protect the phi in her custody long before it ended up in the recycling bin on March 23, 2011. Her actions or omissions, directly contributed to the cascading series of errors and breaches documented in this Report.

[170] In the course of our investigation, we encountered a surprising attitude and belief among those who had a responsibility to comply with HIPA either as a trustee or employees of a trustee. Dr. Ooi has asserted that there is no privacy breach or HIPA breach unless and until it can be proven that patient phi was actually viewed by persons who were not health trustees. There is a problem with such a belief. A HIPA breach occurs when a trustee fails to put in place the

appropriate policies and procedures required by section 16 of HIPA regardless of whether the phi can be proven to have been viewed by a third party.

[171] This problematic misconception contributed significantly to the kinds of breaches mapped in this Report.

iii. Physical Safeguards

[172] Dr. Ooi failed to take reasonable measures in terms of physical safeguards to protect the patient phi.

[173] The room on the second floor of Gold Square used for storage was locked but was also used for storage of the pharmacy's retail products such as confectionary items. This meant that from time to time non-professional staff of the pharmacy would have access to the room to deliver and remove pharmacy inventory and transport it to the pharmacy on the main level. The former Nurse/Office Manager advised me that for the period of 2005-2007, she did not have a key to the second floor storage room. The only key was in the pharmacy. APFMC staff would need to go to the pharmacy in order to get the key to gain access to the second floor storage room where their patient files were stored. Also, the landlord was attempting to rent the storage space to a new tenant so there would have been realtors and prospective tenants with the opportunity to look at APFMC records stored there.

[174] Working in reverse from March 23, 2011, the records ended up in a recycling bin where they were exposed to anyone who had reason to go to the bin on that day. We were advised by one witness that patient files fell out of the recycling bin when this individual opened one of the sliding doors. They were transported there from the basement of Golden Mile Shopping Centre where they had been for approximately three years in an unsecured portion of the basement and available to anyone in that basement who chose to go through them. They were in this unsecured state when Golden Mile Shopping Centre held a Halloween 'haunted house' event whereby men, women and children were invited to enter upon payment of a fee, between October 7th and October 31st, 2010. Anyone entering the basement to either set up or visit the

'haunted house' display would have had the opportunity to peruse the large volume of patient records and papers in that same area.

[175] Approximately 150 boxes of patient records had been moved by employees of the contracted construction company who apparently were never required to sign any kind of confidentiality undertaking and yet were not supervised in any way by any staff member of APFMC. In fact, it was the representative of the Gold Square owner who supervised and assisted the move of patient records to the Golden Mile Shopping Centre basement, then went down after the boxes had been moved to inspect the room and ensure that the room was properly locked. He advised that he took a key to the basement storage room to the former Nurse/Office Manager the day after the move and saw her put the key in a drawer in APFMC. She denied ever seeing or having a key to the basement storage area.

iv. Technical Safeguards

[176] Since we are dealing only with paper records in this investigation, there is no need to consider technical safeguards.

[177] This is an area that obviously will be fully engaged as Saskatchewan moves to electronic medical records in physician clinics and an electronic health record for all persons in the province. Once achieved, hopefully the kind of breach considered in the Report should become much less frequent. Nonetheless, there are new risks associated with thousands of trustees across this province being accredited users of the electronic health record infrastructure. The kinds of deficiencies documented above in the context of considering section 16 of HIPA requirements will continue to be of prime importance. Patient privacy will continue to be at risk unless and until all trustees and their staff have the appropriate training, policies and procedures to ensure satisfactory compliance with HIPA. The experience of our office suggests that Saskatchewan has a considerable distance yet to go to achieve that objective.

E. Did the Trustee Comply with Section 17?

[178] It appears that Dr. Ooi had a retention and destruction policy as discussed above but didn't follow it. This originally provided that all health records shall be retained for a minimum of 10 years after the discharge date. This was changed to 15 years in or about 2003.

[179] On June 25, 2010, APFMC decided to destroy 25 to 30 boxes of old patient files located at APFMC by sending them to a professional record destruction company. This appears to have been the first time in the history of APFMC that old patient files had been shredded in a bulk fashion. There was no record kept of which records were being sent for shredding. There was no formal agreement entered into with the contractor. According to the new APFMC Office Manager, this was arranged solely by telephone and the transmittal of a request for their boxes of files to be picked up for shredding. Dr. Ooi should have taken steps to ensure that there was an appropriate contract in place. An appropriate contract would be one that explicitly imposed on the IMSP for destruction purposes, the same obligations that Dr. Ooi had to meet and discharge. A contract should have required a certificate of destruction at a minimum. In fact, such a certificate was provided to Dr. Ooi after the destruction of the records in 2010. An appropriate destruction policy should have explicitly described all steps that APFMC staff must take to prepare records that would be picked up by a shredding company, set out what terms were needed in the contract for destruction and how that would be documented post destruction. None of these steps were part of APFMC retention and destruction policy.

[180] The retention and destruction policy was not available to patients. There was also no proper recording of files that had been archived in the clinic, in the second floor storage room, in an off-site storage space at the commercial storage facility or in the basement of Golden Mile Shopping Centre. What has made this investigation more complicated is that the boxes were not numbered sequentially so that no one truly knows what patient information has been stored in any place and which ones are unaccounted for since they were moved out of the clinic. In this regard I think the wording in section 17(2)(a) of HIPA is significant. The trustee must ensure that the phi is stored in such a way that it is "retrievable, readable and usable for the purpose for which it was collected for the full retention period." I do not know how health

records can be retrievable, readable and usable if the trustee has no inventory of the files stored off-site. To simply have boxes of files transferred to off-site storage facilities without any kind of index or tracking system, as was the case here, cannot be reconciled with the obligations of a trustee in section 17(2)(a).

[181] In addition, implicit in section 17(2)(a) is that the patient files cannot be lost track of by the trustee in order to be retrievable and useable as required by the subsection. The actions and negligence of Dr. Ooi that is documented in this Report, constitute a violation of section 17(2)(a).

[182] Furthermore, phi, according to section 17(2)(b) must be destroyed in a manner that protects the privacy of the patient. Obviously, tossing patient files and records into a large recycling bin available to the public, fails to protect the privacy of the patient and amounts to a violation of section 17(2)(b).

[183] The CMPA offers the following advice on its website:

> When clinical records no longer need to be retained, the paper record should be securely destroyed (e.g. by burning, shredding, etc.). **They should not simply be thrown out with the garbage where they may fall into the wrong hands**. This has indeed occurred with very unhappy results. Before destroying any records, physicians should consult with any applicable guidelines or statements from their College, privacy commissioner, etc. on the appropriate method of disposal for such records. **However, before destroying any records it is recommended that a list be made of the names of those patients whose records are to be destroyed, and that this list be kept permanently in a secure location. The purpose is to be able to later determine at a glance that a chart has been destroyed and has not simply been lost or misplaced**.[39]
>
> [emphasis added]

[184] Dr. Ooi has asserted that many of the patient files found in the recycling bin date back to 1983. I note, however that many of the records are much newer. In any event, HIPA clearly provides that phi must be protected by the trustee until one of the following occurs:

[39] *A matter of records: retention and transfer of clinical records*, Canadian Medical Protective Association, 2008, at p. 1-2, available at: https://www.cmpa-acpm.ca/cmpapd04/docs/resource_files/infosheets/2003/pdf/com_is0334-e.pdf.

- Transfer to another trustee or designated archive (section 22); or
- Transfer to the patient; or
- The phi relates to an individual who has been dead for more than 30 years (section 3(2)(b)); or
- The records are more than 120 years old (section 3(2)(c)).

[185] There is no evidence, nor any argument advanced by Dr. Ooi, that any of the foregoing circumstances apply. In any event, patients are as entitled to have their phi kept safe whether it is a file 10 or 15 years old or whether it is a current file. It is not for the trustee to decide which files warrant protection and which do not based on criteria not prescribed by HIPA.

[186] The other major way in which Dr. Ooi failed to comply with section 17 of HIPA relates to what appears to be approximately 125 boxes of patient records that cannot be satisfactorily accounted for.

[187] What has not been explained to my satisfaction is what happened to the approximate 125 boxes and contents that were moved to the basement of Golden Mile Shopping Centre in 2007 but which did not end up in the recycle bin. We know that approximately 150 boxes were moved to the basement and that 25 of them were ultimately tossed into the recycle bin. These were the boxes of files and records we seized on March 23, 2011. Since some, but not all, of the files and records found in the recycle bin were neatly boxed, it may well be that some of the 150 boxes may not have been full. We have re-boxed the records we seized to completely fill 25 bankers boxes. Despite numerous interviews with Dr. Ooi and the staff of her clinic over the first three weeks of the investigation, no explanation or information was forthcoming about what became of the missing 125 boxes of patient records.

[188] Then, more than three weeks into our investigation, Dr. Ooi advised that following her recent discussions with the property manager of Gold Square, she thought that the property manager should be interviewed a second time by our office since he could explain the missing boxes. We did interview the property manager again. He suggested that several months after the boxes were moved to the basement he noticed a number of boxes appearing in the additional storage space built at the back of APFMC (see Schedule 2). He advised that the boxes in this

storage space just appeared one day and he was sure they were the same boxes that had been transferred to the basement several months earlier. He didn't apparently look in any of the boxes but he suggested that they were a similar color and had similar markings as the ones transported to the basement. When asked why he had not mentioned this movement of boxes of records when earlier interviewed, he suggested that he hadn't been directly asked by our investigators if any records had been returned to the clinic. We understand that the former Nurse/Office Manager now also recalls that a number of boxes suddenly appeared in the new storage room constructed in 2007. Since presumably it would be APFMC who would have the better grasp than the Gold Square property manager, I accept the evidence of the former Nurse/Office Manager that she cannot confirm where they came from and how they came to appear suddenly in the storage area. She cannot tell us that these boxes that appeared in the new storage room came from the basement of Golden Mile Shopping Centre. Parenthetically, this confusion highlights serious deficiencies in the overall records management regime at APFMC. One might reasonably expect that when boxes suddenly appeared in a new storage area on the main floor that the former Nurse/Office Manager would investigate to determine exactly where they came from. If she thought they came back from the basement of Golden Mile Shopping Centre, one might reasonably expect that she would have immediately visited the storage room in the basement to ensure that all of the records had been returned to the clinic. If she had done such an investigation, she would have learned that the records had been moved from Room #5 and not returned but were in the open area of the basement. Our investigation revealed a remarkable lack of curiosity on the part of the former Nurse/Office Manager about the whereabouts of all 150 boxes of patient records that had been in the basement of Golden Mile Shopping Centre.

[189] There are a number of questions that arise from this late revelation by the property manager including the following:

- How is it that the only suggestion we heard about boxes moving from the basement of Golden Mile Shopping Centre to the main floor storage room of APFMC was not from one of Dr. Ooi's employees but from the property manager of Gold Square? After all, the records in question are the responsibility of Dr. Ooi not the landlord.

- How is it that the first witness who could estimate the number of boxes moved from the second floor storage room to Golden Mile Shopping Centre basement was the property manager for Gold Square who was interviewed by us on April 26, 2011?

- If this theory is correct, why did the property manager, when stating that he had never been back to the basement room since the patient files were moved there in 2007, also say that "[a]fter four or five years they [presumably APFMC] never asked me for access to those files or needed access from me." Why would he talk about access to files in the basement if he believed that all of the boxes had been moved back to the main floor storage room within a few months of being moved to the basement? He is either uncertain where the boxes in the storage room came from or he is uncertain as to how many of the 150 boxes were moved back to the main floor storage room. Either way, this speculation by a third party, not corroborated by any APFMC staff, is not very helpful.

- Why wouldn't the former Nurse/Office Manager be in a position to explain in detail how the boxes would have gotten from the basement of Golden Mile Shopping Centre to the main floor of APFMC and how many were moved? The most definite thing she can offer when we went back to her late in the investigation was that the boxes stacked in the back storage room looked similar to the boxes moved to the basement.

- How is it possible that no employee of APFMC has any personal knowledge of the boxes returning to APFMC?

- Since the property manager of Gold Square indicated that he never looked in the boxes, his evidence at its strongest is that some similar boxes appeared suddenly in the main floor of APFMC and he assumed that they came from the basement. He implicates the former Nurse/Office Manager but she has not corroborated the claim by the property manager.

- How is it possible that Dr. Ooi has no knowledge of this alleged return of boxes although she had originally approved the move of the boxes to the basement?

- Given the fact that it took six men over four hours to move the boxes from the second floor to the basement of Golden Mile Shopping Centre, it would have been a similarly major project to move the boxes back to APFMC. How could this not have been noticed and remembered by any of APFMC staff?

- No one has any particulars of the move. No one knows who would have undertaken such a move. We interviewed again, the construction company that had built the added storage space at the back of APFMC and had moved the 150 boxes in the first place from the second floor to the basement. That construction company had clear records of the move from the second floor to Golden Mile Shopping Centre basement but no records or knowledge of a subsequent move of a large number of boxes from the basement back to the main floor of APFMC. So, who moved the boxes and when?

- The former Nurse/Office Manager described the kinds of records that would be kept in the main floor storage space and those don't correspond to what was found in the boxes in the recycling bin.

- Why did none of the witnesses from APFMC that we interviewed, some on several occasions, make any mention of approximately 125 boxes of patient records suddenly appearing at APFMC in 2007?

- The former Nurse/Office Manager, when initially interviewed, was invited to tell us anything that she thought was important for us to know in terms of trying to understand how the files got where they did. She was prompted to consider anything that happened since the files were lost track off. She was asked to tell us anything else that she thinks was relevant. Her response was that she had nothing else to tell us.

F. Did the Trustee Comply with Section 18?

[190] The definition of an "information management service provider" is found in section 2(j) of HIPA as follows:

> A person who or body that processes, stores, archives or destroys records of a trustee containing personal health information or that provides information management or information technology services to a trustee with respect to records of the trustee containing personal health information, and includes a trustee that carries out any of those activities on behalf of another trustee, but does not include a trustee that carries out any of those activities on its own behalf.

[191] I first considered section 18 of HIPA in Investigation Report H-2005-002. One of the issues in that case was whether a trustee that contracts with another trustee can use the information transferred under that contract for its own purposes. I found that it could not do so. I determined that to qualify as an IMSP, an assessment must be done, apart from any contractual description or label, to see if the definition or elements of that definition apply.[40] In that same Report, I determined that the intention of the Saskatchewan Legislative Assembly was that the conveyance of phi to an IMSP would be a 'use' and not a 'disclosure' for purposes of HIPA.[41]

[192] I also considered section 18 in Investigation Report H-2007-001. In that Report, I concluded that even in the absence of a contractual agreement between two trustee organizations, I could

[40] Supra note 9 at p. 141.
[41] Ibid. at p. 143.

find that one organization is acting in an IMSP role when it processes phi for mailing on behalf of another trustee and at its request.[42]

[193] I considered the role and obligations of a trustee contracting with an IMSP further in our *Advisory for Saskatchewan Physicians and Patients Regarding Out-Sourcing Storage of Patient Records*.[43]

[194] The concept of an IMSP is by no means unique to Saskatchewan. It is a common feature in the other four stand alone health information laws in Canada (Manitoba's *The Personal Health Information Act*[44]; Alberta's *Health Information Act*[45]; Ontario's *Personal Health Information Protection Act*[46]; and Newfoundland and Labrador's *Personal Health Information Act*[47]). The title may be different, but in each of these statutes there is specific provision for a trustee (or custodian) to make arrangements for a third party to store or destroy phi.

[195] I need to consider what might be reasonably expected of a Saskatchewan physician who turns over patient records to an IMSP for purposes of storage or destruction. To do this, requires consideration of not just section 18 but also sections 16 and 17 of HIPA.

[196] A good starting point may be the Regulatory Bylaws of the CPSS. They provide as follows:

> **23.1 Medical Records**
>
> (a) All members of the College of Physicians and Surgeons of Saskatchewan shall keep, as a minimum requirement, the following records in connection with their practice:
>
> (i) In respect of each patient a legibly written or typewritten record setting out the name, address, birthdate and Provincial Health Care Number of the patient;
>
> (ii) In respect of each patient contact, a legibly written or typewritten record setting out:
>
> 1. the date that the member sees the patient;

[42] SK OIPC Investigation Report H-2007-001, at [36].
[43] *Advisory for Saskatchewan Physicians and Patients Regarding Out-Sourcing Storage of Patient Records*, SK OIPC, 2010, available at: http://www.oipc.sk.ca/whats_new.htm.
[44] *The Personal Health Information Act*, C.C.S.M. 2005, c. P33.5.
[45] *Health Information Act*, R.S.A. 2000, c. H-5.
[46] *Personal Health Information Protection Act*, S.O. 2004, c. 3.
[47] *Personal Health Information Act*, S.N.L. 2008, c P-7.01.

2. a record of the assessment of the patient which includes the history obtained, particulars of the physical examination, the investigations ordered and where possible, the diagnosis; and

3. a record of the disposition of the patient including the treatment provided or prescriptions written by the member, professional advice given and particulars of any referral that may have been made. Prescribing information should include the name of medication, strength, dosage and any other directions for use.

(b) The patient record should include every report received respecting a patient from another member or other health professional.

(c) The records are to be kept in a systematic manner.

(d) The records must be completed in a timely manner.

(e) The records may be made and maintained in an electronic computer system providing:

(i) the system provides a visual display of the recorded information;

(ii) the system provides a means of access to the record of each patient by the patient's name and if the person has a Provincial Health Care Number, by the health number;

(iii) the system is capable of printing the recorded information promptly;

(iv) the system is capable of visually displaying the recorded information for each patient in chronological order;

(v) the system maintains an audit trail that:

1. records the date and time of each entry of information for each patient;

2. indicates any changes in the recorded information;

3. preserves the original content of the recorded information when changed or updated; and,

4. is capable of being printed separately from the recorded information of each patient

5. the system includes a password or otherwise provides reasonable protection against unauthorized access, and

6. the system backs up files and allows the recovery of backed up files or otherwise provides reasonable protection against loss of, damage to and inaccessibility of information.

(f) 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.

(g) A member who ceases to practice shall:

(i) transfer the records to a member with the same address and telephone number; or

(ii) transfer the records to:

1. another member practicing in the locality; or

> 2. a medical records department of a health care facility; or
>
> 3. a secure storage area with a person designated to allow physicians and patients reasonable access to the records,
>
> after publication of a newspaper advertisement indicating when the transfer will take place.
>
> (h) A member who attends a patient at a hospital shall complete the medical records for which that member is responsible in accordance with the requirements of Saskatchewan legislation and regulations and the bylaws of the Regional Health Authority.[48]

[197] My view is that, before any trustee turns over patient phi to a third party who will function as an IMSP within the meaning of sections 2(j) and 18 of HIPA, it must put in place a written contract that defines the responsibilities of the IMSP. This will ensure that all parties fully understand their respective roles. This is consistent with recommendations from the CPSS, SMA and COACH. Furthermore, that contract needs to be in place before the phi is transferred to the IMSP. Also, the contract must reflect that the IMSP has no ownership interest in the patient records and holds them in strict confidence on behalf of the Saskatchewan trustee.

[198] I recognize that there may be many different circumstances under which a trustee might engage an IMSP. This could be for purposes of combining records containing phi, dealing with software vendors or developers for information management or information technology services, or in order to process, store, archive or destroy phi. In the result, the provisions in any given IMSP contract will need to be developed by trustees on a case-by-case basis to appropriately capture the nature and scope of the IMSP service in question and to appropriately address the relevant privacy and security issues. Consequently, I will consider first some general requirements for any IMSP contract and then consider what would have been appropriate for any contract between Dr. Ooi and an IMSP, specifically for the storage, transport and destruction of patient records.

[199] In considering what elements such an IMSP contract should contain, I take guidance from the Privacy Toolkit on both the CPSS and SMA websites, instruments and decisions from the

[48] College of Physicians and Surgeons of Saskatchewan Regulatory Bylaws, 2010, at p. 52-54, available at: http://www.quadrant.net/cpss/pdf/CPSS_Regulatory_Bylaws.pdf.

Information and Privacy Commissioners from the provinces of Ontario and Alberta, COACH, College of Physicians and Surgeons of British Columbia and from Newfoundland and Labrador Health & Community Services.[49]

[200] After consideration of these resources, I have determined that Saskatchewan trustees should consider including in any contract with an IMSP the following elements:

- The agreement must be in writing;
- The agreement must provide for the protection of phi against unauthorized access, use, disclosure, disposition, loss or modification in compliance with HIPA;
- The agreement must specify the purposes for which the IMSP may use and disclose phi, and must set out all applicable restrictions to such use(s) and or disclosure(s);
- The agreement must contain a meaningful description of all of the phi maintained by the IMSP;
- The agreement must document the security measures used by the IMSP to protect the phi in its possession;
- The IMSP must agree to comply with HIPA and with the provisions of the agreement, and must acknowledge both obligations in the agreement;
- The IMSP must agree to adhere to the policies and procedures of the trustee;
- The agreement must identify the situations under which the IMSP may disclose phi to another person or entity;
- The agreement must identify all stakeholders involved in the management of the phi including contractors or subcontractors and define the relationships with the identified individuals or groups;

[49] See the following resources: Office of the Information and Privacy Commissioner of Alberta Investigation Reports 2008-IR-002 at [30-31] and H2010-IR-002 at [18, 20, 22-24, and 29]; COACH Guidelines; *Checklist for Compliance with HIPA*, College of Physicians and Surgeons of Saskatchewan, item #9, at p. 3; SK OIPC Investigation Reports H-2005-002 at p. 141 and H-2007-001 at [33-36]; *Advisory for Saskatchewan Physicians and Patients Regarding Out-Sourcing Storage of Patient Records*, SK OIPC, 2010 at p. 9 & 13; *Health Information Act - Guidelines & Practices Manual*, Alberta Health and Wellness, March 2011, at p. 165-166, 267, and 333, available at: http://www.health.alberta.ca/documents/HIA-Guidelines-Practices-Manual.pdf; *Secure Destruction of Personal Information*, Information and Privacy Commissioner, Ontario, 2005, at p. 3 and 4, available at: http://www.ipc.on.ca/images/Resources/fact-10-e.pdf; *Get rid of it Securely to keep it Private - Best Practices for the Secure Destruction of Personal Health Information*, Information and Privacy Commissioner, Ontario, October 2009, at p. 6; *How to Avoid Abandoned Records: Guidelines on the Treatment of Personal Health Information, in the Event of a Change in Practice*, Information and Privacy Commissioner, Ontario, 2007, at p. 4-5, available at: http://www.privacybydesign.ca/content/uploads/2009/05/abandonedrec-gdlines.pdf; *The Personal Health Information Act Policy Development Manual*, Newfoundland and Labrador Health & Community Services, 2010, at p. 34-35, 121-122, 125, available at: http://www.health.gov.nl.ca/health/PHIA/PHIA_Policy_Development_Manual.pdf; and *Medical Records in Private Physicians' Offices*, The College of Physicians and Surgeons of British Columbia, 2010, available at: https://www.cpsbc.ca/files/u6/Medical-Records-in-Private-Physicians.pdf.

- The agreement must reference any other related Service Level Agreements pertaining to the trustee / IMSP relationship;
- The agreement must permit the trustee to review the policies and procedures of the IMSP related to the protection and management of phi to verify they are consistent with those of the trustee;
- The agreement must define notification and other change management processes as they relate to the provision of services by the IMSP;
- There should be an opportunity for the trustee to audit and inspect the IMSP's facilities and practices;
- There should be an obligation on the IMSP to notify the trustee at the earliest reasonable opportunity if phi should be stolen, lost or potentially viewed by unauthorized persons;
- Establishing and maintaining an adequate level of information control to ensure that all records containing health information can be located and retrieved within the required time limits;
- Establishing procedures for authenticating the identity of individuals and of those persons to whom health information is disclosed;
- Establishing procedures for stripping, encoding or transforming individually identifying health information to create non-identifying information;
- Conducting privacy impact assessments for new systems, practices and data matching proposals;
- There should be a provision for the immediate return of the data on demand by the trustee; and
- The agreement should also outline enforcement mechanisms so both the trustee and IMSP understand how the agreement will be enforced and what the consequences are for noncompliance with HIPA.

[201] I have determined that, in the case of a contract between a Saskatchewan trustee and an IMSP for purposes of the storage, transportation or destruction of phi, it should also include the following elements:

- Destruction of phi needs to be documented. If an organization receives a request for access to phi that has been destroyed, this documentation will allow a trustee to establish the actual destruction of the phi;
- The patient's right of access to phi continues until such time as the phi has been destroyed in accordance with a retention and disposition schedule;
- Destruction of phi should always be by a method that removes personal identifiers and minimizes the chance of any inadvertent disclosure of information. There should be provision for destroying phi by mechanical means (such as cross-cut shredding, pulping

or pulverizing) or incineration. When mechanically destroying phi the pieces should be reduced to pieces millimeters in dimension. When incinerated, the material residue should be reduced to white ash and be captured so partially burned materials do not escape;

- If records are to be moved off-site, an inventory must be done by the trustee beforehand and then a further inventory once the records have been moved to the off-site location;
- There should be the right of the trustee to terminate the agreement and recover possession of the records at its discretion and a clear prohibition against the IMSP retaining phi after termination of the contract;
- There should be no disclosure by the IMSP to any third party without the express written authorization of the trustee;
- There should be a prohibition against any unauthorized person viewing, using or disclosing the phi from the time the records leave the trustee's possession until they are fully and properly destroyed;
- There should be a procedure for labeling, segregating and securing phi so it is not treated as material suitable for recycling;
- If the IMSP is providing storage and destruction services, the agreement must ensure that the act of destroying the phi is with the explicit permission of the trustee; and
- The IMSP must provide a Certificate of Destruction which should address:
  - The company name;
  - A unique serialized transaction number;
  - The transfer of custody;
  - A reference to the terms and conditions;
  - The acceptance of fiduciary responsibility;
  - The date and time the information ceased to exist;
  - The location of the destruction;
  - The witness to the destruction;
  - The method of destruction;
  - A reference to compliance with the contract (if employing a secure destruction service provider); and
  - Signature.

[202] There is also a good deal of excellent material available on the Ontario Information and Privacy Commissioner's (Ontario IPC) website, including sample contract clauses, a process for internal authorizations prior to destruction and the contents of a destruction policy.[50]

[50] Information and Privacy Commissioner/Ontario website: http://www.ipc.on.ca/english/Home-Page/.

Although this material is designed specifically for the Ontario legislation, it can readily be adapted by Saskatchewan trustees to conform with HIPA, particularly sections 16, 17 and 18.

[203] In particular, I have found very helpful the resource, *Get Rid of it Securely to Keep it Private - Best Practices for the Secure Destruction of Personal Health Information*.[51] This was co-produced by the Ontario IPC and by the National Association for Information Destruction Inc. (NAID).

i. Application of the Law on IMSPs to These Facts

[204] On the unusual facts of this case, I determined that no less than five different organizations and a much longer list of individuals other than APFMC staff touched the boxes of patient records from the time they were moved out of APFMC starting in approximately 2005 until they were found in the recycling bin. This list includes the following:

- Dr. Ooi's children, aged 15 and 20 at the material times, and a number of their friends who were tasked to review files, purge some of the file material and then transfer records out of APFMC and up to the second floor storage room;
- The Pharmacist, who was the sub-landlord for APFMC and who arranged for storage of APFMC files in the same second floor room where he was storing confectionary items for his pharmacy and also some business records from the pharmacy; and
- The owner of Gold Square which first provided space on the second floor for storage and then arranged for storage space in Room #5 of the Golden Mile Shopping Centre basement.

[205] In the case of these individuals/organizations, the role of each was either determined by Dr. Ooi or at least with the clear knowledge of Dr. Ooi. That leads to my view that in each case these three groups would qualify as IMSPs.

[206] In addition, there is a considerably longer list of individuals or organizations that may have touched the boxes of patient records but in circumstances where Dr. Ooi asserts she had no knowledge of their role and did not authorize any of these organizations to deal with the boxes. I therefore find that they would not qualify as IMSPs. Nonetheless, they were only allowed to

[51] Supra note 24.

have access to the boxes containing patient records by reason of actions or omissions of one or more of the IMSPs.

[207] This list of non-IMSPs includes:

- Realtors and prospective tenants inspecting the second floor storage room;
- A crew of six men who worked for the contracted construction company and who were tasked with moving approximately 150 boxes of patient records from the second floor of Gold Square to the basement of Golden Mile Shopping Centre;
- Contractors doing renovations in the basement of Golden Mile Shopping Centre from 2007 to March 23, 2011;
- The owner of Golden Mile Shopping Centre and staff who had access to the basement of Golden Mile Shopping Centre;
- Contracted maintenance company;
- The owner of Golden Mile Shopping Centre and staff or contractors who set up the 'haunted house' display in the basement of Golden Mile Shopping Centre in the fall of 2010; and
- The 'haunted house' crowd estimated to be 3,600 to 4,800 persons who wandered through the basement of Golden Mile Shopping Centre in October of 2010.

[208] According to the evidence from Dr. Ooi and her former Nurse/Office Manger, none of the above noted individuals or organizations were ever requested by APFMC to have any involvement with the boxes or patient files. According to the same two sources, none of those individuals or organizations and their contribution to the movement of boxes of patient records was known to APFMC or Dr. Ooi prior to this investigation. Notwithstanding that lack of knowledge, the ultimate responsibility for the security of the patient records is vested in the trustee, Dr. Ooi.

[209] A similar approach has been taken by the Office of the Information and Privacy Commissioner of Alberta in its Investigation Report 2008-IR-002, which includes the following statement:

> [31] To summarize, whatever an information manager does on behalf of a custodian must comply with both the agreement with the custodian and the HIA. **The custodian is responsible for whatever an information manager does on its behalf**.[52]
>
> [emphasis added]

[210] Having regard to the authorities and resources discussed above, my view is that a reasonable expectation of Dr. Ooi would be that before any patient records left APFMC the following steps would have been taken:

- Preparation of a comprehensive record of all patients represented by the patient files in question;
- For daily summary sheets and physician billing sheets listing many different patients, that at least a record of the period covered would be retained by APFMC;
- A clear plan in terms of exactly where the boxes would be moved to, how long they would be in that location, how they would be secure in that location, how viewing, use or disclosure by third parties would be prohibited without the express consent of APFMC and when the records would be destroyed and how they would be destroyed in accordance with section 17 of HIPA;
- That there would be a screening and assessment of the suitability of a third party organization to serve as an appropriate IMSP, factoring into the assessment, whether there is a solid knowledge of HIPA and the security obligations of any trustee;
- That each of the boxes would be marked in such a way to allow easy tracking;
- That each of the boxes would be sealed and the seal initialed by APFMC privacy officer or her designate to ensure that snooping would be discouraged and such snooping would be readily apparent if it occurs;
- That a comprehensive written agreement is executed with any IMSP in accordance with sections 16, 17 and 18 of HIPA before any records with phi leave the premises of APFMC;
- That there is an appropriate plan to audit the IMSP's performance to ensure security of the records entrusted to the IMSP; and
- That there is a clear plan to utilize enforcement mechanisms to ensure compliance with HIPA.

[211] Section 18(3) clearly enjoins an IMSP from using, disclosing, obtaining access to, processing, storing, archiving, modifying or destroying phi received from a trustee except for the purposes set out in section 18(1). Section 18 does not explicitly require a written agreement between the

[52] Office of the Information and Privacy Commissioner of Alberta Investigation Report 2008-IR-002 at [31], available at: http://www.oipc.ab.ca/Content_Files/Files/Orders/H2008_IR_002.pdf.

trustee and the IMSP. I find however, that section 18 must be read in conjunction with both sections 16 and 17. It should also be read and interpreted mindful of the requirements of the CPSS in its Privacy Toolkit and the recommendations in the COACH Guidelines. Considering those resources, I have no hesitation in finding that a *reasonable* procedure to achieve the objectives of sections 16(a), 16(b) and 16(c) would be to ensure an appropriate written agreement between the trustee and the IMSP. Failure of a trustee to put such an agreement in place would constitute a breach of section 16.

[212] Next, I need to examine the role of each of the three identified groups/individuals that would qualify as IMSPs for purposes of APFMC records.

1. Children of Dr. Ooi and a number of their friends. This may have been as few as two and as many as four friends of the Ooi children;
2. The Pharmacist; and
3. The owner of Gold Square.

1. Children of Dr. Ooi and Friends

[213] Dr. Ooi's children, aged 20 and 15 at the material times, were looking for work for pay in the summer of 2006 according to the former Nurse/Office Manager. The decision was made by APFMC to employ the children to review old files, cull them and move the files upstairs to the second floor storage room.

[214] Although there are likely a number of jobs that could be done by young people to support their parents' medical clinic, I suggest that handling sensitive patient information would not be an obvious assignment. Given the relatively large staff available to Dr. Ooi and the former partners who operated APFMC, it is hard to imagine that a properly trained staff person could not be assigned to the job of reviewing patient files and deciding what old information should be culled to shrink the size of the file. Otherwise, like any IMSP, the trustee would need to have a confidentiality acknowledgement signed by each of the young people, they would need to receive a HIPA orientation and they would need to be closely supervised. On the evidence

of Dr. Ooi and the former Nurse/Office Manager, none of these reasonable measures was taken. The former Nurse/Office Manager apparently told the young people about confidentiality but given the unfamiliarity with HIPA of that individual, I find that such an instruction would have been insufficient. In the circumstances of this clinic, I have found that none of the principals had any knowledge of HIPA and therefore the assignment of this task to the young people was problematic from the start.

[215] As well, there is no evidence as to how the files were marked before they were moved to the second floor storage room, but apparently this was not done in such a way to allow easy tracking of files once they left APFMC. Furthermore, there is no evidence that the boxes were sealed before they were moved upstairs. Not only was there no written agreement with any of the young people, there was apparently no audit of their activity or any plan to do so. Our impression is that the young persons were largely left to themselves to cull and review files.

[216] This seems to have been a poorly considered arrangement that falls short of the requirements for a Saskatchewan health trustee. This would be a breach of sections 16, 17 and 18 of HIPA.

2. The Pharmacist

[217] The Pharmacist was in an interesting position. He had known Dr. Ooi and her former partner for many years. In fact, he had a similar arrangement at the earlier 5th Avenue Medical Clinic where he leased space in the building and then subleased space adjacent to his pharmacy to the clinic owned by Dr. Ooi and some other physicians from approximately August 2001 to August 2010. He also had a pharmacy beside the original Albert Park Medical Clinic at 4040 Albert Street, Regina. At some point early in APFMC's history, he apparently advised Dr. Ooi and the other physician owners that he would look after all of their file storage requirements. He represented to the physicians that this would be done at no additional rental cost although it would be factored into the annual common area costs as they were adjusted year to year. For example, when there was a space problem in 2007 he arranged for the head landlord to construct and then rent him additional space consisting of a new storage room accessible to

APFMC. The sole purpose was to expand the space available to APFMC for the storage of patient files.

[218] When I questioned the former Nurse/Office Manager for the period 2003 until April 15, 2010, she indicated that when it came to storage of records, the person who would be responsible was not her or any staff member of APFMC but the Pharmacist. When I questioned why he would be responsible, she responded that he was a pharmacist and she trusted him to know how to deal with phi. She advised that she understood the Pharmacist would be responsible for those records once they left APFMC. She also told me that if there was a problem and files went missing she would look to the Pharmacist to be responsible to find out what happened to those records. She confirmed that APFMC had no written agreement with the Pharmacist that addressed responsibility for records stored off-site. She advised that the Pharmacist had agreed to look after whatever Dr. Ooi and her former business partner needed help with. She went on to say that "[A]s a pharmacist he certainly is bound by a code of ethics as well."

[219] She volunteered that if the Pharmacist assured her that APFMC patient files were "behind a locked door" as they were on the second floor of Gold Square she had no reason to doubt him or to question his assertion.

[220] Dr. Ooi had a similar view of the Pharmacist as the person responsible for off-site storage of patient records belonging to APFMC. She advised there was never a written agreement with the Pharmacist since he had told her "[W]hen you run out of space I will be responsible for finding the space for you and whatever rent you pay is already incorporated into paying for the space."

[221] She indicated that was why they utilized the storage room arranged by the Pharmacist on the second floor. She specifically stated that "[the Pharmacist] is responsible for finding us extra space."

[222] The problem is that among Dr. Ooi, the former Nurse/Office Manager and the Pharmacist, there was no written agreement or even a shared understanding of who would be responsible

for off-site storage of APFMC patient files. The Pharmacist clearly had acted as an IMSP when it came to arranging for storage of patient files with the commercial storage facility. This included entering into a lease, possessing the sole key to the space, transporting patient files to the space and retrieving files as required by APFMC. Then in February 2011, he arranged for the transport of approximately 250 boxes of patient records (referenced in paragraphs [74] and [139] of this Report) from the commercial storage facility to another medical clinic owned by Dr. Ooi known as the Transcona Medical Clinic. All of this was done with the knowledge of Dr. Ooi and APFMC staff. Although there was no contract as there should have been to satisfy sections 16, 17 and 18 of HIPA, it is clear that Dr. Ooi viewed the Pharmacist as having responsibility for the files involved in that off-site storage arrangement.

[223] I also learned that the Pharmacist had recently functioned as an IMSP when Dr. Ooi sold her 5th Avenue Medical Clinic to another physician. According to the Pharmacist, the files were in such a mess that he arranged, at his expense, to undertake with four workers to organize the records and destroy old ones in the 5th Avenue Medical Clinic. This work, according to the Pharmacist, extended over a month.

[224] The Pharmacist also represented that he believed he had followed best practices when it came to health records, notwithstanding he had never read HIPA, never had any training in HIPA and most importantly had no understanding of key elements of HIPA including sections 9, 10, 16, 17, 18, 22 and 23.

[225] Dr. Ooi and the former Nurse/Office Manager both told our investigators that the Pharmacist had arranged for the space in the basement of Golden Mile Shopping Centre. The owner of Gold Square confirmed that the Pharmacist was involved in arranging that basement storage. The Pharmacist's explanation of his role over several interviews was not consistent. At one point, he insisted that he knew nothing about this arrangement. In a subsequent interview, he acknowledged having had discussions with both the owner of Gold Square and the former Nurse/Office Manager about the basement storage room. I find that it is not necessary to determine which of the explanations from these three individuals is most accurate. The point is that in the absence of an IMSP agreement and clear written arrangements for off-site storage,

responsibility for what we found during this investigation must rest with the only trustee ultimately responsible for those patient records, Dr. Ooi. In fact the confusion we found in this investigation ultimately must be laid at the feet of Dr. Ooi. That confusion led directly to the improper dumping of patient files and records in the recycling bin.

3. The Owner of Gold Square

[226] Although there is considerable contradiction in the accounts by the various principals (Dr. Ooi, the Pharmacist, the former Nurse/Office Manager and the owner of Gold Square) as to who was responsible for the move of the 150 boxes of patient files from the second floor of Gold Square to the basement of Golden Mile Shopping Centre, there can be no question that this was done with the full knowledge of Dr. Ooi. The owner of Gold Square can be considered as an IMSP within the meaning of sections 2(j) and 18 of HIPA. The services it provided was the arrangement of storage space in the basement of Golden Mile Shopping Centre. It did this by entering into a Temporary Occupancy Agreement (the lease) for Room #5. The term of the lease was from February 15, 2007 to August 31, 2007. The owner of Gold Square then requested and agreed to an over holding arrangement with the owner of Golden Mile Shopping Centre from September 1, 2007 to March 31, 2011. The owner of Gold Square also apparently arranged for the transport of the patient files from the second floor storage space to the basement room in Golden Mile Shopping Centre. This was done by directing a contractor who was doing other work for them, the contracted construction company, to physically move the boxes. The move of the boxes with patient phi was supervised by the property manager of Gold Square. According to the property manager, he also helped lift and move a number of the boxes himself. That same individual stated that after the boxes had been moved to Room #5, he personally inspected the room to make sure it was locked.

[227] Having made that determination, it is clear on the evidence that there was no written agreement between Dr. Ooi and the owner of Gold Square as contemplated by sections 16, 17 and 18 of HIPA. For reasons that are not apparent, Dr. Ooi effectively abdicated her responsibility for the patient records by turning them over to third parties without having taken any reasonable measures to exercise continuing control over those records. This is perhaps most apparent

when the only contract relating to basement storage of APFMC patient records was between the owner of Gold Square and the owner of Golden Mile Shopping Centre. APFMC was not even a party to the lease for the basement storage room despite the fact these were the patient records of APFMC. The lease was solely about the rental of the space for the "storage of medical and other office files only". There was no reference in the lease to the fact that the records included personally identifiable health information of APFMC patients. There is no acknowledgment that the records belonged to a third party, Dr. Ooi. There is no mention of what steps must be taken by the Gold Square owner to keep the records safe and confidential. There was no indication to the owner of Gold Square of the importance that the records not be disturbed in any way without the prior consent of APFMC. The lease agreement did not obligate the owner of Golden Mile Shopping Centre to take all reasonable measures to protect the phi. There is no evidence of any kind of collateral agreement to that effect between APFMC and the owner of Golden Mile Shopping Centre. As the owner of Gold Square himself stated:

> I understood it was the medical clinic's responsibility to ensure those files were secure. I was simply renting that space on their behalf and if I was to do it over again I would insist that they take out the lease rather than myself so again, I managed quite a bit of property but I never considered medical files.

[228] The vulnerability of the patient files was underscored when the owner of Gold Square stated to me that "[W]e have no oversight of their employees" [referring to employees of Golden Mile Shopping Centre].

[229] When the staff of Golden Mile Shopping Centre had to deal with water damage in the basement of the mall, they notified the owner of Gold Square that they needed the key to enter Room #5 and deal with the water problem. Presumably they did this since their subsisting lease for Room #5 was only with the owner of Gold Square. Significantly, neither the owner of Golden Mile Shopping Centre nor the owner of Gold Square thought to notify APFMC that there was a problem with water affecting Room #5 where their patient files were stored. That, however, should have been no surprise since Dr. Ooi had not taken reasonable measures to ensure that she would be notified of such an event that would or may affect the security of her clinic's patient files. After all, Dr. Ooi was not a party to the lease agreement. She had no

written agreement with either the owner of Golden Mile Shopping Centre or the owner of Gold Square requiring safeguarding of the patient files.

[230] Dr. Ooi had no process to monitor the storage arrangement and to periodically check on the patient files. She made no request to either the owner of Golden Mile Shopping Centre or the owner of Gold Square to confirm that the storage of her clinic's patient files continued to be secure and appropriate. I find it curious that on the evidence, no one from APFMC at any time between February or March 2007 until March 23, 2011, ever inspected Room #5 in the basement of Golden Mile Shopping Centre or even made any inquiry of either the owner of Gold Square or the owner of Golden Mile Shopping Centre as to the state of the patient files. In fact, it appears that on March 23rd and 24th, 2011, none of the principals involved in this investigation even mentioned the possibility that the files and records in the recycling bin may have come from the basement storage area. My belief is that Dr. Ooi, her former Nurse/Office Manager and staff had forgotten about the basement storage area and the files in it.

[231] Dr. Ooi contends that the fault for the records in the recycling bin should be assigned to the janitorial staff of the owner of Golden Mile Shopping Centre who didn't understand what was in the boxes and may have mistaken the boxes as material intended for recycling. While clearly there were mistakes made by staff of the owner of Golden Mile Shopping Centre who tossed the patient files into the recycling bin, I find that the end result can be attributed to the failure four years earlier by Dr. Ooi in ignoring and failing to meet the minimum requirements of sections 16, 17 and 18 of HIPA. That early failure by Dr. Ooi was compounded by her failure to take reasonable steps to monitor the storage arrangements. Simply having someone check on the records in the basement of Golden Mile Shopping Centre at any time over the four years would immediately have revealed that the records were unsecured in either an open common area in the basement or in unlocked Room #19.

[232] I should note that although the former Nurse/Office Manager and Dr. Ooi have been critical of both the owner of Golden Mile Shopping Centre and the owner of Gold Square for not keeping better track of the patient files, the responsibility for the files is clearly that of Dr. Ooi as is the responsibility for failing to have taken any measures, let alone reasonable measures, as

required by sections 16, 17 and 18 of HIPA. No one can say for certain that if Dr. Ooi had put in place appropriate policies and procedures as contemplated by section 16 of HIPA and had been familiar with her obligations under sections 16 and 18 that the large volume of patient phi would not have ended up in the recycling bin on March 23, 2011. Such actions as listed above would, however, have substantially reduced the risk that this would happen.

IV. CONCLUSION

[233] Dr. Ooi displayed a total lack of awareness of the requirements of HIPA that came into force September 1, 2003 and this lack of awareness continued until March 23, 2011. As a direct result of that lack of awareness and her failure to take any appropriate measures to protect the phi of a large number of patients over a period of approximately six years, patient records ended up in the recycling bin.

[234] I wish to acknowledge that Dr. Ooi was cooperative with our investigation as was her new Office Manager. During the course of this investigation, we have discussed with Dr. Ooi and her staff the need for extensive remedial work to move to a position of HIPA compliance. She has, through her solicitor, presented us with a new Policy Binder that incorporates a letter from the Minister of Health dated April 13, 2011, Re: Legal Obligations Regarding Protection of Personal Health Information. She is requesting that her APFMC staff read the letter and initial same to verify they have read it. They have now posted in APFMC, in visible places, a privacy poster created by the CMA and the SMA. The binder also includes a copy of HIPA, a copy of materials from the SMA Privacy Toolkit, a new procedure for tracking requests and processes for shredding to be done by a commercial document destruction firm. As well, the new Policy Binder includes a copy of the OIPC December 14, 2009, *Report on Management of Access Requests from Patients to Saskatchewan Regional Health Authorities.*[53] These steps taken by Dr. Ooi represent a positive first step. We have offered to provide feedback as Dr. Ooi develops more granular material that will be required for HIPA compliance.

[53] *Report on Management of Access Requests from Patients to Saskatchewan Regional Health Authorities*, SK OIPC, 2009, available at: http://www.oipc.sk.ca/whats_new.htm.

[235] In addition, Dr. Ooi has now reviewed the SMA/CPSS Privacy Toolkit materials respecting HIPA and trustee obligations. She has amended APFMC internal policies. She has sought advice from the Ministry of Health in preparing draft agreements and procedures manuals. She advises that the Ministry of Health intends to provide online HIPA training and that this training will be taken by all APFMC employees. She has also formally designated her new Office Manager as APFMC privacy officer.

[236] Dr. Ooi has advised us that she will follow the OIPC *Helpful Tips: Privacy Breach Guidelines* available at our website.[54] Dr. Ooi has proposed a plan to provide notice to patients by means of display advertisements in the Regina *Leader-Post* and will correspond directly with a number of patients affected by this breach.

[237] It should be noted that, in the interests of procedural fairness, I provided the lawyer acting for Dr. Ooi, the Pharmacist and the owner of Gold Square with a portion of the draft Report. I invited them to identify any factual errors. I provided a 42 page portion of the draft document to the lawyer on June 3, 2011, and advised that we would need to hear back from him no later than June 7, 2011. At the request of the lawyer, I extended the deadline for fact checking to June 10, 2011. On June 10, 2011, I received a five page letter from the lawyer. The letter made no reference to any pending feedback from the Pharmacist nor did it indicate that anything further would be provided to our office from any of his three clients. We then proceeded to complete our Report.

[238] On June 27, 2011, the lawyer phoned to advise for the first time since the extended deadline, that his client, the Pharmacist, had some feedback that he wanted to share. He requested more time. I advised that the Report had already moved to the formatting stage and the deadline had passed almost three weeks earlier. Nonetheless, I advised him that if he had any factual errors to bring to our attention, he must do so by the end of that day. I sent the lawyer an email at 5:00 p.m. on June 27, 2011, advising that if he had anything to provide us with that we needed it that day and not later.

[54] *Helpful Tips: Privacy Breach Guidelines*, SK OIPC, 2010, available at: http://www.oipc.sk.ca/Resources.

[239] On June 28, 2011, the lawyer and his client, the Pharmacist, phoned our office. They advised that the Pharmacist still wished to provide input into the Report. To that end, they requested they have until July 4, 2011. I replied that since two extensions had already been provided, we would not delay further. Any factual errors needed to be provided in that conversation. What the Pharmacist raised in the conversation was mostly matters of opinion and interpretation and not new facts. I confirmed with the Pharmacist and his lawyer that we would proceed to issue the Report without further delays.

V. FINDINGS

[240] That the patient files and records found in the recycling bin qualified as "personal health information."

[241] That these patient files and records came from Albert Park Family Medical Clinic and had been in the custody or control of Dr. Teik Im Ooi at all material times. Prior to April 1, 2010 Dr. Teik Im Ooi was a co-trustee with a number of partners from 1993 until March 2003. From March 2003 until April 1, 2010, Dr. Teik Im Ooi was co-trustee with one other physician. Commencing April 1, 2010 Dr. Teik Im Ooi was the sole trustee with custody or control of the patient files in issue.

[242] That the trustee was Dr. Teik Im Ooi carrying on business as Dr. Teik Im Ooi Medical Professional Corporation, Albert Park Medical Clinic, Albert Park Medical Centre and Albert Park Family Medical Centre.

[243] That the trustee allowed her children and their friends unsupervised access to patient personal health information over a number of weeks in the summer of 2006.

[244] That, starting in approximately 2005, the trustee moved to the second floor storage room in Gold Square approximately 150 boxes of patient records without creating any kind of catalogue or index of the contents of the boxes. The boxes themselves were not numbered sequentially.

[245] That the trustee failed to require any kind of written agreement with the Pharmacist in the adjacent drug store or the owner of Gold Square to ensure the protection of the contents of the 150 boxes in the second floor storage space.

[246] That, for more than one year, the staff of the pharmacy, including administrative and maintenance staff, had ready access to the second floor storage room without notification to the trustee.

[247] That the only key to the second floor storage room was at all times in the custody of the pharmacy which allowed pharmacy staff access without the consent of or notice to the trustee.

[248] That the trustee did not require any kind of agreement with the contracted construction company to ensure protection of the contents of the 150 boxes when they were moved to the basement of Golden Mile Shopping Centre.

[249] That the trustee failed to be present when the boxes were moved to the basement storage room, failed to supervise the move and failed to inspect the basement room to which the patient records were being moved.

[250] That the trustee failed to have a written agreement with the owner of Golden Mile Shopping Centre to ensure appropriate protection of the patient records once located in the basement of that mall.

[251] That the trustee had no knowledge that in 2007 the lock to the basement storage room was deliberately broken by Golden Mile Shopping Centre owner and the patient records moved to an open area of the basement.

[252] That the trustee had no knowledge of the location and circumstances of storage of the patient records from 2007 to March 23, 2011.

[253] That the trustee failed to send any staff person to Golden Mile Shopping Centre to inspect the patient records and to ensure they were appropriately protected from 2007 until March 23, 2011.

[254] That, for almost four years, the patient records and personal health information were unsecured in such a way that anyone who entered the basement of Golden Mile Shopping Centre, including workmen, contractors, employees of the Mall owner, tenants of the Mall, and more than 3,600 persons who wandered through the basement in October 2010 would have had ready access to all of that personal health information.

[255] That the trustee failed to have the policies and procedures required by section 16 of *The Health Information Protection Act.* More specifically, the trustee failed to have policies and procedures for the administrative and physical safeguards required by section 16 including:

- No designated privacy officer;
- No appropriate privacy policy;
- Inadequate privacy procedures;
- Failure to have appropriate agreements;
- No privacy awareness and education program;
- Inadequate treatment of consent/communication with patients; and
- Inadequate security protections.

[256] That the trustee failed to comply with section 17 of *The Health Information Protection Act.*

[257] That the following information management service providers handled the patient files and had access to the patient records:

- Children of Dr. Ooi and a number of their friends
- The Pharmacist
- The owner of Gold Square

[258] That the trustee failed to comply with section 18 of *The Health Information Protection Act.*

[259] That the trustee's failure to comply with sections 16, 17, and 18 of *The Health Information Protection Act* led directly to the 180,169 items of personal health information including 2,682 patient files found in the recycling bin on March 23, 2011.

[260] That the trustee has failed to provide a satisfactory explanation for the approximately 125 boxes of patient files that went missing between February 2007 and March 23, 2011.

[261] That the trustee has failed to catalogue and index the patient records in approximately 250 boxes stored at her Transcona Medical Clinic.

[262] That the trustee, as of March 23, 2011, had no adequate plan to deal with the patient files in the 250 boxes stored at Transcona Medical Clinic.

VI. RECOMMENDATIONS

[263] That Dr. Teik Im Ooi provide notification to affected patients, past and present of Albert Park Family Medical Clinic consistent with the Office of the Information and Privacy Commissioner's *Helpful Tips: Privacy Breach Guidelines* available on our website.

[264] That for those patients related to the 2,682 files involved in this breach, a letter in a form satisfactory to our office, be mailed to each patient explaining what has happened, what corrective action will be taken to prevent a reoccurrence of the breach and advising them that they have the right to contact the Office of the Information and Privacy Commissioner if they are dissatisfied with the action taken by Dr. Teik Im Ooi and Albert Park Family Medical Clinic.

[265] That a newspaper advertisement be published at least twice in the Regina *Leader-Post* on Saturday on two successive weeks that provides the information described in paragraph [264] above.

[266] That Dr. Teik Im Ooi provide our office, within 30 days, with comprehensive written policies and procedures for the administrative and physical safeguards contemplated by sections 16, 17 and 18 of *The Health Information Protection Act*.

[267] That Dr. Teik Im Ooi enter into formal written agreements with all existing information management service providers within 30 days and provide our office with copies.

[268] That Dr. Teik Im Ooi undertake, within 60 days, an intensive training program for all staff at any of her clinics in the city of Regina with respect to *The Health Information Protection Act* with particular emphasis on those requirements that go beyond simply a confidentiality requirement.

[269] That Dr. Teik Im Ooi ensure that each member of Albert Park Family Medical Clinic staff execute a confidentiality undertaking that includes an acknowledgement that breach of *The Health Information Protection Act* and the Albert Park Family Medical Clinic privacy policies and procedures may be grounds for dismissal with cause.

[270] That Dr. Teik Im Ooi provide our office, within 60 days, a written plan that outlines how she intends to address the large volume of un-catalogued patient records currently being stored at Transcona Medical Clinic. The written plan should include what is contemplated for the retention and destruction of the records.

[271] That the College of Physicians and Surgeons of Saskatchewan implement a mandatory requirement for a comprehensive training program on *The Health Information Protection Act* and monitors attendance of its members.

[272] That the Ministry of Health complete a comprehensive manual on *The Health Information Protection Act* that provides detailed, concrete and practical information to all trustees and the public on compliance with all provisions of *The Health Information Protection Act* with particular emphasis on sections 16, 17 and 18.

[273] That the Minister of Justice consider commencing a prosecution pursuant to section 64 of *The Health Information Protection Act* in respect to the multiple breaches of *The Health Information Protection Act* documented in this Investigation Report.

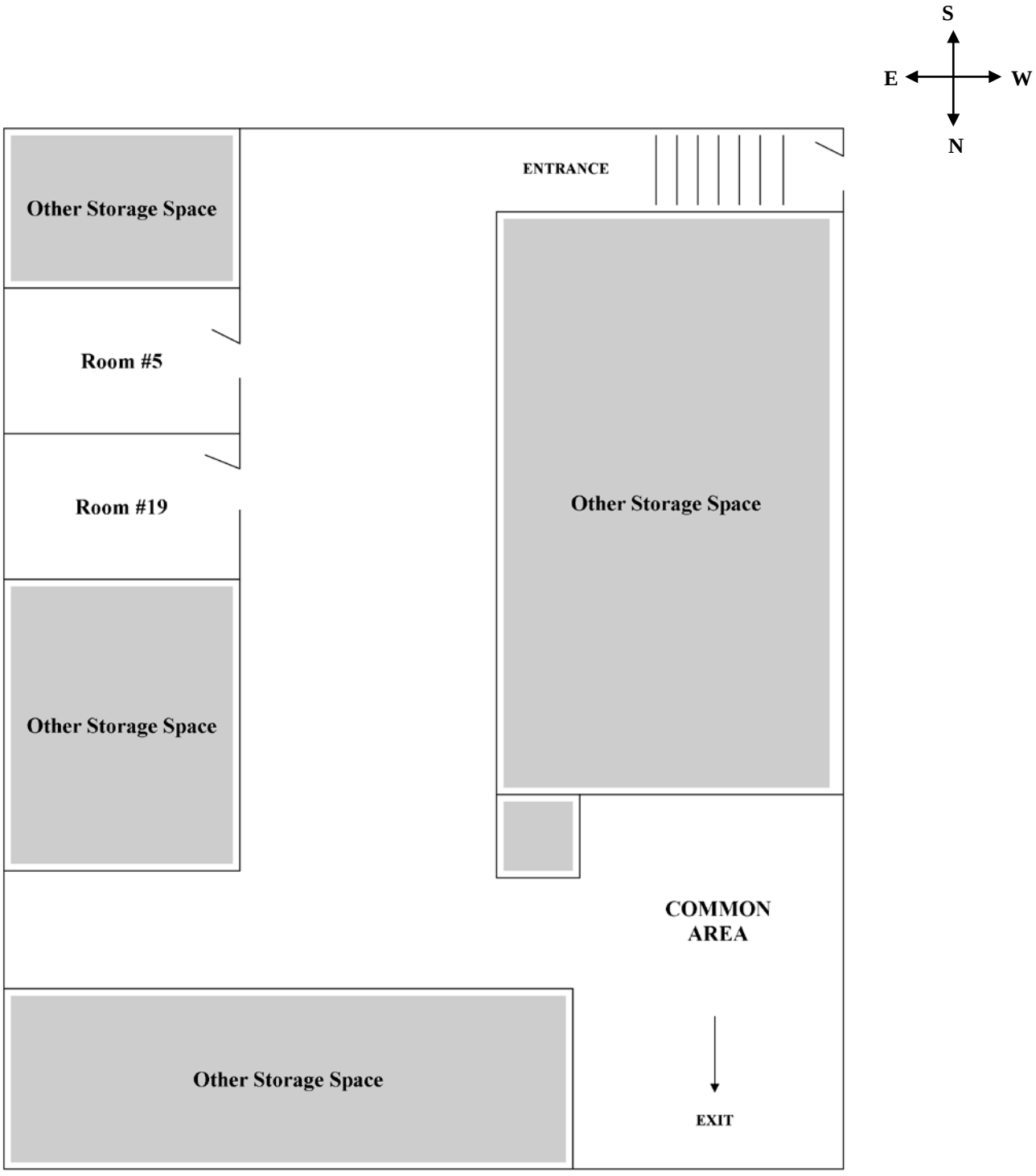
Dated at Regina, in the Province of Saskatchewan, this 14th day of July, 2011.

R. GARY DICKSON, Q.C.

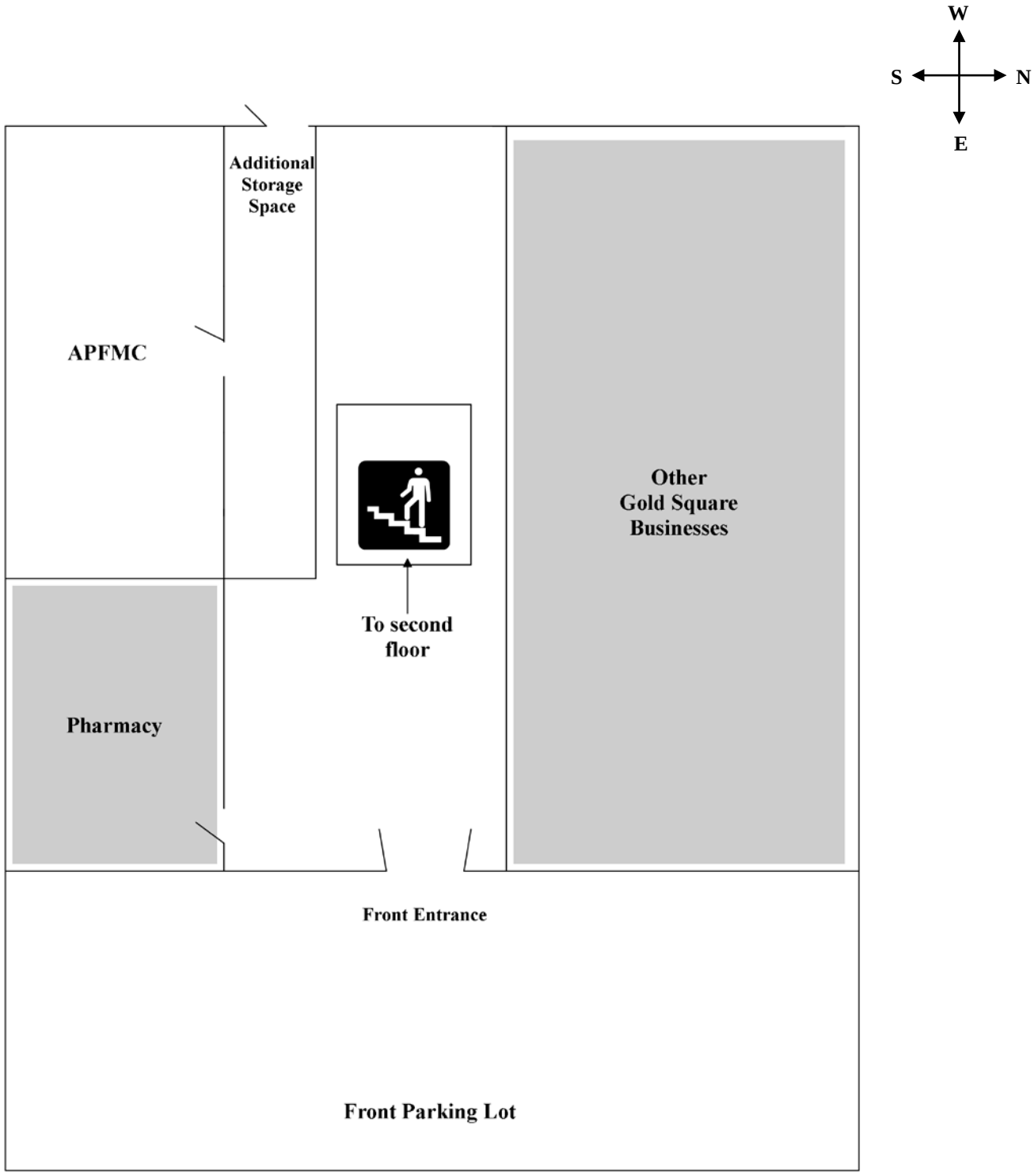
Saskatchewan Information and Privacy Commissioner

VII. SCHEDULES

Schedule 1: Map of Basement Storage at Golden Mile Shopping Centre



Schedule 2: Map of Gold Square and Additional Storage at APFMC



Schedule 3: Key Individuals

Albert Park Family Medical Clinic (APFMC)

From 1983 to 1993, APFMC was located at 4040 Albert Street, Regina, Saskatchewan. The medical clinic moved to 3992 Albert Street, Regina, Saskatchewan in 1993 (Gold Square).

Dr. Teik Im Ooi
Dr. Ooi, at all material times, owned APFMC either solely or jointly. She has been licensed as a physician in Saskatchewan for almost 25 years. She currently owns two other medical clinics in Regina where she continues to practice medicine.

Former Nurse/Office Manager
The former Nurse/Office Manager is a registered nurse. She has worked for Dr. Ooi since 1987. She took on the dual role of office manager and registered nurse in 2003 for APFMC. This role included the general running of the office and responsibility for records management. She continued in this dual role until April 15, 2010, when the new Office Manager took over the office manager duties only. The former Nurse/Office Manager continues to work for APFMC as a registered nurse.

New Office Manager
The new Office Manager is currently the full time office manager at APFMC. She started in this role on April 15, 2010. She has worked for Dr. Ooi since the late 90s and moved between the different clinics that Dr. Ooi owned. The new Office Manager would be responsible for the general running of the office which includes hiring, training and orienting new staff. The role also includes responsibility for records management.

The Pharmacy

The pharmacy is also located at 3992 Albert Street, Regina, Saskatchewan. The pharmacy is owned and operated by the Pharmacist.

The pharmacy was also previously located at 4040 Albert Street, Regina, Saskatchewan. The pharmacy moved to 3992 Albert Street, Regina Saskatchewan (Gold Square) around the same time as APFMC (1993).

The Pharmacist
The Pharmacist has been licensed as a pharmacist in Saskatchewan since 1979. He currently owns and operates three pharmacies in Regina, including, the pharmacy at 3992 Albert Street, Regina, Saskatchewan. All three pharmacies are located next to medical centers.

Owner of Gold Square

The owner of Gold Square owns the property that houses APFMC and the pharmacy – 3992 Albert Street, Regina.

Property Manager
The property manager is employed by the owner of Gold Square. He has been employed by the owner for almost 30 years.

Owner of Golden Mile Shopping Centre

The owner of Golden Mile Shopping Centre leased storage Room #5 in the basement of Golden Mile Shopping Centre to the owner of Gold Square under the terms of a Temporary Occupancy Agreement.

Contracted Construction Company

The construction company was contracted to do work at Gold Square. During this investigation, it was determined that the contracted construction company performed numerous construction jobs at the Gold Square including renovating the second floor of the Gold Square to accommodate a new doctor's office and the addition of extra storage space at the back of APFMC. Both renovations occurred during 2006 and 2007.

This company moved 150 boxes of patient records belonging to APFMC from the second floor of Gold Square to the basement of Golden Mile Shopping Centre in 2007.

Contracted Maintenance Company

The maintenance company was contracted by the owner of Golden Mile Shopping Centre to do maintenance work at Golden Mile Shopping Centre.

Employees of this company were involved in the move of approximately 25 boxes of patient records from Room #19 in Golden Mile Shopping Centre basement to the recycling bin.

Schedule 4: Photographs

Basement Stairs – Golden Mile Shopping Centre

Photo Date: March 30, 2011

Basement Hallway – Golden Mile Shopping Centre

Photo Date: March 30, 2011

Basement Storage Room #19 – Golden Mile Shopping Centre

Photo Date: March 30, 2011

Basement Storage Room #19 – Found Unlocked by Investigators

Photo Date: March 30, 2011

Transcona Medical Clinic – Storage room full of un-catalogued boxes of patient records and files that originated from APFMC. These boxes constitute some of the 250 boxes of patient records moved from the commercial storage facility (as referenced in paragraphs [74], [139] and [222] of this Report).

Photo Date: April 6, 2011

Transcona Medical Clinic – Storage room full of un-catalogued boxes of patient records & files that originated from APFMC. These boxes constitute some of the 250 boxes of patient records moved from the commercial storage facility (as referenced in paragraphs [74], [139] and [222] of this Report).

Photo Date: April 6, 2011