Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 158-2022

Métis Addictions Council of Saskatchewan Inc.

March 15, 2023

Summary: On August 5, 2022, the Commissioner's office responded to a report of client records being left in a recycling bin in Regina that appeared to be associated with the Métis Addictions Council of Saskatchewan Inc (MACSI). The Commissioner found he had jurisdiction to conduct an investigation and concluded that a privacy breach occurred. The Commissioner also found that MACSI did not take all the steps it could have to contain the privacy breach and did not make enough effort to notify the affected individuals. The Commissioner recommended MACSI post notification of this privacy breach in areas of its office and on its website that are accessible to its clients. The Commissioner found MACSI conducted an adequate investigation into this privacy breach. In addition, he found that MACSI has not taken adequate steps to prevent future breaches. In order to satisfy risk mitigation efforts, the Commissioner recommended MACSI implement a clean desk policy for all employees. Further, the Commissioner recommended MACSI develop a record retention and disposition schedule that clearly outlines the requirements and expectations of employees for records retention and disposal. Finally, the Commissioner recommended that in addition to personal shredders, MACSI continues to have a secure shredding bin in its office that requires an employee to witness the shredding of materials.

I BACKGROUND

[1] On August 5, 2022, my office was contacted by a member of the media advising that someone brought files to their office that came from a recycling bin in the Douglas Park area of Regina. They further advised the files appeared to be patient drug addiction files and looked to be associated with the Métis Addictions Council of Saskatchewan Inc (MACSI).

[2] That same day, my office attended the recycling bin where the files were found. Upon inspecting the contents of the recycling bin, my office recovered what amounted to a large envelope of papers. Upon initial investigation, some pages consisted of blank pages or blank forms, but others contained identifiable information.

[3] In total, 174 pages were recovered from the recycling bin. These include pages recovered by a private citizen and sent to the media, and the pages found in the recycling bin by my office.

[4] On August 11, 2022, my office spoke with the lawyer representing MACSI, who advised they are representing MACSI and the Métis Nation – Saskatchewan (MN–S). The lawyer also advised that MACSI and MN-S are affiliated. The lawyer advised my office that MACSI may be a trustee (of personal health information pursuant to *The Health Information Protection Act* [HIPA]) as it has a contractual agreement with the Ministry of Health (Health) to provide health services.

[5] On September 7, 2022, the lawyer provided my office with a copy of the signed agreement. As that agreement had expired, on September 14, 2022, my office received an amended agreement that expired December 31, 2022. Once my office commenced its analysis, it requested the current agreement between MACSI and Health. The lawyer provided my office with an agreement that is valid to March 31, 2023.

[6] By email on September 14, 2022, my office notified the lawyer representing MACSI that my office would be undertaking an investigation into this matter. On November 2, 2022, the lawyer provided my office with its response to the notice of this investigation.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[7] 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 a trustee.

[8] Subsection 2(m) of HIPA defines "personal health information" as follows:

> **2**(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;

[9] From the investigation details provided to my office, MACSI advised that there were approximately 39 affected individuals and that the disposed information included the following types of data elements: names, contact information, treatment information, referral information, location, gender, health card numbers, dates of birth, legal information, employment information and partially redacted credit card information.

[10] This information was collected for the purpose of providing addiction services to the 39 individuals. Therefore, it qualifies as personal health information pursuant to subsection 2(m) of HIPA.

[11] I will now consider if there is a trustee.

[12] As noted in the background of this Report, MACSI provided my office with a copy of a service delivery agreement between MACSI and Health that is valid to March 31, 2023. This agreement outlines that MACSI is providing "…the delivery of alcohol and drug treatment services through the Regina Centre, Saskatoon Centre and Prince Albert Centre…"

[13] Subsection 2(t) of HIPA provides the definition of a "trustee". Specifically, subsections 2(t)(i) and (xiv) provide:

> **2**(t) **"trustee"** means any of the following that have custody or control of personal health information:
>
> (i) a government institution;
>
> …
> (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;

[14] Health qualifies as a trustee pursuant to subsection 2(t)(i) of HIPA. As outlined above, Health has entered into an agreement with MACSI to deliver addiction services on behalf of Health. Further, the agreement specifically states:

> 11.3 The parties [MACSI and Health] acknowledge that for the purposes of providing the services pursuant to this agreement, [MACSI] may be required to collect and use personal health information from its clients. [MACSI] specifically acknowledges that it is a *"trustee"* within the meaning of [HIPA] and as such agrees to comply with that Act in the course of providing the services.

[15] Therefore, as MACSI has entered into an agreement with Health to provide services on its behalf, it also qualifies as a trustee pursuant to subsection 2(t)(xiv) of HIPA.

[16] Finally, I must determine if MACSI has custody or control of the records. "Custody" is the physical possession of a record by a trustee with a measure of control. "Control" means having authority over a record. A record is under a trustee's control when the trustee has the authority to manage the record, including its disposal.

[17] The agreement states the following:

> 11.4 The Ministry acknowledges that personal health information in the custody and control of [MACSI] may only be disclosed to the Ministry in accordance with the provisions of [HIPA]. For greater certainty, the Ministry and [MACSI] agree to the use and disclosure of personal health information for the purposes of planning, delivering, evaluating or monitoring the services of the Agency.
>
> 11.5 Upon the expiration or termination of this Agreement, the duties imposed on [MACSI] as trustee with respect to personal health information in its custody or control continue to apply until [MACSI] transfers custody and control of the personal health information to either of the following at the direction of the Ministry:
>
> (a) another trustee; or
>
> (b) an information management service provider that is a designated archive within the meaning of [HIPA].

[18] Based upon the wording of the agreement, MACSI has been established as having custody and control of the personal health information.

[19] Therefore, as all three elements are present, I find I have jurisdiction to conduct this investigation.

[20] A privacy breach occurs when there is an unauthorized collection, use and/or disclosure of personal health information or if HIPA does not authorize the collection, use and/or disclosure. As the personal health information in question was found unattended in a recycling bin, it was an unauthorized disclosure. MACSI does not dispute this. As such, I find that a privacy breach occurred.

[21] I will now assess how MACSI managed the privacy breach.

2. Did MACSI properly manage the privacy breach?

[22] As set out in my office's *Rules of Procedures*, when my office determines there has been a privacy breach, my office will analyze whether the trustee appropriately managed the breach by considering if it:

- Contained the breach (as soon as possible);

- Notified affected individuals (as soon as possible);
- Investigated the breach; and
- Taken appropriate steps to prevent future breaches.

[23] I will consider each step separately and make any necessary recommendations at the end of this Investigation Report.

Contained the breach (as soon as possible)

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

- Stopping the unauthorized practice.
- Recovering the records.
- Shutting down the system that was breached.
- Revoking access to personal health information.
- Correcting weaknesses in physical security.

(*Privacy Breach Guidelines for Trustees* [*Privacy Breach Guidelines*] at page 3)

[25] As noted above, my office was informed of the privacy breach on August 5, 2022 by a member of the media. My office attended the recycling bin that same day and upon searching, retrieved what amounted to a large envelope of papers. In its investigation details, MACSI advised my office that its staff searched the recycling bin the following week, and did not find any additional documents.

[26] As noted above, 174 pages were recovered from the recycling bin. These include pages recovered by a private citizen and sent to the media, and the pages found in the recycling bin by my office. However, not all of these pages contained personal health information. I will discuss this later in this Investigation Report.

[27] As stated in my office's Investigation Report 154-2022 at paragraph [27]:

> As part of analyzing containment, I want to be able to conclude the trustee took reasonable steps to contain the breach. I want to have some reassurance the trustee has reduced the magnitude of the breach and the risk to individuals. In this matter, I am not considering the records my office seized and returned to Dr. Malhotra on November 30, 2022. Rather, I am looking at what may have occurred to some records after Dr. Malhotra's staff dumped them. In so doing, I am considering different factors, including how Dr. Malhotra disposed of the records, the timeline of what occurred, and Dr. Malhotra's efforts to contain the records. I need to consider these against what happens to recycling that goes for further processing after it passes through the PA facility. As I previously stated in this Investigation Report, from the PA facility, materials go on to be further processed into recycled paper products.

[28] I will take the same factors under consideration in this matter.

a. How MACSI Disposed of the Records

[29] In interview investigation details provided to my office from MACSI, sometime after lunch on August 4, 2022, an employee took the recycling materials to bins located in the Douglas Park area of Regina. The employee also advised that they do not check in the office to determine if there are materials that require shredding in the recycling bins.

[30] I am also mindful that a private citizen initially found records and provided them to the media. My office is appreciative that the media contacted my office and provided my staff the papers. Although I would hope the private citizen and media would not disseminate any of what was found, I have no proof that they have not.

[31] Further, in my office's Investigation Report 154-2022, it was stated in part at paragraph [31], "loosely dumped records, though, are much harder to contain, particularly when they are dumped with a huge mass of recycling…." This is the same issue in this matter. The records were dumped in an unsecured recycling bin and anyone who came to the bin would have the ability to view or even take the MACSI records. From the time the records were dumped in the recycling bin to the time of recovery, MACSI lost total control of the records including who could have potentially viewed or taken them from the bin.

b. Lapsed time

[32] The media advised my office of the materials in the recycling bins on August 5, 2022 – one day after the employee advised they took the materials to the recycling bins at Douglas Park.

[33] My office searched the recycling bins in the afternoon of August 5, 2022, and retrieved what amounted to a large envelope of papers.

[34] MACSI learned of the privacy breach on August 5, 2022. However, MACSI staff did not search the recycling bin until the following week and did not recover additional records. This is of concern as MACSI should have searched the recycling bin immediately upon learning of the breach.

[35] By waiting until the following week to search the recycling bins, any additional materials in the recycling bin were not secure and remained in a state where they could be viewed or taken by others. They may have also gone on for further recycling where the breach would have continued.

c. MACSI Efforts to Contain

[36] Through investigation details provided to my office, MACSI learned of this matter on Friday, August 5, 2022 when my office contacted them. It also appears that the only step MACSI took to contain the breach was to search the recycling bin.

[37] In addition, MACSI should have made attempts to learn if the recycling bin had been emptied between the time MACSI disposed of the records and then went to search the bin. MACSI could have also attempted to find out who initially found the records and if they were aware request that they destroy anything they had and not further disseminate the information. MACSI could have contacted the facility that picks up the recycling to determine if or where any records could have gone for further processing. Taking such

steps can help a trustee better understand how far a breach may have spread, and also help with containment efforts.

[38] Although my office conducted a thorough search of the recycling bin, given the above factors, I cannot be certain if all possible records have been recovered. As such, I find MACSI did not take all the steps it could have to contain the privacy breach.

Notified affected individuals (as soon as possible)

[39] Notice to affected individuals should happen as soon as possible when learning of a breach. Notifying an individual that their personal health information has been inappropriately accessed or disclosed is important for a number of reasons. Not only do individuals have a right to know, but they need to know in order to protect themselves from potential harm that may result from the inappropriate disclosure. Unless there are compelling reasons not to, trustees should always provide notification.

[40] My office's *Privacy Breach Guidelines* suggests the following elements be included in notification to affected individuals:

- a description of the breach (a general description of what happened);
- a detailed description of the personal information involved (e.g. name, credit card numbers, medical records, financial information, etc.);
- a description of possible types of harm that may come to them as a result of the privacy breach;
- steps taken and planned to mitigate the harm and to prevent future breaches;
- if necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g. how to contact credit reporting agencies, how to change a health services number or driver's license number etc.);
- contact information of an individual within your organization who can answer questions and provide further information;
- a notice that individuals have a right to complain to the IPC (provide contact information); and

- recognition of the impacts of the breach on affected individuals and, an apology.

[41] In its investigation details, MACSI advised it identified 39 affected individuals in this matter. It also advised that the breached information varies by individual, but includes information such as names, contact information, treatment information, referral information, employment information and partially redacted credit card information.

[42] In its investigation details provided to my office, MACSI advised that, "… most of the impacted individuals are highly vulnerable and many do not have current address or contact information so it is very difficult to securely contact them to notify them about the Incident." Through the course of this investigation, my office followed up with the lawyer representing MACSI in regard to notification efforts. By email on February 14, 2023, the lawyer advised my office, in part:

> …the clients are very vulnerable and do not have current contact information – e.g. homeless or transient. As such, not only is there a concern of unknown current contact information but there is also a concern in potential for breaching the confidentiality and privacy of the individuals if the previous information is used to try to notify the individuals.

[43] Therefore, MACSI has not notified the 39 affected individuals of this incident.

[44] I agree that there may be some risk with notifying the specific individuals affected by this matter given it is likely MACSI would not have current contact information of the individuals. However, MACSI should take steps to inform clients of this breach. MACSI could post notices of the incident in its office, including who an individual could speak to if they are concerned their personal health information may have been involved in this matter.

[45] Based on the preceding, I find MACSI did not make enough effort to provide notification to affected individuals. I recommend that MACSI post notification of this privacy breach on its website and in areas of its office that is accessible to its clients.

Investigate the breach

[46] Investigating the privacy breach to identify the root cause is key to understanding what happened. Identifying the root cause will help prevent similar breaches in the future. The internal investigation should also consider whether the safeguards that were in place at the time of the incident were adequate.

[47] MACSI has advised my office that the root cause of this privacy breach was due to human error of not properly disposing of old client files. It appears that the recovered information was that of an employee who had placed papers on top of their shredder that jammed with paper at the time, and therefore, placed the materials on top of the shredder. They had planned to unjam the shredder later and continue to shred the materials. However, MACSI was not able to conclude how the materials went from being placed on top of the shredder to ending up in the recycling bin.

[48] Section 16 of HIPA requires a trustee to establish administrative, technical and physical safeguards to protect personal health information 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.

[49] Subsection 17(2)(b) of HIPA requires that a trustee securely destroy personal health information as follows:

> **17**(2) A trustee must ensure that:
>
> …
> (b) personal health information is destroyed in a manner that protects the privacy of the subject individual.

[50] As outlined in my office's *Privacy Breach Guidelines*, *administrative safeguards* are controls that focus on internal organization policies, procedures, and maintenance of security measures that protect personal health information. *Physical safeguards* are physical measures, policies, and procedures to protect personal information and related buildings and equipment from unauthorized intrusion and natural and environmental hazards. Examples include locked filing cabinets, offices and storage rooms, alarm systems, and clean desk approaches.

[51] It appears that MACSI had administrative safeguards in place, such as policies on how to detail with confidential client information, including its disposition. It also appears those policies were not fully being followed by employees. In addition, some of its physical safeguards were inadequate. This includes shredders that did not work, locks that could be bypassed and no security cameras.

[52] Staff that work with client files are responsible to ensure that confidential materials and those containing personal health information are disposed of in a secure manner. It is the responsibility of the employer to ensure the employees receive proper training regarding their obligations to meet the requirements of HIPA. In my office's Investigation Report H-2011-001, it was stated, in part, at paragraph [92] and [93]:

> [92] … I suggest that, in considering the reasonably 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) …
>
> (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 [personal health information] without the consent of the patients.

[53] The root cause, then, was a failure of staff who work with MACSI clients to follow administrative safeguards and a lack of physical safeguards. While MACSI had in place policies and procedures for managing and safeguarding client personal health information, it failed to follow them and so did not fully meet its obligations pursuant to section 16 and subsection 17(2)(b) of HIPA. As a result of this incident, MACSI has taken steps to rectify these issues, which I will discuss in the next part of this investigation report.

[54] I find MACSI conducted an adequate investigation into this privacy breach.

Prevent future breaches

[55] In responding to a breach of privacy, it is important that a trustee take steps to mitigate the risk of a similar breach occurring in the future. The following are some steps that can be taken:

- 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?

[56] In its investigation details provided to my office, MACSI advised the following:

MACSI has put into place additional measures to strengthen safeguards and to prevent similar incidents in the future including, for example:

- changing all doorknob locks in the building to deadbolt locks;
- changing all keys;
- implementing new procedures, including reviewing logbook activities daily and locking all doors nightly;
- installing three new security cameras;
- relocating photocopier and fax machines to a more secure location; and
- replacing old non-functioning shredders.

In addition to the above, MACSI has and will continue to provide all employees with refresher training and at least annual training reminders thereafter relating to the importance of confidentiality and privacy as well as processes for the proper disposal of confidential documents.

[57] Through the course of this investigation, MACSI also advised it has implemented secure shredding bins, centralized filing systems and secure online sharing of documents.

[58] These are good steps to mitigate the risk of this type of breach occurring in the future. However, there are a few more steps I recommend MACSI take within 30 days of issuance of this Investigation Report, including:

- If it does not already have one in place, implement a clean desk policy for all employees. Meaning that employees are required to lock any client files in their desk drawers or filing cabinets when the files are not in use, including at the end of the workday, and if the employee is not in the office.

- If it does not already have one in place, develop a record retention and disposition schedule that clearly outlines the requirements and expectations of employees for records retention and disposal.

- Provide employees with personal shredders and ensure it continues to have a secure shredding bin that requires an employee to witnesses the shredding of materials. If they are not already utilizing this service, MACSI may also consider mobile shredding trucks that will come to a place of business and shred materials onsite; such services are available in Regina.

[59] Therefore, while MACSI has taken some steps to prevent future breaches, I find it could do more. I recommend MACSI implement the additional risk mitigation steps I have outlined in the preceding paragraph.

III FINDINGS

[60] I find I have jurisdiction to conduct this investigation.

[61] I find that a privacy breach occurred.

[62] I find MACSI did not take all the steps it could have to contain the privacy breach.

[63] I find MACSI did not make enough effort to provide notification to the affected individuals.

[64] I find MACSI conducted an adequate investigation into this privacy breach.

[65] I find MACSI has not taken all possible steps to prevent future breaches.

IV RECOMMENDATIONS

[66] I recommend within 30 days, that MACSI post notification of this privacy breach in areas of its office and on its website that is accessible to its clients.

[67] I recommend within 30 days, MACSI implement a clean desk policy for all employees.

[68] I recommend within 30 days, MACSI develop a record retention and disposition schedule that clearly outlines the requirements and expectations of employees for records retention and disposal.

[69] I recommend within 30 days, MACSI provide employees with personal shredders and ensure it continues to have a secure shredding bin that requires an employee to witness shredding of materials.

Dated at Regina, in the Province of Saskatchewan, this 15th day of March, 2023.

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