Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 251-2024, 004-2025

Dr. Chukwuemeka Odenigbo and Dr. Nebeolisa Ezeasor (Elphinstone Medical Clinic)

March 26, 2025

Summary: Two individuals learned on social media about abandoned patient records containing personal health information in the area surrounding the Elphinstone Medical Clinic (Clinic) in Regina. Out of concern, they went (on their own at separate times) to search the area and recover what records they could. It was later determined that the records belonged to patients of Dr. Chukwuemeka and Dr. Nebeolisa Ezeasor (Dr. Odenigbo and Dr. Ezeasor), who are associated with the Clinic; they are also trustees of the personal health information contained in the patient records at issue. An employee of the Clinic's contracted cleaner had discarded the records, which were intended to be shredded, into a blue recycling bin behind the Clinic. The A/Commissioner opened investigation files into the matter. After finding that a privacy breach occurred, the A/Commissioner found that Dr. Odenigbo and Dr. Ezeasor had not taken any steps to ensure the breach was contained and did not provide adequate notice to affected individuals. The A/Commissioner also found that the trustees had not complied with their obligations to protect the personal health information in their custody and control pursuant to sections 16 and 17 of *The Health Information Protection Act*, and sections 5 and 6 of *The Health Information Protection Regulations, 2023*. The A/Commissioner made recommendations accordingly.

I BACKGROUND

[1] Regina's Elphinstone Medical Clinic (Clinic) has a contract (with its owner Dr. Chukwuemeka Odenigbo) with a cleaning company to do its cleaning. On October 26, 2024, an employee of the cleaning company dumped medical records (records) from open recycling bins inside the Clinic and placed them, unshredded, in a big blue recycling bin

behind the Clinic. The open recycling bins inside the Clinic indicated the contents were confidential and for shredding.

[2] On October 27, 2024, Individual A saw a post on a Facebook community group about patient records being strewn outside the Clinic. Out of concern, Individual A went to investigate and found the records, loosely blown about, in the alley behind and in the empty lot north of the Clinic. Individual A retrieved what records they could find and took them home for safekeeping.

[3] On October 28, 2024, Individual A reported the matter to my office. That day, Individual A met with staff from my office behind the Clinic to turn over the recovered records and to show where they had recovered them. My staff also swept the area outside the Clinic and retrieved one additional medical record.

[4] Upon reviewing the records Individual A had provided, it seemed apparent to my office that they came from the Clinic as some records identified Dr. Nebeolisa Ezeasor (Dr. Ezeasor), one of the psychiatrists associated with the Clinic. On October 28, 2024, my office contacted the Clinic and spoke with its office manager to discuss what had occurred. The office manager agreed to relay the message and have Dr. Ezeasor and Dr. Chukwuemeka Odenigbo (Dr. Odenigbo), another psychiatrist associated with the clinic (the owner), arrange to come to my office to identify the records.

[5] On October 28, 2024, the College of Physicians and Surgeons of Saskatchewan (CPSS) also contacted my office to advise that an individual had contacted it about records "blowing around the alley" behind the Clinic. My office confirmed with CPSS that our office had received a call and was looking into the matter, including contacting the Clinic.

[6] On October 29, 2024, a second individual, Individual B, contacted my office to state that they had also seen the Facebook community message about the records on October 27, 2024. Out of concern, they indicated that they also went to the Clinic on that same day to investigate and collect what records they could find (I note that it appears that Individual B searched around the Clinic earlier in the day than Individual A had). Individual B said

they retrieved records from the blue recycling bin behind the Clinic, and in the immediate area surrounding the bin. They thought they had collected about 100 pages. Individual B added that they reported the matter to the CPSS. On the afternoon of October 29, 2024, Individual B dropped off at my office the records they had retrieved.

[7] On October 29, 2024, Dr. Ezeasor and Dr. Odenigbo contacted my office. My office advised them of what had occurred and provided a general description of the records. My office confirmed that the records would be kept secured in my office. My office stated the first step would be for the doctors to come identify the records as belonging to the Clinic; if they could do so, then my office would discharge the records to their custody. My office also let them know that CPSS was aware of what had occurred.

[8] On October 30, 2024, both doctors attended my office, and when it became clear that the records came from the Clinic, my office discharged the records into their custody. My office also advised them that I would be undertaking an investigation and would be issuing a public investigation report.

[9] On October 31, 2024, my office provided notification to Dr. Ezeasor and Dr. Odenigbo asking them to complete and return a copy of my office's *Privacy Breach Investigation Questionnaire*. My office asked the doctors to include any necessary supporting documentation.

[10] My office also instructed Dr. Ezeasor and Dr. Odenigbo to not destroy any materials related to the investigation. My office also advised that, pursuant to section 17 of *The Health Information Protection Act* (HIPA) and section 6 of *The Health Information Protection Regulations, 2023* (HIPA Regulations), the records may not yet be up for destruction.

[11] On December 12, 2024, legal counsel for Dr. Ezeasor and Dr. Odenigbo provided the Clinic's submission.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[12] HIPA applies when three elements are present: 1) there is personal health information; 2) there is a trustee involved; and 3) the personal health information is in the custody or control of the trustee.

Personal health information

[13] The doctors acknowledge that the records contain the "patient names, dates of birth, and descriptions of their symptoms and medical treatment" of 88 individuals.

[14] Upon review, most of the records found were copies of a "Psychiatric Intake Form", which appears to be a standardized type of intake that psychiatrists use with patients. The form contains the patient's name, date of birth, names of primary care physician and counselor/therapist, and sections to indicate what issues they are currently experiencing. Responses may regard risk to suicide, substance use (including illegal substances), family background/history (including names/ages of family members and details of current or past relationships), medications used, and history of trauma or abuse.

[15] Other medical records include self-assessments or questionnaires that ask yes/no types of questions, or that elicit details on symptoms, etc., of various conditions. There are also letters or notes from family doctors or other specialists (e.g., other psychiatrists) forwarding assessment information that includes matters such as reasons for referral, chief complaints, history of presenting illness, summary of psychiatric concerns, medical history (e.g., history of surgeries or physiological/medical conditions), medications prescribed or history of, known allergies, social development, and impressions. Some documents contain a score, which appears to relate to how likely someone is to be predisposed to a condition or to be affected by one, or that may be used for diagnostic purposes. There also appears to be records from when individuals attended at the hospital. These records also contain information such as presenting information and medical history. All these other types of records also invariably contain tombstone information such as the patient's name, date of birth, address, Saskatchewan Health Number (SHN), etc. (which I have commonly referred

to as registration information; see Investigation Report 008-2017). Of note, most records appear to have been dated between October 1st to 4th 2024; some records, such as ones that would be attachments to letters or referrals, are older but still appear to have been created within the year prior to October 2024.

[16] All this information is considered 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;

[17] As there is personal health information, the first element is met.

Trustee

[18] Dr. Odenigbo and Dr. Ezeasor advised my office that of the 88 affected patients, 86 were Dr. Ezeasor's patients, and two were Dr. Odenigbo's. The doctors provided my office with copies of their separate electronic medical record (EMR) service agreements. Based on the agreements, each is responsible for his own EMR and patient records.

[19] According to the CPSS website, Dr. Odenigbo and Dr. Ezeasor are licensed health professionals (psychiatrists) in the province. Practice as a psychiatrist in the province is governed by *The Medical Professions Act, 1981*, and so a medical professional would qualify as 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

[20] Based on this information, each is a trustee pursuant to subsection 2(1)(t)(xii)(A) of HIPA. My office opened two separate files – one for each trustee.

[21] Further, an Information Services Corporate Registry search confirms that the Clinic's owner is Odenigbo Medical Prof. Corporation of Regina. The owner, Dr. Odenigbo, is listed as sole proprietor, and the registration is effective from August 16, 2017, to August 31, 2026. Subsection 4(b) of the HIPA Regulations states as follows:

> **4** For the purposes of subclause 2(1)(t)(xv) of the Act, the following are prescribed as trustees:
>
> …
> (b) every person who owns or operates a privately-owned facility in or from which health services are provided by a health professional;

[22] Dr. Odenigbo further qualifies as a trustee pursuant to subsection 4(b) of the HIPA Regulations.

[23] I will next determine if the trustees have custody or control.

Custody or control

[24] On the third element, "custody" is the physical possession of a record by a trustee with a measure of control. "Control" connotes authority. Personal health information is under the control of a trustee when the trustee has the authority to manage the information, including restricting, regulating and administering its use, disclosure or disposition. Custody is not a requirement for control to be present (Investigation Report 306-2019 at paragraphs [15] to [16]).

[25] Dr. Odenigbo and Dr. Ezeasor each has his own EMR containing the medical records of their respective patients. As noted, the records came from the Clinic. The personal health information in this matter was therefore, in their respective custody or control.

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

2. Did a privacy breach occur?

[27] As described earlier in this Investigation Report, patient records containing personal health information were found scattered outside the Clinic. A privacy breach occurs in different ways, including if there is an unauthorized disclosure of personal health information. Privacy breaches can result from the inappropriate management of personal health information, such as by not following legal obligations for retention and disposal.

[28] As stated, Individuals A and B saw the records outside the Clinic. Individuals A and B took physical possession of the records they collected to keep them safe. I will speak a bit more to these exposures, as well as other potential exposures, later in this Investigation Report, but anyone who saw the records outside the Clinic was not authorized to view them, and so the disclosure of the records was also not authorized.

[29] Dr. Odenigbo and Dr. Ezeasor acknowledge that a "breach occurred due [to] an error made by an employee of the cleaning company…" They advised that the breach occurred on

October 26, 2024, and have accepted responsibility. They do not dispute the fact that a privacy breach occurred.

[30] I find, therefore, that a privacy breach occurred. I will assess how Dr. Odenigbo and Dr. Ezeasor managed the breach.

3. Did Dr. Odenigbo and Dr. Ezeasor properly manage the privacy breach?

[31] My office's *Rules of Procedure*, outlines that my office will analyze whether the trustee properly managed the breach and took the following steps in responding:

- Contain the breach (as soon as possible);
- Notify affected individuals (as soon as possible);
- Investigate the breach; and
- Prevent future breaches.

[32] I will assess each step separately and make recommendations accordingly.

Contain the breach (as soon as possible)

[33] Upon learning that a privacy breach has occurred, steps should be taken to immediately contain the breach. Depending on the nature of the breach, this can include:

- Stopping the unauthorized practice;
- Recovering the records;
- Shutting down the system that has been breached;
- Revoking access privileges; and
- Correcting weaknesses in physical security.

(*Privacy Breach Guidelines for Trustees*, August 2022, p. 3)

[34] In terms of containment, Dr. Odenigbo and Dr. Ezeasor acknowledge that my office discharged to their custody the records recovered by Individuals A and B. Subsequently, they "reviewed and cataloged" the records. They added that the "matter was immediately raised with the contractor, and the contractor took steps to address the employee's performance…" They did not provide much else beyond this to address containment efforts.

[35] As part of analyzing containment, I must conclude that the trustee took reasonable steps to contain the breach. I want to have some reassurance that the trustee has reduced the magnitude of the breach and the risk to individuals. I caution that while containment is the end goal in mind, it is not common that full containment in a breach such as this can ever be guaranteed or achieved. There are several reasons for this, which I outline below.

[36] While Individuals A and B were arguably the biggest contributors to containment by retrieving and turning the records over to my office, there is the fact that the records were exposed to them. That is, they could have viewed them, and even if they did not physically retain or copy any personal health information, they could have committed personal health information to memory. A privacy breach occurs when an unauthorized individual sees or overhears the personal health information of others being communicated.

[37] This brings me to the fact that other individuals who read about the records on Facebook may have gone searching, found records, and not turned anything over. I have no proof that this occurred, but it is a possibility. I add that this matter occurred on a weekend when there was a football game (October 26, 2024), at the nearby stadium. Game attendees often park in surrounding neighborhoods and walk to the stadium. Anyone walking behind the Clinic that day, or even parking there, may have come across and viewed the records and even picked some up.

[38] Further, there are residential areas directly behind and to the south of the Clinic that share the same alleyways. There is a possibility that records could have blown into some yards and been picked up by the homeowners. None have come forward to my office, and the

Clinic has not reported that any have either, but it does not negate the fact that neighboring homeowners may have found records.

[39] In this matter, physical containment efforts were taken by external parties. Dr. Odenigbo and Dr. Ezeasor could have taken some steps towards containment by, for example, following up with individuals on the Facebook group who may have indicated they found or saw records, or by asking residents who share the alleyway if they had found or seen records. Given that they did not take such steps, I find that Dr. Odenigbo did not take adequate steps to ensure the breach was fully contained.

Notify affected individuals (as soon as possible)

[40] It is a best practice to inform affected individuals and my office of a privacy breach. The following is a list of individual organizations that may need to be notified as soon as possible after learning of the incident:

- The organization's privacy officer;
- My office;
- The police, if criminal activity is suspected; and
- The affected individual(s) (unless there are compelling reasons why this should not occur).

(*Privacy Breach Guidelines for Trustees*, pp. 3 - 4)

[41] Providing notice to individuals affected by the breach should occur as soon as possible after key facts about the breach have been established. In terms of notification, my office's resource, "Privacy Breach Guidelines for Trustees" offers the following guidance at page 4:

> It is best to contact affected individuals directly, such as by telephone, letter or in person. However, there may be circumstances where it is not possible, and an indirect method is necessary or more practical. Such situations would include where contact information is unknown or where there are a large number of affected individuals. An indirect method of notification could include a notice on a website, posted notices,

media advisories, and advertisements. Ensure the breach is not compounded when using indirect notification.

[42] Soon after learning of the breach, Dr. Odenigbo and Dr. Ezeasor stated that they notified "approximately 14" patients in person. Legal counsel for the doctors stated that these patients were advised of the events involving the cleaning staff, how the Clinic stores the records within the Clinic, how the records were discovered and that my office was contacted, and that they will be provided a written letter.

[43] They also provided my office with a copy of their draft notification letter to affected individuals. The elements contained in the letter include the following: what occurred including the circumstances that led to the breach; that records were discovered by members of the public and returned to the Clinic via my office; information on how to minimize risk by monitoring credit; an apology for what occurred; and the right to contact my office including information on how to do so. Regarding risk, the letter stated that "there is still a risk of identity theft, as it contained your [name] and [birth date]." The doctors' legal counsel did confirm with my office on February 24, 2025, that they had mailed their notices to affected individuals.

[44] The letter does not state exactly what data elements are or were involved for each affected individual; rather, the letters only state in a general way that "a privacy breach… recently took place involving your personal health information." At paragraphs [14] and [15] of this Investigation Report, I laid out in detail the types of data elements or personal health information at stake in many of the records found. While the level of detail of personal health information may vary for each affected individual, there are some details that could lead to an increased risk of identity theft, because of the inclusion of home addresses, telephone numbers and SHNs. Given the highly sensitive nature of some of the personal health information involved, there is also a risk to reputation or character. In my office's Investigation Report 129-2024, concerning the Ministry of Advanced Education, I discussed that affected individuals should be apprised of the possible types of harm that may result from the privacy breach. Harm is linked to the types of data elements breached.

[45] While the doctors' notice does include risk of identity theft based on name and birth date, the notices should have also included what specific data elements were involved for each patient so that the doctors, and affected individuals, could have gauged personal risk accordingly. The letters should have also included ways that affected individuals could mitigate risks such as risk to reputation.

[46] In my office's Investigation Report 129-2024, I also discussed that affected individuals should be offered credit monitoring. The doctors did advise affected individuals to monitor their credit, but did not offer any credit monitoring. In Investigation Report 129-2024, I stated that the length of credit monitoring provided should depend on the level of risk and other factors that may mitigate that risk. In my office's Investigation Report 136-2024, 169-2024, 183-2024, 187-2024, 191-2024, for example, my office recommended that 10 years credit monitoring be offered because of a cybersecurity breach in which over 7,000 individuals were affected. In this matter, the risk of identity theft is comparatively low because there is a sense of how many individuals were affected and how many records recovered, even if it is possible some records were not recovered, and because the incident did not involve something like a cybersecurity breach. In Investigation Report 129-2024, I found the circumstances of that matter were such that one year of credit monitoring be offered based on the number of affected individuals (121) and the types of data elements involved. I am of the same view here that one year of credit monitoring would be appropriate given that there were 88 identified affected individuals, and that it is likely, but not certain, that most records were recovered.

[47] Based on this, I find that Dr. Odenigbo's and Dr. Ezeasor's notice letters should have included what exact data elements were involved for each affected individual and the type of risk associated with those data elements, and that they should have also included a one-year offer of credit monitoring. I recommend that within 30 days of the issuance of this Investigation Report that Dr. Odenigbo and Dr. Ezeasor update their policies and procedures to ensure that privacy breach notice templates include the specific types of data elements involved and what the associated risks may be. I also recommend that within 30 days of the issuance of this Investigation Report, that Dr. Odenigbo and Dr. Ezeasor offer affected individuals one year of credit monitoring.

Investigate the breach

[48] When considering why a privacy breach occurred, a trustee should reflect on the root causes, or what led to the breach occurring. It is an important step in mitigating the risk of a future breach of a similar nature from occurring. The following are some key questions to ask during a privacy breach investigation:

- When and how did your organization learn of the privacy breach?
- What occurred?
- How did the privacy breach occur?
- What is the applicable legislation and what specific sections are engaged?
- What safeguards, policies, and procedures were in place at the time of the privacy breach?
- Was the duty to protect met?
- Who are the affected individuals?

(*Privacy Breach Guidelines for Trustees,* p. 5*)*

[49] Section 16 of HIPA sets out a trustee's duty to protect personal health information in its custody or control. It is one of the most important provisions of HIPA, placing a duty on trustees to make sure they have comprehensive written policies and procedures to keep trustees from falling short in their duties. This provision 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.

[50] The purpose of investigating a privacy breach is to identify the root cause. In any investigation, assessing the root cause is to investigate where a trustee did not have any or adequate safeguards in place to prevent a privacy breach from occurring. Safeguards can be administrative (e.g., policies, procedures, confidentiality statements on contracts), technical (e.g., access controls on electronic storage) or physical safeguards (e.g., locked cabinets or bins, locked doors, security cameras). When a trustee says the root cause was human error, what a trustee needs to consider is what led to the human making the error. On the prevention side, they can then look at what measures to put in place to minimize the possibility that the same error will occur again.

[51] I will separately review the factors that contributed to the root cause of the breach. When I consider prevention, I will make recommendations on how Dr. Odenigbo and Dr. Ezeasor can make their practices more compliant with sections 16 and 17 of HIPA, and sections 5 and 6 of the HIPA Regulations.

a. Contractor

[52] As mentioned previously in this Investigation Report, Dr. Odenigbo and Dr. Ezeasor learned of this privacy breach from my office on October 28, 2024. They claimed the breach occurred when an employee of the cleaning company they contract with placed the records in the blue recycling bin behind the clinic. The contractor noted that they could not do the cleaning that day, and that one of their employees who came in to do the cleaning was responsible for the breach. The doctors noted that this employee apparently neglected to notice that the plastic bins used to place records prior to shredding were marked as confidential and for shredding. They identified the root cause as "human error." They added:

> A contractor's employee was the cause of the privacy breach. The matter was immediately raised with the contractor, and the contractor took steps to address the

> employee's performance. The measures taken by the contractor are outlined in the enclosed letter of [name withheld] dated November 7, 2024.

[53] The contractor apparently terminated the employee who had caused the breach. The doctors' legal counsel also stated that as the Clinic has changed its practice to lock any shredding up at the end of the day, the contractor should no longer encounter any personal health information.

[54] The doctors' legal counsel provided my office with a copy of the contractor's signed "Confidentiality Agreement for Patient Records" (confidentiality agreement). The confidentiality agreement outlines the obligation of the cleaner to "maintain strict confidentiality regarding all Confidential Information." The contractor was apparently trained by Clinic staff who are responsible for privacy. The doctors' legal counsel explained that the contractor was responsible for training any of their employees on the need for confidentiality, adding as follows:

> …prior to the breach, Dr. Odenigbo and Dr. Ezeasor understood that [name withheld] was the only person attending the Clinic to clean. They did not know [they] had staff. Further, they never tasked [name withheld] with shredding paper records. Dr. Odenigbo and Dr. Ezeasor understood that [name withheld] was trained on securing any paper documents in the Clinic. In other words, [they were] trained that any paper documents [they] may encounter while cleaning the Clinic are private and they should not be disturbed.

[55] Upon review, the confidentiality agreement is specifically between the Clinic (signed by Dr. Odenigbo) and the contractor. It does not mention anything about employees of the contractor who may substitute for the contractor, or anything about who should train such substitutes. The confidentiality agreement does appear to consider the contractor as an "employee" of the Clinic. Subsection 2(1)(a)(i) of the HIPA Regulations defines a contractor as an "employee" as follows:

> **2**(1) In these regulations:
>
> …
> **"employee"** means:
>
> (a) an individual:

> (i) who is employed by a trustee, including an individual retained under a contract to perform services for the trustee; and
>
> …
> but does not include a health professional who is retained under a contract, that is not an employment agreement, to perform services for the provincial health authority;

[56] Subsection 16(c) of HIPA states that trustees are supposed to establish policies and procedures regarding administrative, technical and physical safeguards and ensure that their employees comply with HIPA in this regard. Section 5 of the HIPA Regulations further states as follows:

> **5** To ensure compliance with the Act by its employees, a trustee that has custody or control of personal health information must:
>
> (a) provide orientation and ongoing training for its employees about the trustee's policies and procedures respecting the protection of personal health information; and
>
> (b) ensure that each of its employees signs a pledge of confidentiality that includes an acknowledgement that the employee:
>
> (i) is bound by the trustee's policies and procedures mentioned in clause (a); and
>
> (ii) is aware of the consequences of breaching those policies and procedures.

[57] Section 5 of the HIPA Regulations places the onus on a trustee to ensure that the trustee provides orientation on HIPA to all its employees, including contractors, and that the trustee has them sign a pledge of confidentiality. Even if the contractor apparently no longer has access to any personal health information (or should no longer have exposure to any), the confidentiality agreement in this matter was only between the Clinic and the contractor (or employee). While the doctors state they did not know the contractor would send a substitute in to clean that day, the confidentiality agreement with the contractor should clearly express that a contractor needs to make known if any of their employees will be attending the office and provide a list of those employees, and that those employees also need to be trained by the trustee (or Clinic) and sign an oath of confidentiality.

b. Process for the destruction of paper records

[58] When disposing of or destroying paper records that have been scanned into an EMR, trustees need to manage them in accordance with HIPA that provide for their secure retention and destruction. Trustees are to ensure that employees follow such policies and procedures pursuant to section 16 of HIPA. Section 17 of HIPA also requires a trustee to ensure they have written policies regarding the retention and destruction of personal health information and to ensure that personal health information is stored in a format that is retrievable, readable and useable. Section 17 of HIPA provides as follows:

> **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.
>
> (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.

[59] Essentially, if a trustee uploads personal health information to an EMR, the trustee must ensure that the source (paper) record on which the copied (or digitized) record is based is managed and destroyed in an appropriate manner. Trustees must also ensure that the copied or digitized record is "retrievable, readable and useable" for the purpose for which it was collected. Neither HIPA nor the HIPA Regulations define these terms, but the *Oxford Dictionary* (2025) offers these definitions:

- "Retrievable" means the ability to "find or extract (information stored in a computer)"; "the ability to store, update, retrieve and print your data".

- "Readable" means "(of data or a storage medium or device) capable of being processed by a computer or other electronic device."
- "Useable" means "able to be fit or used".

[60] In terms of personal health information, this means that once a paper record is uploaded to an EMR, a trustee should have a process to verify that the uploaded record of personal health information can be used in the same way a paper record can be. For example, a physician should be able to update the record or print a copy if a patient requests one. The record should also be able to be viewed or read in a common format. A trustee should not destroy the paper record until verifying this. All this should be outlined in a trustee's policies and procedures.

[61] The doctors provided my office with a copy of the Clinic's "Privacy Policy Document." The "Destruction/Disposal…" policy states as follows:

> …
> 6. When transferring personal health information to a new system, this Medical Practice will not destroy or dispose of the existing personal health information until the accuracy and integrity of the information transferred to the new system has been documented.

[62] I note that the Clinic's policies and procedures do state that personal health information, when "transferred to the new system" won't be destroyed or disposed of until the "accuracy and integrity" of the scanned personal health information "has been documented." The Clinic's policies and procedures do not outline how this will be accomplished or by what procedures.

[63] For guidance on the topic of handling paper records that have been scanned into an EMR, my office consulted several resources.

[64] The Canadian Medical Protective Association (CMPA) states the following regarding the destruction of paper records:

> Most, if not all, Colleges permit the destruction of paper records once they have been appropriately scanned. When the appropriate steps have been taken, it may be reasonable to destroy the original record in a manner in keeping with physicians'

> obligation of confidentiality as well as any applicable legislative and College requirements. In exceptional cases, such as when the quality of the paper records makes the converted document difficult to read, it may be prudent to retain the paper records for at least the period of retention recommended by the CMPA.

[65] The CPSS states the following in its *Confidentiality of Patient Information* guidelines:

> **a. QUESTION**: Can physicians destroy paper records if the information from those records is scanned into an electronic health record?
>
> **Answer**: Neither *The Health Information Protection Act* nor College bylaws require a physician to keep more than one source of information. If all of the information in the paper record is contained in the electronic health record the paper record can be destroyed using a method which protects the confidentiality of that information.
>
> [Emphasis in original]

[66] The Provincial Archives of Saskatchewan (Provincial Archives) in its "Guidelines for the Management of Transitory Records" states as follows:

> **Transitory records** are records of temporary usefulness that are needed only for a limited period of time, to complete a routine task or prepare an ongoing document. Also, exact copies of official records made for convenience of reference.
>
> …
> **TR20 Convenience/Duplicate Copies**
> Exact copies of an official record where nothing has been added, changed or deleted, the copies have been produced only for convenience of reference and the official record has been filed in the institution's classification and retention system.
>
> Includes: photocopies of paper documents, extra electronic copies of electronic documents, reading or circulation copies, duplicates of microfilm, CDs or DVDs, obsolete stationary, blank copies of forms, etc.
>
> …
> **Retention**
> Destroy when no longer required.
>
> [Emphasis in original]

[67] The Provincial Archives states that the instruction is to delete duplicate copies of records when they are no longer required. The Provincial Archives also states that institutions (or in this case trustees) should have policies that outline how to properly manage and destroy

such records. In its *Imaging and Source Records Disposal Guidelines*, the Provincial Archives add, in part, as follows:

> **Disposal of Source Records**
>
> - The institution will prepare an inventory of the source records which are to be disposed of, including the business unit to which they belong, title/description of records, inclusive dates, location, box numbers and identification of business unit responsible for the official records.
>
> - The individual assigned the responsibility for approving disposal of source records will review the inventory, verify that the source records have been imaged/microfilmed and ensure that the records are not subject to FOI access requests or litigation. Once this is done, the individual will authorize the destruction of the source records in writing.
>
> - The records will be destroyed in a manner that ensures they cannot be reconstructed. Any containing confidential, sensitive or restricted information (e.g. personal health information, etc.) should be destroyed in a secure environment with limited access.
>
> - If records are destroyed by the institution, their destruction must be witnessed and signed off by two staff members.
>
> - If records are destroyed off-site, confirmation of the destruction must be received in writing.
>
> …

[68] Based on the above, the CMPA, CPSS and Provincial Archives all agree that a paper record can be destroyed once it is scanned or digitized and uploaded to a repository where the scanned copy will effectively become the official record. This is after, as HIPA states pursuant to subsection 17(2)(a), the trustee has established that the scanned or digitized copy of the record of personal health information is "retrievable, readable and useable" for the purpose for which it was collected. None of these bodies outlines a particular retention period, nor does HIPA nor the HIPA Regulations, so it appears that once a scanned record has been verified that it is retrievable, readable and useable, then the paper record can be destroyed without any particular period of retention.

[69] A trustee should outline in their policies and procedures, how they will verify that a scanned record is retrievable, readable and useable, and how the source record (paper copy) was destroyed. A trustee should also have a verification document to this effect. As far as best practices, the following would align with what the Provincial Archives suggests should occur when scanning a record of personal health information into an EMR and then disposing of the original or source record:

1. Include a title or description of the record;
2. Include the name of the name of the individual reviewing/disposing the record. Also include their confirmation that they have reviewed the source (paper) record against the scanned copy and have determined it is retrievable, readable and useable;
3. Include the individual's authorization (e.g., their signature) for the destruction of the original or source (paper) record; and
4. Include a notation on how the paper record was destroyed (or by what method), on what date it was destroyed, and that the destruction was witnessed and by whom.

[70] As noted, Dr. Odenigbo and Dr. Ezeasor do outline in their policies/procedures that a scanned record needs to be reviewed for accuracy and integrity, and that this has been documented. Their policy and procedures, however, could be a bit more explicit in this regard and include what needs to be documented. When a breach occurs, such a practice can help account for a situation such as in this matter where the source (paper) records were breached.

c. In-office recycling bins

[71] As noted, the identified resources offer no guidance on whether an original or source (paper) record has been scanned needs to be retained for any length of time. Rather, it appears that the original or source (paper) record can be destroyed at any time after the verification process. Dr. Odenigbo and Dr. Ezeasor state they now have in-office shredders to immediately shred in most instances, but also do use open blue shredding bins (the type that would fit under a desk) to store paper records that are awaiting shredding. They state that each doctor has one of these bins under his desk, and that one is located behind the front reception desk. They add that patients are escorted into each doctor's office, and so

the bins are inaccessible to patients. As far as the contractor inadvertently accessing any patient records, they stated they keep records in a "dedicated locked confidential drawer" at the end of each day.

[72] In this matter, what contributed to the breach was the fact that the contractor's employee had ready access to the patient records. Even if they were unaware that these records should not be touched, it appears that the contractor would have still had regular access. If the Clinic had locked bins as a form of physical safeguard from the start, it is likely that the privacy breach would have never occurred. An open bin containing personal health information, regardless of where it is located, would not comply with subsection 17(1)(a) of HIPA, or subsection 6(b) of the HIPA Regulations, which states as follows:

> **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:
>
> …
> (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

[73] Not keeping the paper records in locked recycling bins in the first place contributed to the privacy breach that occurred. Regardless of the changes they have implemented, because Dr. Odenigbo and Dr. Ezeasor continue to use open recycling bins in their offices and behind the front desk, there is still risk of unintended access. This includes by staff who are not designated to manage the paper records.

d. Conclusion

[74] Based on the information before me, I find that Dr. Odenigbo and Dr. Ezeasor did not adequately identify the root cause of the privacy breach, and that the root cause of the privacy breach was a lack of sufficient administrative and physical safeguards pursuant to sections 16 and 17 of HIPA and sections 5 and 6 of the HIPA Regulations.

[75] I will make recommendations to address this in the next part of this Investigation Report.

Prevent future breaches

[76] The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring. Essentially, this is what steps can be taken to prevent a similar privacy breach from occurring. To assist, some questions trustees can ask are:

- Can your organization create or make changes to policies and procedures relevant to this privacy breach?
- Are additional safeguards needed?
- Is additional training needed?
- Should a practice be stopped?

(*Privacy Breach Guidelines for Trustees*, p. 6)

[77] Dr. Odenigbo and Dr. Ezeasor state they have made several changes to their practices because of the breach, including:

- They have placed shredders in each examining room so that paper records can be shredded immediately. If any paper records are left at the end of the day, then they are placed in a locked drawer pending shredding. Until then, these records may be kept in one of the open blue recycling bins.
- They have also designated one staff member to be responsible for shredding, rather than multiple staff. Because they lock records intended for shredding at the end of each day, they have also minimized the risk that the contractor may witness any personal health information. I note, however, that their policy on destruction, does not mention witness shredding, which simply means having a second person witness any confidential shredding process.

[78] While Dr. Odenigbo and Dr. Ezeasor have taken some steps to address the privacy breach that occurred, I recommend that they take a additional steps to help them meet their obligations pursuant to sections 16 and 17 of HIPA, and sections 5 and 6 of the HIPA Regulations.

Administrative safeguards

[79] I recommend that Dr. Odenigbo and Dr. Ezeasor ensure that they sign a confidentiality agreement with each contractor and whoever the contractor may employ, and that as trustees, Dr. Odenigbo an Dr. Ezeasor ensure whoever is responsible for the Clinic's privacy is training those individuals. This should be captured in the Clinic's policies and procedures.

[80] I recommend that Dr. Odenigbo and Dr. Ezeasor implement a verification document when scanning a source (paper) record and uploading it to their EMR and update their "Privacy Policy Document" accordingly. The verification document should include:

1. a title or description of the record;
2. the name of the individual reviewing/disposing of the record. Also include their confirmation that they have reviewed the source (paper) record against the scanned copy and have determined it is retrievable, readable and useable;
3. the individual's authorization (e.g., their signature) for the destruction of the original or source (paper) record; and
4. a notation on how the paper record was destroyed (or by what method), on what date it was destroyed, and that the destruction was witnessed and by whom.

Physical safeguards

[81] I recommend Dr. Odenigbo and Dr. Ezeasor replace the open recycling bins in their offices and behind the front desk with ones that have a lockable cover, or that they keep paper records awaiting destruction in a locked drawer or cabinet.

III FINDINGS

[82] I find that as HIPA is engaged, I have jurisdiction to conduct this investigation.

[83] I find that a privacy breach occurred.

[84] I find that Dr. Odenigbo and Dr. Ezeasor did not take adequate steps to ensure the breach was fully contained.

[85] I find that Dr. Odenigbo's and Dr. Ezeasor's notice letters should have included what exact data elements were involved for each affected individual and the type of risk associated with those data elements, and that they should have also included a one-year offer of credit monitoring.

[86] I find that Dr. Odenigbo and Dr. Ezeasor did not adequately identify the root cause of the privacy breach, and that the root cause of the privacy breach was a lack of sufficient administrative and physical safeguards pursuant to sections 16 and 17 of HIPA and sections 5 and 6 of the HIPA Regulations.

IV RECOMMENDATIONS

[87] I recommend that within 30 days of the issuance of this Investigation Report that Dr. Odenigbo and Dr. Ezeasor update their policies and procedures to ensure that privacy breach notice templates include the specific types of data elements involved and what the associated risks may be.

[88] I recommend that within 30 days of the issuance of this Investigation Report, that Dr. Odenigbo and Dr. Ezeasor also offer affected individuals one year of credit monitoring.

[89] I recommend that Dr. Odenigbo and Dr. Ezeasor ensure that they sign a confidentiality agreement with each contractor and whoever the contractor may employ, and that as trustees, Dr. Odenigbo an Dr. Ezeasor ensure whoever is responsible for the Clinic's privacy completes the training for those individuals. This should be captured in the Clinic's policies and procedures.

[90] I recommend that within 30 days of issuance of this Investigation Report, Dr. Odenigbo and Dr. Ezeasor implement a verification document when scanning a source (paper) record

and uploading it to their EMR and update their "Privacy Policy Document" accordingly. The verification document should include:

1. a title or description of the record;

2. the name of the individual reviewing/disposing of the record. Also include their confirmation that they have reviewed the source (paper) record against the scanned copy and have determined it is retrievable, readable and useable;

3. the individual's authorization (e.g., their signature) for the destruction of the original or source (paper) record; and

4. a notation on how the paper record was destroyed (or by what method), on what date it was destroyed, and that the destruction was witnessed and by whom.

[91] I recommend Dr. Odenigbo and Dr. Ezeasor immediately replace the open recycling bins in their offices and behind the front desk with ones that have a lockable cover, or that they keep paper records awaiting destruction in a locked drawer or cabinet.

Dated at Regina, in the Province of Saskatchewan, this 26th day of March, 2025.

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