Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 313-2025[1]

Ministry of Health

-and-

ARCAS Group Inc

May 1, 2026

Summary: The Ministry of Health (Health) proactively notified the Office of the Saskatchewan Information and Privacy Commissioner (OIPC) of a privacy breach that occurred on November 6, 2025. The privacy breach occurred when the personal health information of 224 individuals was accidentally sent to 167 unintended recipients during the mailout of the No Tax Return (NTR) letters for the Special Support Program administered by the Drug Plan and Extended Benefits Branch (DPEBB) of Health. These NTR letters were processed and mailed out by a third-party company, ARCAS Group Inc (ARCAS).

The Commissioner found that:

(1) ARCAS meets the definition of an information management service provider (IMSP) pursuant to *The Health Information Protection Act (HIPA);*

(2) a privacy breach occurred when an ARCAS employee failed to follow proper administrative safeguards which resulted in the personal health information of 224 affected individuals being mailed to 167 unintended recipients in contravention of *HIPA*;

(3) Health did not make adequate containment efforts in relation to the privacy breach;

[1] The other OIPC file number associated with this matter is 028-2026.

(4) Health notified the affected individuals appropriately and in a timely manner with respect to this matter;

(5) both Health and ARCAS conducted a fulsome investigation regarding this privacy breach;

(6) the root cause of this privacy breach was a senior employee of ARCAS who failed to follow proper administrative safeguards during the printing and mailout process;

(7) ARCAS had appropriate and reasonable safeguards in place to prevent this privacy breach had they been followed;

(8) ARCAS took reasonable steps to prevent similar privacy breaches from happening in the future including addressing the employee and requiring retraining; and

(9) Health did not have a formal written agreement in place with ARCAS as legislated by *HIPA*.

The Commissioner recommended that:

(1) Health make additional efforts to contact the outstanding 140 unintended recipients in an effort to fully contain this privacy breach; and

(2) Health engage ARCAS in a written formal contract as required by section 18(2) (a trustee must enter into a written agreement with the information management service provider) of *HIPA* and detailed in section 7 (agreement with information management service provider) of *The Health Information Protection Regulations, 2023*. This agreement should be completed and put in place within 90 days of the issuance of this Investigation Report. Health should provide OIPC with a copy of this agreement.

I BACKGROUND

[1] On November 26, 2025, the Ministry of Health (Health) contacted the Office of the Saskatchewan Information and Privacy Commissioner (OIPC) to proactively report a privacy breach.

[2] Health indicated that the breach occurred on November 6, 2025, when 224 affected individuals' No Tax Return (NTR) letters for the Special Support Program administered

by the Drug Plan and Extended Benefits Branch (DPEBB) of Health were mailed out to 167 unintended recipients.

[3] NTR letters are sent annually by DPEBB to advise clients that their Special Support coverage cannot be automatically renewed, and that updated Income Tax information is required. The letters were printed, stuffed, sealed and posted by a third-party company, ARCAS Group Inc (ARCAS).

[4] ARCAS is a Regina-based company that provides daily mailing services for multiple government ministries and private sector clients. ARCAS has performed mailings of a similar nature for Health for more than 10 years.

[5] On January 12, 2026, Health provided OIPC with a completed *Privacy Breach Investigation Questionnaire* and supporting documentation.

[6] On January 29, 2026, OIPC notified Health that an investigation would be commenced with respect to the privacy breach. A second investigation file was opened to allow ARCAS to make representations on the matter.

[7] ARCAS provided OIPC with a completed *Privacy Breach Investigation Questionnaire* and supporting documents on February 24, 2026.

II DISCUSSION OF THE ISSUES

1. Jurisdiction

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

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

i. First element – trustees

[9] Health qualifies as a trustee as defined by section 2(1)(t)(i) of *HIPA*:

> **2**(1) In this Act:
>
> ...
> (t) "**trustee**" means, any of the following that have custody or control of personal health information:
>
> (i) a government institution;

There is no dispute that Health is a government institution for the purposes of this Investigation Report.

ii. Second element – personal health information

[10] The NTR letters sent out in error contained the affected individuals' first and last names, addresses and Health Services Numbers (HSN). This office has found that this type of basic demographic information, coupled with the HSN, constitutes registration information under *HIPA*. This information also qualifies as personal health information. [3] Section 2(1)(m)(v) of *HIPA* provides as follows:

> **2**(1) In this Act:
>
> ...
> (m) "**personal health information**" means, with respect to an individual, whether living or deceased:
>
> …
> (v) registration information;

[11] Section 2(1)(q) of *HIPA* defines "registration information" as follows:

> **2(**1) In this Act:
>
> …

[3] OIPC Investigation Report 034-2025 at paragraph [11].

> (q) **"registration information"** means information about an individual that is collected for the purpose of registering the individual for the provision of health services, and includes the individual's health services number and any other number assigned to the individual as part of a system of unique identifying numbers that is prescribed in the regulations;

[12] Based on the above, personal health information was involved in this privacy breach.

iii. Third element - Trustee Custody and/or Control of Personal Health Information

[13] "Custody" is the physical possession of a record by a trustee combined with a measure of control. "Control" implies authority. Personal health information is under the control of a trustee when the trustee has 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.[4]

[14] Health provided the personal health information of its clients to ARCAS via a secured server. ARCAS used the information provided by Health to populate the NTR letters. Health had custody over the personal health information because it originated from its own databases. Health also managed and shared the personal health information of its clients with ARCAS for the purposes of processing and distributing the NTR letters.

[15] As Health ultimately retained the authority to manage the personal health information of its clients, OIPC concludes that Health had both custody and control over the personal health information in this matter.

[16] The three requisite elements are present for the engagement of *HIPA* in this matter such that this office has jurisdiction to undertake this investigation under the authority as afforded by *HIPA*.

[4] OIPC Investigation Report 166-2025 at paragraph [22].

2. ARCAS is an IMSP under *HIPA*

[17] Section 2(1)(j) of *HIPA* defines "information management service provider" as follows:

> **2**(1) In this Act:
>
> …
> (j) **"information management service provider"** means a person who or body that processes, stores, archives or destroys records of a trustee containing personal health information or that provides information management or information technology services to a trustee with respect to records of the trustee containing personal health information, and includes a trustee that carries out any of those activities on behalf of another trustee, but does not include a trustee that carries out any of those activities on its own behalf;

[18] At the material time, Health was engaged contractually with ARCAS to complete various printing and mailing services on its behalf which included the printing, stuffing, sealing, and mailing of the NTR letters involved in this matter[5]. This office has established an organization that processes personal health information through the mail at the request and behalf of Health, functions as an information management service provider (IMSP) under *HIPA*.[6]

[19] Section 18 of *HIPA* details the expectations on both trustees and IMSPs regarding personal health information:

> **18**(1) A trustee may provide personal health information to an information management service provider:
>
> (a) for the purpose of having the information management service provider process, store, archive or destroy the personal health information for the trustee;

[5] Health provided this office with a copy of the four-year contract (April 4, 2023 – April 3, 2027) between itself and ARCAS, which detailed the scope of professional direct mailing services required by Health and to be delivered by ARCAS.

[6] OIPC Investigation Report H-2007-001 at paragraph [36].

> (b) to enable the information management service provider to provide the trustee with information management or information technology services;
>
> …
> (d) for the purpose of combining records containing personal health information.
>
> (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.
>
> (3) An information management service provider shall not use, disclose, obtain access to, process, store, archive, modify or destroy personal health information received from a trustee except for the purposes set out in subsection (1).
>
> (4) An information management service provider must comply with the terms of the agreement entered into pursuant to subsection (2).
>
> [Emphasis added]

[20] Based on the definition above and the services provided to Health during the material time, ARCAS clearly met the definition of an IMSP under *HIPA*.

[21] Section 18(2) of *HIPA* explicitly requires that all trustees have a written agreement with the contractual IMSP. Although the explicit requirement for a written agreement is a more recent development,[7] this office has recommended since 2003 that trustees enter into formal written agreements with IMSPs to ensure that all obligations under *HIPA* are met.[8]

[7] OC 376/2023 - Amending Order - Proclaim Subsections 17(1), 18(2) and 18(4) of *The Health Information Protection Act* on Tuesday, August 1, 2023.

[8] *Supra* footnote 6 at paragraph [83].

[22] In the course of this investigation, Health conceded that it has no formal contract with ARCAS as legislated by *HIPA*.

3. A Privacy Breach Occurred

[23] A privacy breach occurs when personal health information is collected, used and/or disclosed without authority under *HIPA*. As noted previously, the personal health information of 224 affected individuals contained in the NTR letters was sent to 167 unintended recipients. This type of access constitutes "disclosure" under *HIPA*.

[24] *HIPA* does not directly define the term "disclosure." However, OIPC has defined "disclosure" as the sharing of personal health information with a separate entity, not a division or branch of the trustee in custody or control of that information.[9]

[25] Section 27(1) of *HIPA* outlines the restrictions on disclosing personal health information:

> **27**(1) A trustee shall not disclose personal health information in the custody or control of the trustee except with the consent of the subject individual or in accordance with this section, section 28 or section 29**.**

[26] In this matter, both Health and ARCAS agreed that an unauthorized disclosure occurred when the NTR letters were mailed to the wrong individuals. Further, it is evident an unauthorized disclosure occurred as none of the affected individuals had provided consent for the public disclosure of their personal health information. Therefore, a privacy breach has occurred.

4. The Response to the Privacy Breach

[27] Once a privacy breach has occurred, several factors are relevant in the analysis of a trustee response to the breach:[10]

[9] OIPC Investigation Report 097-225 at paragraph [30].

[10] *Supra,* footnote 4 at paragraph [60].

a. Was the breach contained;

b. Were affected individuals notified;

c. Was the breach investigated;

d. Were appropriate steps taken to prevent future breaches.

a. Containment of the Breach

[28] Upon learning that a privacy breach has occurred, a trustee should immediately take steps to contain the breach. These steps will depend on the nature of the breach, but they can include:[11]

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

[29] OIPC applies a standard of reasonableness to assess the containment of a breach. A privacy breach is a very serious matter, and the trustee must demonstrate that it has reduced the magnitude of the breach and the resulting risk to affected individuals in order to reassure the public as well as the clients it serves.[12]

[30] Health initially became aware of the breach on November 14, 2025, when an individual called DPEBB to report that they had mistakenly received someone else's NTR letter along with their own letter in the mail. DPEBB received a second report of a similar nature on November 17, 2025.

[11] *Ibid,* at paragraph [61].

[12] OIPC Investigation Report 253-2025 at paragraph [23].

[31] After receiving the second report on November 17, 2025, Health emailed ARCAS to indicate that a breach had occurred. Health demanded that all Health mailings be put on hold until the breach was fully investigated and resolved.

[32] By November 24, 2025, Health had received an additional three breach reports from other individuals. One report indicated that an individual had received a double-sided NTR letter with their own information on the front of the page and another individual's information on the back. Health promptly communicated this to ARCAS on the same date.

[33] ARCAS performed an audit of its printing data and determined that NTR letters containing the personal health information of 224 affected individuals had been inadvertently sent to 167 unintended recipients.

[34] Between November 28 and December 1, 2025, Health wrote the 167 unintended recipients and requested the return of the NTR letters received in error.

[35] In response to this request Health received:

- 17 NTR letters "returned to sender" due to incorrect mailing address;
- four NTR letters mailed back to Health by unintended recipients; and
- confirmation from another five unintended recipients that they had shredded the letters received in error.

[36] On March 18, 2026, this office requested an update from Health regarding any additional NTR letters that had been returned or shredded. Health indicated that one more person had come forward on March 10, 2026, confirming that they had promptly shredded an NTR letter sent to them in error.

[37] As of April 8, 2026, Health confirmed that it had taken no further action to contain the breach beyond the letters it sent to the unintended recipients. To date, this breach has not been fully contained as there are still 140 NTR letters that have not been recovered, and

Health did not sufficiently follow up. The containment efforts of Health, in this matter, are insufficient.

[38] Privacy best practices state that a trustee should attempt to retrieve personal health information that has "gone astray."[13] Given the magnitude of this breach and considering it involves HSNs, Health should make additional efforts to recover this critical personal health information as it is unique to the individual. For example, Health should have contacted the 140 outstanding unintended recipients a second time by letter, telephone call or email to request that the NTR letters received in error be returned or shredded.

b. Notification of Affected Individuals

[39] It is best practice for trustees to inform affected individuals as soon as possible when personal health information has been breached. This is an obvious step that invokes the principles of fairness. Affected individuals should be informed of the possible risks so they can take any steps they deem necessary to protect themselves. An effective notification should include:[14]

- A general description of how the breach occurred.
- A detailed description of the personal health information involved (e.g., name, health number, medical record information, etc.).
- A description of the types of harm that may result from the breach.
- Steps the trustee has taken to mitigate the harm and prevent future breaches.
- Actions that affected individuals can take to mitigate harm from the breach.
- Contact information of an individual within the organization who can answer questions and provide information.
- A notice that individuals have the right to complain to OIPC.

[13] OIPC Investigation Report 015-2025 at paragraph [48].

[14] *Supra,* footnote 3 at paragraph [36].

- Recognition of the impact of the breach on affected individuals and an apology.

[40] Between November 28 to December 1, 2025, Health mailed notification letters to all 224 affected individuals.

[41] OIPC reviewed this notification letter and noted that it contained a description of the breach and personal health information involved, steps taken to prevent future breaches, an apology and contact information for Heath. The notification letter also informed individuals of their right to complain to OIPC regarding this breach as well as contact information for this office. This letter could have acknowledged the possible harm, but it is evident that identity theft is the main concern and quite obvious from the description of the breach provided by Health.

[42] Based on the information above, this office is satisfied with the notification efforts of Health regarding this breach.

c. Investigate the breach

[43] Trustees must conduct an investigation in the wake of a privacy breach to learn the cause of the breach and to prevent a future occurrence. The investigation should address the incident on a systemic basis and include a root cause analysis.[15]

[44] Trustees must consider their "duty to protect" under section 16 of *HIPA*, which requires that trustees establish policies and procedures to maintain administrative, technical and physical safeguards to protect personal health information. Section 16 of *HIPA* provides:

> **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the integrity, accuracy and confidentiality of the information;

[15] *Ibid,* footnote 3 at paragraph [41].

(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.

[45] The Pharmacist Manager of Client Services at DPEBB initiated the investigation on November 17, 2025. ARCAS was informed of the breach and told to investigate the root cause.

[46] On November 18, 2025, ARCAS held a meeting with its Privacy Officer, the Lead on Health Mailings, and other management to assess the magnitude and scope of the breach. ARCAS also met with all staff, including the employee involved in the printing of the NTR letters.

[47] By November 24, 2025, ARCAS determined that the employee tasked with printing the final batch of 334 NTR letters had accidentally printed them in duplex (double-sided) not simplex (single-sided), which resulted in 167 double-sided NTR letters. As some of these letters were sent to families, it was further revealed that 57 of these 167 letters also contained two HSNs, resulting in a total of 224 affected individuals in this matter. ARCAS communicated these findings to DPEBB on November 24, 2025, via email.

[48] It is evident that ARCAS had the appropriate administrative safeguards in place at the time to prevent the privacy breach that occurred had they been followed. The root cause of this breach was a senior employee who failed to follow the ARCAS administrative safeguards in place at the material time. The employee in question did not follow the proper steps as outlined in the ARCAS policy "*Process for Ministry of Health's Mailings*". The employee somehow missed a programming check and did not change the printer settings to simplex. Additionally, that same employee also missed an auditing check and did not ensure that

the print numbers on the audit tracking sheet for the last batch of NTR letters matched the total count of envelopes to be mailed on the Statement of Mailing (SOM) to Canada Post.

[49] DPEBB notified Health's Chief Privacy and Access Officer as well as the Health Information and Privacy Branch on November 24, 2025, to indicate the nature and scope of the breach. Health discussed the breach during an internal meeting on November 25, 2025, and proactively reported the matter to OIPC on November 26, 2025. Given the timelines, both Health and ARCAS took timely action to address the privacy breach and complete their investigations.

[50] ARCAS indicated in the materials it submitted to this office that management spoke with the employee who was the cause of the privacy breach on November 18, 2025. No disciplinary action was deemed necessary. The employee had been with ARCAS for 15 years, was remorseful and agreed to undertake re-training with respect to ARCAS data security and confidentiality.

[51] Investigating a privacy breach to identify the root cause is key to understanding what happened so that similar breaches will not occur in the future. ARCAS provided this office with an overview of the relevant corporate safeguards in place.

[52] Administrative safeguards include fundamental corporate documents that preserve the security of personal health information. They can include policies and procedures regarding privacy and security of the premises, and they will almost always require employee oaths/affirmations that the policies will be honoured by the employee.[16]

[53] ARCAS had several administrative safeguards in place at the time of the privacy breach. The first was the *Staff Data Security Agreement* which outlined expectations of ARCAS employees for maintaining the confidentiality of sensitive information and protecting this information from unauthorized disclosure, use or access. This document is signed by all

[16] *Ibid*, at paragraph [47].

ARCAS employees at the commencement of employment, including the employee who was the root cause of this privacy breach.

[54] ARCAS also provided this office with the following policies and procedures that were in place at the time of this matter:

- *Privacy Training Manual for Data Processing & Mail Fulfillment Facilities:* details best practices for protecting the confidentiality of sensitive information and contained relevant guidance specifically directed at employees who work within the lettershop[17] area and deal with confidential information as part of their duties.

- *Process for Ministry of Health's Mailings:* details a 16-step process to be followed by ARCAS employees when completing mailings for Health. These steps include transferring confidential mailing data, generating batch cover sheets and Statements of Mailing (SOM) for print jobs, validating print quantities through audit sheets, keeping batches aligned before they are inserted and sealed for mailing and most importantly, confirming that the audit sheets total match the SOM before letters are sent to Canada Post.

d. Steps taken to prevent future breaches

[55] The most important aspect in responding to a privacy breach is the implementation of measures to prevent similar future breaches. Prevention measures can include strategies such as adding/enhancing safeguards, providing additional training, and monitoring or auditing systems and users.[18]

[56] The employee at the center of this privacy breach voluntarily repeated essential training in data security and confidentiality, including:

- Reviewed the *Privacy Training Manual for Data Processing & Mail Fulfillment Facilities* (November 18 and 24, 2025);

[17] Lettershop staff are involved in supervising the physical printing of documents, putting the documents are put into the inserter (which folds documents, inserts them into envelopes and seals the envelopes), and checking/weighing batches for accuracy before they are sent to Canada Post.

[18] *Supra,* footnote 3 at paragraph [56].

- Reviewed and re-signed the *Staff Data Security Agreement* (March 27, 2026);[19]

- Reviewed additional documents related to data privacy and responses to privacy breaches.

[57] Following the breach, ARCAS created an amended version of its *Process for Ministry of Health's Mailings* which included several additional audit checks targeted at preventing future breaches of a similar nature. OIPC reviewed this document and noted that these additional checks included:

- A partial redaction of the HSN on all out-going Health mailings with only the last 3 digits of the HSN denoted on the correspondence.

- A requirement that lettershop staff bring their completed audit sheet, tracking sheet and SOM to the supervising manager.

- A managerial review of the audit sheet, tracking sheet and SOM to verify that the number of letters printed matches the number of prints indicated on the SOM before the mailing is released to Canada Post.

[58] ARCAS' amended *Process for Ministry of Health's Mailings* also included an option to provide final tracking sheets and Canada Post SOMs to clients, such as Health. ARCAS indicated that the additional improvements to this document have been implemented in some of its mailings with the goal of implementing this level of security for all ARCAS mailings.

[59] Additionally, ARCAS indicated it will be holding monthly meetings to discuss data integrity, security and confidentiality as well as update and monitor its privacy training materials as needed.

[60] OIPC commends ARCAS for the targeted efforts it made in updating its policies to prevent breaches of a similar nature from occurring.

[19] ARCAS submitted that this employee initially signed this document on March 1, 2010, at the commencement of employment with ARCAS.

[61] Regarding Health and its role as a trustee under *HIPA*, Health should implement a formal IMSP agreement with ARCAS as explicitly required by section 18(2) of *HIPA*.

[62] Health carries the burden of responsibility for safeguarding the sensitive personal health information in its custody and control. It is crucial that Health upholds its duties under *HIPA* to ensure that personal health information is protected when it is shared with outside organizations for the purpose of providing information management services.

[63] Section 7 of *The Health Information Protection Regulations, 2023,*[20] clearly outlines the requirements for formal written agreements between trustees and IMSPs. This section provides:

> **7.** For the purposes of subsection 18(2) of the Act, a written agreement that is entered into between a trustee and an information management service provider must include:
>
> (a) a description of the specific service the information management service provider will deliver;
>
> (b) provisions setting out the obligations of the information management service provider respecting the security and safeguarding of personal health information;
>
> (c) provisions for the destruction of the personal health information, if applicable;
>
> (d) a requirement that the information management service provider not use, disclose, obtain access to, process, store, archive, modify or destroy personal health information received from a trustee except for the purposes set out in subsection 18(1) of the Act;
>
> (e) a requirement that the information management service provider comply with the terms of the agreement entered into with the trustee; and
>
> (f) a requirement that the information management service provider notify the trustee at the first reasonable opportunity of any breach of the agreement.

[20] *The Health Information Protection Regulations, 2023*, RRS c H-0.021 Reg 2 (effective August 1, 2023), as amended by Saskatchewan Regulations 68/2023.

[64] Health should make immediate efforts to engage ARCAS and become compliant with *HIPA*.

III FINDINGS

[65] OIPC has jurisdiction to undertake this investigation under the authority afforded by *HIPA*.

[66] Health is the trustee with custody and control of the personal health information in this matter. *HIPA* is engaged.

[67] ARCAS meets the definition of an IMSP pursuant to *HIPA*.

[68] A privacy breach occurred when an ARCAS employee failed to follow proper administrative safeguards which resulted in the personal health information of 224 affected individuals being mailed to 167 unintended recipients in contravention of *HIPA*.

[69] Health did not make adequate containment efforts in relation to the privacy breach.

[70] Health notified the affected individuals appropriately and in a timely manner with respect to this matter.

[71] Both Health and ARCAS conducted a fulsome investigation regarding the privacy breach.

[72] ARCAS had appropriate and reasonable safeguards in place to prevent the privacy breach had they been followed.

[73] The root cause of this privacy breach was a senior ARCAS employee who failed to follow proper administrative safeguards during the printing and mailout process.

[74] ARCAS took reasonable steps to prevent similar privacy breaches from happening in the future including addressing the employee and requiring retraining.

[75] Health did not have a formal written agreement in place with ARCAS as required by *HIPA*.

IV RECOMMENDATIONS

[76] I recommend that Health makes additional efforts to contact the outstanding 140 unintended recipients in an effort to fully contain this privacy breach.

[77] I recommend that Health engage ARCAS in a formal written contract as required by section 18(2) of *HIPA* and detailed in section 7 of the *HIPA Regulations*. This agreement should be completed and put in place within 90 days of issuing this Investigation Report. Health should provide OIPC with a copy of this agreement.

Dated at Regina, in the Province of Saskatchewan, this 1st day of May 2026.

Grace Hession David
Saskatchewan Information and Privacy Commissioner