Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 021-2024

Dr. Harold Smith

July 8, 2024

Summary: Dr. Harold Smith (Dr. Smith) proactively reported the premature destruction of personal health information after he became aware he had disposed of patient records before the appropriate retention period had expired. The Commissioner found that Dr. Smith did not meet his ongoing duties pursuant to section 22 including his duty to sufficiently safeguard and account for personal health information through storage to destruction pursuant to section 16 and subsection 17(2) of HIPA The Commissioner recommended that within 30 days of issuance of this Investigation Report, Dr. Smith place an advertisement in a community newspaper in Yorkton, where he formerly practiced, so his former patients are aware that their records have been destroyed.

I BACKGROUND

[1] In this Investigation Report, Dr. Harold Smith (Dr. Smith) has been represented by his legal counsel. I consider that the representations made by Dr. Smith's legal counsel are Dr. Smith's and so will write this Investigation Report as if Dr. Smith provided the representations.

[2] In December 2023, Dr. Smith was contacted by the College of Physicians and Surgeons of Saskatchewan (CPSS) about a former patient who sought access to their personal health information (or medical record). This led to Dr. Smith discovering that he had prematurely destroyed this former patient's records. On January 19, 2024, Dr. Smith telephoned to

advise them of this, and also sent them a letter acknowledging the destruction and offering an apology for the error. The letter also stated that he reported the matter to CPSS and to my office.

[3] On February 2, 2024, Dr. Smith proactively reported the matter to my office as follows:

> In October 2023, Dr. Smith securely shredded medical records for his former patients. He retired and ceased practising [sic] medicine in December 2019. When he destroyed the records in October 2023, Dr. Smith thought he had satisfied the applicable retention period...

[4] Dr. Smith also confirmed with my office that his practice did not maintain electronic medical records; there were only physical paper records, which he had destroyed.

[5] On March 26, 2024, my office notified Dr. Smith that my office would be conducting an investigation. On May 2, 2024, Dr. Smith provided a completed *Privacy Breach Investigation Questionnaire*.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[6] *The Health Information Protection Act* (HIPA) is engaged when three elements are present: 1) there is a trustee; 2) there is personal health information; and 3) the personal health information is in the custody or control of the trustee.

[7] As noted in the Background, Dr. Smith has already destroyed the records in question, but he practiced as an ophthalmologist. The patient records of an ophthalmologist would normally contain information such as registration information (full name, date of birth, address, Saskatchewan Health Number), information about a patient's physical health, information gained from testing or examining, and information related to the services an ophthalmologist provides. This information would qualify as personal health information as defined by subsections 2(1)(m)(i), (ii), (iii), (iv) and (v) of HIPA as follows:

> **2**(1) In this Act:
>
> …
> (m) **"personal health information"** means, with respect to an individual, whether living or deceased:
>
> (i) information with respect to the physical or mental health of the individual;
>
> (ii) information with respect to any health service provided to the individual;
>
> (iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
>
> (iv) information that is collected:
>
> (A) in the course of providing health services to the individual; or
>
> (B) incidentally to the provision of health services to the individual; or
>
> (v) registration information;

[8] There is personal health information involved in this incident.

[9] Once establishing personal health information is involved, I need to consider if there is a trustee. Dr. Smith does not dispute that he is the trustee in this matter and that he was the sole owner of his medical practice, "Dr. Harold M. B. Smith, MD". The Information Services Corporation (ISC) Saskatchewan Corporate Registry lists Dr. Smith as the Officer and Director of "Dr. Harold M.B. Smith Medical Professional Corporation". CPSS' website lists Dr. Smith with a specialty of ophthalmology, and his license history indicates his license as being "inactive" with a status date of December 1, 2019. As an ophthalmologist, Dr. Smith's practice was governed by *The Medical Professions Act, 1981*, an Act for which the Minister of Health has oversight (OC 33/2023). Based on the above, Dr. Smith would be considered a trustee pursuant to subsection 2(1)(t)(xii)(A) of HIPA as follows:

> **2**(1) In this Act:
>
> …

> (t) **"trustee"** means any of the following that have custody or control of personal health information:
>
> …
> (xii) a person, other than an employee of a trustee, who is:
>
> (A) a health professional licensed or registered pursuant to an Act for which the minister is responsible; or

[10] As such, Dr. Smith qualified as a trustee pursuant to HIPA. Dr. Smith has ongoing duties as a trustee even after his retirement for any personal health information in his custody or control as outlined at subsection 22(1) of HIPA as follows:

> **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.

[11] I now need to consider if Dr. Smith had custody or control of the personal health information at issue.

[12] "Custody" is the physical possession of a record by a trustee with a measure of control. "Control" means having authority over a record.

[13] At the time he destroyed his patient records, Dr. Smith was retired, but had been the sole owner of his medical practice. He stored the records prior to disposing them, and then took them to a third-party company, Cosmo Shred in Saskatoon, to have them shredded at his direction. Throughout, Dr. Smith continued to have control over the personal health information, including for their destruction. As such, the personal health information remained under Dr. Smith's custody and control and he had ongoing duties pursuant to section 22 of HIPA.

[14] As all three elements are present, I find that HIPA is engaged and that I have jurisdiction to undertake this investigation.

2. Did Dr. Smith meet his ongoing duties pursuant to section 22 including his duty to sufficiently safeguard and account for personal health information through storage to destruction pursuant to section 16 and subsection 17(2) of HIPA?

[15] Trustees have a duty to protect personal health information. This includes establishing policies and procedures to maintain administrative, technical and physical safeguards. Among other things, written policies and procedures should deal with how records are kept secure and managed. When such safeguards are lacking, privacy breaches can occur. Section 16 of HIPA provides as follows:

> **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.

[16] In this matter, I am considering whether Dr. Smith had appropriate safeguards in place to maintain the records of his former patients in a safe manner. This includes assessing what safeguards he had in place to protect them, including when he destroyed them. Subsection 17(2) of HIPA provides that a trustee must ensure personal health information is retained for the full retention period and destroyed in a secure manner:

> **17**(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);

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

What Occurred

[17] Prior to his retirement, Dr. Smith stated his office would periodically review patient records and securely destroy them when they were past their retention period. At the time of his retirement in December 2019, he retained 12 bankers' boxes (boxes) of patient records. The patient records were for patients Dr. Smith saw in the six years preceding his retirement in 2019. While practicing, Dr. Smith maintained the following two categories of records:

- Category 1: records for patients seen in the last three years; and
- Category 2: records for patients seen in the last four to six years.

[18] After closing his practice, Dr. Smith transported the records in his personal vehicle from his former office (in Yorkton, Saskatchewan) to an airplane hangar (hangar) at the Saskatoon Airport. Dr. Smith stated that he stored the patient records in the boxes on metal shelves in the hangar. Dr. Smith added that all doors were locked, that only he had a key, and that no one else accessed the space without being accompanied by him.

[19] After storing the patient records in the hangar for three years, Dr. Smith determined he could take them to be shredded. Dr. Smith stated he did not retain any documentation to help him determine when he should destroy the records. Instead, he said he relied on the fact that over three years had passed since his retirement, and apparently destroyed the records based on this assumption. He noted that his use of the two, three-year categories likely played a role in his mistaken belief that the retention period was three years. Dr. Smith apparently did not keep an index (or record) of which patient records he had retained or that he was destroying.

[20] On October 13, 2023, Dr. Smith took the records in his personal vehicle to Cosmo Shred to have them shredded at his direction. Dr. Smith advised that he did not witness the shredding, even though Cosmo Shred stated that customers have the option to remain outside of the destruction area while shredding occurs. Cosmo Shred added that if a

customer chooses to witness the shredding, then only that customer's materials are in their view.

[21] Cosmo Shred provided Dr. Smith with a Certificate of Destruction (Certificate) dated October 13, 2023, which verified that it had shredded the 12 boxes of records. While Dr. Smith stated that Cosmo Shred informed him shredding would occur the same day, Cosmo Shred noted that shredding would have been completed "no later than October 18, 2023, as our NAID [National Association for Information Destruction] certification requires us to have all materials destroyed within three business days". Cosmo Shred stated it does not maintain a record of the exact date that shredding for the ticket number assigned to each shredding job is completed. The Certificate issued to Dr. Smith states that the 12 boxes were "completely destroyed beyond recognition and recycled."

[22] Regarding the retention of patient records, section 23.1(f) of the College of Physicians and Surgeons of Saskatchewan's *Regulatory Bylaws for medical practice in Saskatchewan* dated January 19, 2024, provides as follows:

> **23.1 MEDICAL RECORDS**
>
> …
> (f) for the purpose of this paragraph the "last entry in the record" means the last entry of document received by the member which relates to the care provided by the member. A member shall retain the records required by this bylaw 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 for six years after the date of the last entry in the record, whichever is the later date.

[23] I add that on August 1, 2023, amendments to *The Health Information Protection Regulations* (HIPA Regulations) came into force. Section 6 of the HIPA Regulations provides the following regarding the retention and destruction of personal health information:

> **6** For the purposes of clause 17(1)(a) of the Act, a written policy concerning the retention and destruction of personal health information must include:
>
> (a) either:

> **(i) a requirement that personal health information be retained by a trustee for at least 10 years after the date of the last episode of care or until age 20 if the subject individual is a minor, whichever period is longer; or**
>
> **(ii) a retention schedule that sets out:**
>
> **(A) all legitimate purposes for retaining the information; and**
>
> **(B) the retention period and destruction schedule associated with each purpose set out pursuant to paragraph (A);**
>
> (b) measures to provide for the secure retention and destruction of records to minimize the risk of any unauthorized use or disclosure of, or unauthorized access to, personal health information; and
>
> **(c) a process to keep a record of:**
>
> **(i) the name of each individual whose personal health information is destroyed;**
>
> **(ii) a summary of what personal health information was destroyed;**
>
> **(iii) the time period of the personal health information;**
>
> **(iv) the method of destruction of the personal health information; and**
>
> **(v) the name and job title of the individual responsible for supervising the destruction of the personal health information.**
>
> [Emphasis added]

[24] It is possible that when Dr. Smith took all his records for destruction on October 13, 2023, he legitimately destroyed some records when they were due for destruction. It is also possible that he should have continued to retain others within the required six years. It is further possible that the amendment to the HIPA Regulations may have had some bearing on the retention period of some of his patient files. At any rate, because he did not keep an index of patient records, and because all the records are already destroyed, it is not known what the individual status of each patient record would have been.

[25] As previously stated, lacking any type of safeguard can lead to a situation where a privacy breach may occur. Based on what occurred, it appears that Dr. Smith lacked both administrative and physical safeguards. I will discuss each separately.

Administrative Safeguards

[26] Administrative safeguards focus on internal policies, procedures and maintenance of security measures that protect personal health information. It includes, among other things, written policies and procedures, written retention and destruction schedules, and agreements with Information Management Service Providers (IMSP).

[27] Dr. Smith stated that when he retired, he did not retain a copy of policies and procedures related to retention and destruction. On August 1, 2023, subsection 17(1) of HIPA was proclaimed, which addressed the requirement for a trustee to have written policies for the retention and destruction of personal health information. However, even before the proclamation of this subsection, such policies and procedures would be best practice and an example of an administrative safeguard to protection personal health information, pursuant to section 16 of HIPA. The provision at subsection 17(1) of HIPA, which would have been in force at the time of the destruction of the records, provides the following requirement for trustees regarding a retention and destruction policy:

> **17**(1) A trustee must:
>
> (a) have a written policy concerning the retention and destruction of personal health information that meets the requirements set out in the regulations; and
>
> (b) comply with that policy and any prescribed standards with respect to the retention and destruction of personal health information.

[28] Keeping these policies and procedures would have helped him determine the correct retention and destruction periods for each of his patient records and ensure the personal health information was retained for the full retention period, as required by section 17(2)(a) of HIPA. CPSS' resource, *Leaving Practice, a Guide for Physicians and Surgeons* (May 2023), states that physicians who leave practice must ensure former patients have access

to their records to support continuity of care. This requires preserving patient records and destroying them only when it can be confirmed that they can be destroyed.

[29] In terms of such confirmation, what would have helped Dr. Smith keep track of his former patients' records is to have kept an index. In past investigation reports of my office involving medical professionals (e.g., Investigation Report 154-2022 and Investigation Report H-2011-001), it was stated that one of the strongest safeguards a doctor can put into place is to document or inventory records going for destruction. Both these reports quoted the following from *The Canadian Medical Protective Association* (February 2022):

> Before destroying records, it is recommended that you make a list of the names of the patients whose records are to be destroyed, and that this list be kept permanently in a secure location. This is to be able to later determine at-a-glance that a medical record has been destroyed and not simply been lost or misplaced.

[30] Because he did not keep an index, he could not account for the record of the former patient who had asked for theirs. Going forward, it also makes it impossible for him to account for the records of other former patients who might come forward. An index would have helped him clearly identify which patient records he had, and which he had already sent for destruction; or, in general, to just to be able to account for them. It would have also helped identify if any patient records were possibly subject to the amended HIPA Regulations, and thus should have been retained for 10 years.

[31] Earlier, I noted that Cosmo Shred does not maintain a record of the exact date it completes the shredding for each ticket number assigned to each job. My office asked Cosmo Shred for any documentation relating to the shredding completed for Dr. Smith. Along with a copy of the Certificate, Cosmo Shred provided my office with an invoice addressed to "walk-in" with a ticket number, and further noted the following:

> The customer delivered 12 boxes to our facility and did not request a name on the invoice, we did not do a pickup request for this customer therefore a service agreement would not be required as we take debit and credit for payment, the boxes would not have left our facility and would have been on camera the entire time, we are only required by I-Sigma to have video stored for 90 days. The boxes would have been

> destroyed no later than October 18th, 2023, as our NAID certification requires us to have all material destroyed within 3 business days.
>
> In November or December, the customer came back in with his invoice to request a Certificate of Destruction which I was able to find due to the invoice number being present, I then wrote his name, and signed the document, in the PDF you'll notice that we have language which would qualify as a Certificate of Destruction on our walk-in invoices…

[32] Upon review of the Certificate, I note that it has Dr. Smith's name on it, but it does not verify the types of records that Cosmo Shred destroyed for him. Because Dr. Smith's Certificate serves as an official record of what he destroyed, it should have stated that personal health information was being destroyed.

[33] Another administrative concern is with the agreement for shredding between Dr. Smith and Cosmo Shred. Cosmo Shred would qualify as an IMSP pursuant to subsection 2(1)(j) of HIPA, which provides as follows:

> **2**(1) In this Act:
>
> …
> (j) **"information management service provider" <u>means a person who or body that processes, stores, archives or destroys records of a trustee</u>** 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;
>
> [Emphasis added]

[34] Subsection 18(2) of HIPA lays out what elements a written agreement between a trustee and an IMSP must cover. The agreement should include elements such as how the records will be destroyed and by what method (e.g., will an entire box be shredded, or will records be removed from the box prior to shredding), how the records will be kept secure while awaiting shredding, and who will have access to the records during this time. Subsection 18(2) of HIPA provides as follows:

> **18**(2) Before providing personal health information to an information management service provider, **a trustee must enter into a written agreement** with the information management service provider that:
>
> (a) governs the access to and use, disclosure, storage, archiving, modification and destruction of the information;
>
> (b) provides for protection of the information; and
>
> (c) meets the requirements of the regulations.
>
> [Emphasis added]

[35] Dr. Smith advised that he did not inquire with Cosmo Shred as to the safeguards they had in place and selected them because they offered "confidential shredding". When a trustee involves an IMSP, the trustee should ensure the agreement is in compliance with subsection 18(2) of HIPA. Cosmo Shred's general service agreement states as follows:

> **1) Confidential Shredding:** Cosmo Shred will provide Services for the secure destruction of Customer documents ("Services"). The Services may, at Customer's option, be performed as part of a regular schedule or pursuant to specific directions which Customer shall give Cosmo Shred from time to time. Cosmo Shred will pick up material from the Customer. Destruction of confidential documents will be **undertaken at Cosmo Shred's secure location**. Cosmo Shred assumes responsibility only when the driver takes control of document/materials. All work will be done in a timely and secure manner to insure complete confidentiality. **Cosmo Shred** is **AAA Certified by NAID**.
>
> [Emphasis in original]

[36] While Cosmo Shred's standard agreement states destruction will occur at its secure location and that work will be timely and secure, the agreement does not fully describe how the records themselves will be managed within the facility. In this case, as Dr. Smith was a walk-in customer who transported the records to Cosmo Shred's facility in his personal vehicle. Cosmo Shred stated that as he was a walk-in, it did not require Dr. Smith to sign their agreement.

[37] Not signing an agreement is concerning, but the bigger issue here is that trustees need to drive the development of an agreement and be satisfied that an IMSP's agreement meets

the requirements set out in subsection 18(2) of HIPA. Additionally, as noted earlier in this Investigation Report, subsection 17(2)(b) of HIPA requires that a trustee ensure "personal health information is destroyed in a manner that protects the privacy of the subject individual." In order to comply with subsection 17(2)(b) of HIPA, Dr. Smith should have taken appropriate steps to ensure Cosmo Shred had appropriate safeguards in place for the destruction of the records to protect the personal health information. This was not the case here. It is incumbent on trustees to know and understand what processes or procedures an IMSP will use to securely shred records and how it will keep the records secure throughout the process. A trustee should then seek to ensure this type of information is included in a service agreement that the trustee either drives or develops.

Physical Safeguards

[38] Physical safeguards include measures taken to physically protect personal health information from natural and environmental hazards, as well as unauthorized intrusion. Physical safeguards include locked cabinets and storage rooms and alarm systems.

[39] Trustees have an obligation to store records in a place that is safe and protected from the elements, including from water or fire damage. They are also required to keep records stored in a place that is kept locked and where personal health information is not accessible to unauthorized individuals.

[40] My office asked Dr. Smith how he transported and stored his patient records after he closed his medical practice. He responded that he transported the records in his personal vehicle, a truck with a box cap, and when he did so, he was the only occupant. Dr. Smith added that he drove directly from the Yorkton clinic to the hangar where he stored the boxes of records on metal shelves. Dr. Smith noted that the hangar did not have a security system, but that there would have been security checks to reach the hangar due to it being located at the Saskatoon airport. Dr. Smith added that he is the only person with a key to the locks on the hangar and that no one had access to the space without being accompanied and supervised by him at all times. As an example, Dr. Smith stated that he was present when a mechanic

attended the hangar to conduct annual inspections on the airplane that was also stored in the hangar.

[41] My office's resource, *Best Practices for Transporting Personal Information (PI) and Personal Health Information (PHI) Outside of the Office* provides the following regarding transporting records:

> The following are some safeguards to consider when transporting PI and PHI outside of the office:
>
> …
>
> - Have secure storage that is approved by your organization for your files that are outside of the office and are being transported from place to place.
>
> - Do not leave files in vehicles unattended.
>
> …
>
> - Do not leave laptops, computers, documents, or anything containing sensitive information unattended.

[42] In Investigation Report 124-2017 and 135-2017, my office also noted the following regarding the transportation and handling of patient records:

> [27] Also, I recommend that Dr. A. Lawani establish policies and procedures regarding the transportation and handling of patient records. For example, after she obtains records… she may have to physically transport them to the billing clerk. The records should be locked in a storage case (such as briefcase or a storage box) and also locked in the trunk of a vehicle. Unless there are no alternatives, the records should not be left unattended in the trunk while she is elsewhere.

[43] Other resources, such as *Guidelines for Protecting Medical Records Outside the Practice* from the British Columbia Medical Association (BCMA), caution that records left unattended in a trunk are "no less accessible to thieves than the front seats". The BCMA also advises that records should not be visible or in view, and if kept in boxes, the boxes themselves should be secured (e.g., taped closed). Finally, the BCMA recommends the use of a courier service when transporting a large number of records.

[44] It is unclear if Dr. Smith actually took any of the steps outlined above, such as ensuring the records were not visible inside his truck box or if there were any periods where he may

have left the records unattended. What may have minimized any of the associated risks in this matter, is to have considered options such as using a secure courier service or pick up service, such as those offered by shredding companies.

[45] Regarding storage, my office asked Dr. Smith if he could provide photos of the hangar or a floor plan of the space. In response, Dr. Smith advised he was "unable to provide a floor plan or pictures depicting where the records were stored." As he was unable to provide this information, it is unclear if the hangar had an office or enclosed storage area, or even if it had locked cabinets that he could have stored the records in. The use of a locked space or cabinet allows for an additional layer of physical security that can protect records from unauthorized accesses, and to also protect them from the elements or damage (e.g., water damage).

[46] Regarding the shredding, Cosmo Shred stated it would have removed the records from the boxes prior to shredding, and that the shredding process is supervised. As previously noted, Dr. Smith chose to not witness the shredding, and so would not be able to confirm what steps Cosmo Shred took or what processes it followed. Cosmo Shred also added that, in this matter, shredding would have occurred "no later than October 18, 2023", which means Dr. Smith's records could have been shredded the day he dropped the records off, or on a later date. As trustee, Dr. Smith needed to be aware of how Cosmo Shred would have managed the records if it had to store them for any length of time prior to shredding them to ensure they would have been physically protected from unauthorized access.

Conclusion and Recommendation

[47] Because Dr. Smith did not ensure adequate administrative and physical safeguards were in place, I find that he did not meet his obligations as a trustee to protect personal health information pursuant to section 16 of HIPA. By not doing so, he left the records of his former patients open to potential privacy breaches. I find that Dr. Smith also failed to ensure that the personal health information was properly accounted for and retained for the full retention period and to ensure the IMSP had appropriate safeguards in place to protect

the privacy of patients pursuant to section 17(2) of HIPA. Accordingly, I find that he did not meet his ongoing requirements pursuant to section 22 of HIPA.

[48] Regarding recommendations, Dr. Smith no longer practices, and has already destroyed the patient records that were in his possession and control. He also did not keep an index of the patient records he had retained. This limited his ability to ensure continuity of care, and his ability to provide direct notice to his former patients of what occurred. He should make efforts, to provide such notice. As such, I recommend that Dr. Smith place an advertisement in a community newspaper in Yorkton, where he formerly practiced, so his former patients are aware that their records have been destroyed.

III FINDINGS

[49] I find that I have jurisdiction to conduct this investigation.

[50] I find that Dr. Smith did not meet his ongoing duties pursuant to section 22 including his duty to sufficiently safeguard and account for personal health information through to destruction pursuant to section 16 and subsection 17(2) of HIPA.

IV RECOMMENDATION

[51] I recommend that within 30 days of issuance of this Investigation Report, Dr. Smith place an advertisement in a community newspaper in Yorkton, where he formerly practiced, so his former patients are aware that their records have been destroyed.

Dated at Regina, in the Province of Saskatchewan, this 8th day of July, 2024.

Ronald J. Kruzeniski, K.C.
A/Saskatchewan Information and Privacy Commissioner