Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 303-2025[1]

Autism Services of Saskatoon Inc.

Ministry of Social Services

August 7, 2026

Summary: In March 2025, Autism Services of Saskatoon Inc. (Autism Services) suffered a ransomware attack and certain systems within its information technology (IT) network were rendered inaccessible. In November 2025, Autism Services proactively reported this privacy breach to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC).

Autism Services has a *Service Agreement* with the Ministry of Social Services (Social Services) and a *Funding Agreement* with the Saskatchewan Health Authority. The Commissioner found that Social Services, a government institution and trustee, still had control over the relevant personal information and personal health information in this matter. As a trustee and local authority, Autism Services shared possession, custody and control over the personal information and personal health information that was impacted by this privacy breach.

At the time of the ransomware attack, Autism Services' firewall had limited capability to log activities such as network traffic to detect and investigate threats to its IT network. As a result, a forensic investigation could not conclusively identify how the threat actor gained access to Autism Services' IT network. Autism Services submitted that the threat actor likely accessed and exfiltrated information off its online system. Autism Services concluded that the likely entry point was vulnerability within a firewall even though it had been patched prior to the attack occurring.

The Commissioner made several findings, including:

1) A privacy breach occurred.

2) Autism Services took reasonable steps to contain the privacy breach;

[1] The other OIPC case file number associated with this investigation is 361-2025.

3) Autism Services properly notified the affected individuals of the privacy breach;

4) Autism Services undertook a forensic investigation into the privacy breach but because of an IT security deficiency at the material time, Autism Services was unable to come to a final conclusion with respect to the root cause of the privacy breach;

5) Autism Services took reasonable steps to enhance the security of its IT network.

The Commissioner made several recommendations, including:

1) Autism Services should ensure that future privacy breach notices to affected individuals include information about the right to complain to OIPC and OIPC office contact information;

2) Autism Services should undertake regular vulnerability assessments and penetration testing in the future to identify gaps in its IT security system;

3) Autism Services should regularly remind affected individuals to be vigilant in their efforts to protect themselves against fraud and identity theft by checking their credit reports and credit scores on a regular basis; and

4) Social Services should establish baseline IT security requirements and provide support for community based organizations, such as Autism Services, that engage in a service agreement with Social Services.

I BACKGROUND

[1] Autism Services of Saskatoon Inc.[2] (Autism Services) is an organization that provides supports to individuals and the families of those with autism spectrum disorder. It has an *Agreement for Services* (*Service Agreement*) with the Ministry of Social Services (Social Services) and a *Funding Agreement* in place with the Saskatchewan Health Authority (SHA).

[2] Autism Services of Saskatoon, Inc.

[2] On March 20, 2025, Autism Services discovered that it had suffered a ransomware attack and certain systems within its information technology (IT) network became inaccessible.

[3] Autism Services immediately isolated the affected systems and terminated network access. A forensic investigation revealed that the threat actor had likely accessed and exfiltrated data that Autism Services had collected from its online application from clients and former employees. A ransomware demand was discovered on a desktop computer. The day after the breach, Autism Services began to restore its servers. The stolen data elements included:

- Names;
- Dates of birth;
- Home addresses;
- Social insurance numbers;
- Saskatchewan health numbers;
- Medical and therapeutic information;
- Credit card information; and
- Client referral and intake information, (including service plans, case notes and progress updates).

[4] On September 3, 2025, Autism Services notified the 2,168 individuals affected by this privacy breach by letter and email.

[5] On November 17, 2025, Autism Services proactively reported this privacy breach to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC).

[6] On December 23, 2025, OIPC notified both Autism Services and Social Services that an investigation of this matter would commence.

[7] On February 2, 2026, Autism Services filed a submission with this office.

[8] On February 27, 2026, Social Services opted to not file a submission.

II DISCUSSION OF THE ISSUES

1. Establishing Jurisdiction

a. The Health Information Protection Act (*HIPA*)[3]

[9] *HIPA* is engaged when three elements are present: (i) a trustee; (ii) personal health information; and (iii) the trustee has custody or control over the personal health information.

i. First element – a trustee

[10] Section 2(1)(t)(ii) of *HIPA* defines "trustee" as follows:

> **2**(1) In this Act:
>
> ...
> (t) **"trustee"** means any of the following that have custody or control of personal health information:
>
> ...
> (ii) the provincial health authority or a health care organization;

[11] Section 1-2 of *The Provincial Health Authority Act* [4] defines "health care organization" as follows:

> **1-2** In this Act:
>
> **"health care organization"** means:
>
> (a) an affiliate; or
>
> (b) a prescribed person that receives funding from the provincial health authority to provide health services;
>
> [Emphasis added]

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

[4] *The Provincial Health Authority Act*, SS 2017, c P-30.3, as amended.

[12] Section 6(1) of *The Provincial Health Authority Administration Regulations*[5] provides:

> **6**(1) For the purposes of the definition of **"health care organization"** in section 1-2 of the Act, the persons set out in Table 1 are prescribed as health care organizations.

[13] Table 1 in Part 1 of the Appendix of the above current provincial regulations lists a previous name for Autism Services: "Autism Treatment Services of Saskatchewan, Inc."

[14] Information Services Corporation has a current listing for Autism Services of Saskatoon Inc. This registration database also lists previous entity names for Autism Services such that we conclude the regulations refer to the same entity:

Previous Entity Names

Type	Name	Effective Until
Registered Name	SASKATOON SOCIETY FOR AUTISM INC.	09-Jul-2000
Registered Name	AUTISM TREATMENT SERVICES OF SASKATCHEWAN, INC.	27-Jun-2013

[15] Section 2-29 of *The Legislation Act*[6] defines the term "person" as:

> **"person"** includes a corporation and the heirs, executors, administrators or other legal representatives of a person;

[16] Since the term "person" in *The Provincial Health Authority Act* can include a corporation, we conclude that Autism Services is a "health care organization" pursuant to section 1-2(b) of that statute.

[17] Autism Services qualifies as a "trustee" as defined by section 2(1)(t)(ii) of *HIPA*.

[5] *The Provincial Health Authority Administration Regulations*, RRS c P-30.3 Reg 1, (effective December 4, 2017) as amended.

[6] *The Legislation Act*, SS 2019, c L-10.2, as amended.

ii. Second element – personal health information

[18] We now categorize the data elements involved in this incident which qualify as personal health information: health services numbers, medical and therapeutic information, and client referral and intake information (including service plans, case notes and progress updates).

[19] Section 2(1)(m) and (q) of *HIPA* defines "personal health information" 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;
>
> ...
> (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;
>
> …
> (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;

[20] Information such as names, dates of birth, health services numbers, medical and therapeutic information that are involved in this incident qualify as "personal health information" as defined by section 2(1)(m) and (q) of *HIPA*.

iii. Third element – the trustee has custody or control over the personal health information

[21] The *Funding Agreement* between Autism Services and SHA confirms that Autism Services is a trustee that has control over personal health information:

> 11.8 **Personal Health Information:** The Parties hereby acknowledge that SHA and Autism Services of Saskatoon are both trustees pursuant to HIPA, SHA at clause (2)(t)(ii) as the "provincial health authority", and Autism Services of Saskatoon at 2(t)(ii) as a prescribed health care organization. The Parties further acknowledge that for the purposes of providing the Services pursuant to this Agreement, Autism Services of Saskatoon will be required to collect and use personal health information of its Clients. Autism Services of Saskatoon explicitly acknowledges that by doing so, it becomes a trustee and agrees to comply fully with its obligations pursuant to *The Health Information Protection Act* (Saskatchewan), including in respect of disclosure of such personal health information to SHA only in accordance with *The Health Information Protection Act* (Saskatchewan). In such case, both Parties agree to collect, use or disclose such personal health information only for the purposes of planning, delivering, evaluating and monitoring the Services for Clients in accordance with the applicable governing provincial legislation.
>
> [Emphasis added]

[22] Based on the above, we conclude that Autism Services has custody and control over the personal health information at issue.[7]

[23] Since all three elements are present, *HIPA* is engaged. OIPC undertakes this investigation pursuant to the jurisdiction as afforded by *HIPA*.

b. The Freedom of Information and Protection of Privacy Act (FOIP)[8]

[24] Social Services often refers their clients to Autism Services for support and assistance. The files of clients of Social Services have been impacted by this breach. The following analysis

[7] *Custody* means that a trustee has physical possession of records with a measure of control over them. *Control* means having the authority to manage the records including storing, restricting, and regulating their use. OIPC Investigation Report 266-2024 at paragraph [14].

[8] *The Freedom of Information and Protection of Privacy Act*, SS 1990-91, c F-22.01, as amended.

will reveal that Social Services has a duty to maintain the integrity of its client's records that have been referred to Autism Services and as such, *FOIP* is relevant to this analysis..

[25] *FOIP* applies to **"government institutions"** as defined by section 2(1)(d) of *FOIP*. On its own, Autism Services is not a "government institution". However, Social Services is a government institution because Social Services maintains control over the records and dictates how Autism Services is to maintain the records, including returning "confidential information" if requested by the Minister. Therefore, Social Services has "control" over the "Client Records" and "Services Records" as defined in the *Service Agreement* it entered into with Autism Services by virtue of sections 9.1(b), (d), and (e) of this agreement:

> 9.1 The Agency acknowledges that in the course of providing the Services, it will require and receive documents, data and other information from the Minister, including personal information within the meaning of *The Freedom of Information and Protection of Privacy Act* and/or personal health information within the meaning of *The Health Information Protection Act* (collectively referred to throughout this paragraph as "confidential information"). This confidential information will be included in Records that come into existence as a result of the provision of Services under this Agreement. In that regard, the Agency agrees that it will:
>
> …
> (b) protect and secure confidential information to ensure that it remains confidential;
>
> …
> (d) not use or disclose the confidential information for any purpose other than for the provision of the Services under this Agreement;
>
> (e) promptly return the confidential information to the Minister, if requested;

[26] Social Services is a "government institution" as defined by section 2(1)(d)(i) of *FOIP*.[9] As such, *FOIP* is engaged in this matter as it relates to the "Client Records" and "Service Records" as defined in the *Service Agreement*. OIPC has jurisdiction to investigate this matter pursuant to PART VII of *FOIP*.

[9] Social Services is also a "trustee" as defined by section 2(1)(t)(i) of *HIPA* of personal health information in the "Client Records" and "Services Records" pursuant to section 9.1 of the *Service Agreement*.

[27] The data elements that are subject to *FOIP* in this Investigation Report include most of the data elements listed in paragraph [3] of this Investigation Report because of the definitions in clause 1.1 of the *Service Agreement.* We will review the data elements that were affected by this breach in terms of whether they can be precisely categorized as personal information in more detail in the next section of this Investigation Report, but for now the terms of the *Service Agreement* are broad enough to apply to most of the data elements listed in paragraph [3] above:

> **1.1** In this Agreement:
>
> …
> (c) **"Client Records"** means file recordings, documents and information kept by the Agency which relate to the provision of Services by the Agency to its clients;
>
> ...
> (e) "**Records"** means Client Records and Services Records;
> ...
>
> (g) **"Services Records"** means all documents, books, accounts and other information of the Agency relating to the provision of Services under this Agreement other than Client Records;

[28] Since *FOIP* is engaged, OIPC undertakes this investigation pursuant to the jurisdiction as afforded by *FOIP*.

c. *The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP)*[10]

[29] *LA FOIP* applies to "local authorities" as defined by section 2(1)(f) of *LA FOIP*. Section 2(1)(f)(xvii) of *LA FOIP* defines a "local authority" as follows:

> **2**(1)(f)(xvii) any board, commission or other body that:
>
> (A) receives more than 50% of its annual budget from the Government of Saskatchewan or a government institution; and

[10] *The Local Authority Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c.L-27.1, as amended.

(B) is prescribed;

[30] PART II of the Appendix of *The Local Authority Freedom of Information and Protection of Privacy Regulations*[11] (*LA FOIP Regulations*) mandates:

> PART II: Boards, Commissions and Other Bodies Prescribed as Local Authorities
> [*Subclause 2(f)(xvii) of the Act*]
>
> ...
> 3. health care organizations as defined in *The Provincial Health Authority Act*

[31] In paragraph [16] above, OIPC concluded that Autism Services is a "health care organization" pursuant to section 1-2 of *The Provincial Health Authority Act*.

[32] Upon review of recent Financial Statements posted to its website, Autism Services receives most of its funding from government institutions such as Social Services.[12] Autism Services is also a prescribed "health care organization" as defined by section 1-2 of *The Provincial Health Authority Act*.

[33] Since Autism Services qualifies as a "local authority" as defined by section 2(1)(f)(xvii) of *LA FOIP*, OIPC has jurisdiction to investigate this matter pursuant to PART VI of LA FOIP.

2. A privacy breach occurred

[34] A privacy breach occurs when personal health information and personal information is collected, use and/or disclosed in a way that is not authorized by *HIPA, FOIP*, and/or *LA FOIP*.

[11] *The Local Authority Freedom of Information and Protection of Privacy Regulations*, RRS c L-27.1 Reg 1, (effective July 1, 1993) as amended.

[12] Financial Statements appear on at the bottom of the *Governance* page of Autism Services' website.

[35] OIPC established in paragraph [20] above that personal health information as defined by *HIPA* was involved.

[36] At this point we will now focus on the data elements that constitute personal information in more detail. Section 24(1) of *FOIP* defines "personal information":

> **24**(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:
>
> ...
> (d) any identifying number, symbol or other particular assigned to the individual, other than the individual's health services number as defined in *The Health Information Protection Act*;
>
> …
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual;

[37] Section 23(1) of *LA FOIP* defines "personal information" as follows:

> **23**(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:
>
> ...
> (b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
>
> ...
> (d) any identifying number, symbol or other particular assigned to the individual;
>
> (e) the home or business address, home or business telephone number, fingerprints or blood type of the individual;
>
> ...
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual;

[38] Further, section 24(1.1) of *FOIP* provides that "personal information" does not include information that qualifies as "personal health information" under *HIPA*:

> **24**(1.1) Subject to subsection (1.2), "personal information" does not include information that constitutes personal health information as defined in *The Health Information Protection Act*.

[39] Similarly, section 23(1.1) of *LA FOIP* provides that "personal information" does not include information that qualifies as "personal health information" under *HIPA*:

> **23**(1.1) On and after the coming into force of subsections 4(3) and (6) of *The Health Information Protection Act*, with respect to a local authority that is a trustee as defined in that Act, "personal information" does not include information that constitutes personal health information as defined in that Act.

[40] In paragraph [20] above, we concluded that information such as names, dates of birth, health service numbers, medical and therapeutic information qualifies as personal health information as defined by section 2(1)(m) and (q) of *HIPA*. This leaves the rest of the data elements in paragraph [3] of this Investigation Report that were also subject to the privacy breach for consideration. For example, information such as social insurance numbers[13] and client referral information in the "Client Records" and "Service Records" qualify as personal information as defined by section 24(1)(d) and (k) of *FOIP*.

[41] Finally, information with respect to current and former employees of Autism Services such as their names, social insurance numbers, contact information and employee number qualifies as personal information as defined by section 23(1)(b), (d), (e) and (k)(i) of *LA FOIP*.

[42] Both personal health information and personal information were subjected to this privacy breach. The next step in the analysis is to determine if the personal information and personal information was collected, used and/or disclosed in a way that was not authorized by *HIPA*, *FOIP* and *LA FOIP*.

[13] At paragraph [10] of Review Report 129-2024, OIPC found that social insurance numbers qualify as personal information pursuant to section 24(1)(d) of *FOIP*.

[43] *HIPA* defines the terms "collect" and "use" as follows:

> **2**(1) In this Act:
>
> ...
> (b) **"collect"** means to gather, obtain access to, acquire, receive or obtain personal health information from any source by any means;
>
> ...
> (u) **"use"** includes reference to or manipulation of personal health information by the trustee that has custody or control of the information, but does not include disclosure to another person or trustee.

[44] The term "disclosure" in the context of *HIPA* means the sharing of personal health information with a separate entity that is not a division or branch of the trustee organization.[14]

[45] Neither *FOIP* nor *LA FOIP* define the terms "collect," "use," or "disclosure". In the past, OIPC has defined these terms as follows:[15]

- "Collection" means to bring together, assemble, accumulate or obtain personal information from any source by any means.
- "Use" indicates the internal utilization of personal information by a government institution and includes the sharing of the personal information in such a way that it remains under the control of the government institution.
- "Disclosure" means to share personal information with a separate entity, not a division or branch of a government institution in possession or control of that record or information.

[46] Autism Services submitted that the threat actor "likely accessed and exfiltrated" information.[16] The exfiltration of personal information and personal health information

[14] OIPC Investigation Report 080-2022 at paragraph [14].

[15] OIPC Investigation Report 251-2025 at paragraph [30]. OIPC Investigation Report 041-2021 at paragraph [15].

[16] In Investigation Report 003-2025, OIPC defined the term "exfiltration" as meaning to steal sensitive data from a computer.

constitutes an unauthorized "disclosure" of personal information and personal health information. As such, a privacy breach occurred.

3. The Response to the Privacy Breach

[47] The analysis of an organization's response to a privacy breach involves several factors. OIPC considers the following to determine if an organization has appropriately responded to a privacy breach:[17]

- Containment of the breach as soon as possible;
- Notification of affected individuals;
- Investigation of the breach; and
- The adoption of preventative measures.

a. Containment of the Breach

[48] Upon learning that a privacy beach has occurred, an organization should take immediate steps to contain the breach. Depending on the nature of the breach, this can include:[18]

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

[49] Autism Services indicated that it learned of the privacy breach on March 20, 2025, when the threat actor accessed and exfiltrated data from its systems. Upon learning of the attack, Autism Services isolated the affected systems and terminated network access to contain the privacy breach. Then Autism Services immediately retained outside legal counsel to advise and outside cyber security experts were engaged on behalf of Autism Services to assist with containment and remediation. The cyber security experts also conducted a complete investigation into the scope and cause of the incident. This privacy breach was

[17] OIPC Investigation Report 099-2025 at paragraph [24].

[18] *Supra,* footnote 16 at paragraph [34].

also reported to the federal policing authorities (RCMP). These are all essential containment steps.

[50] Autism Services reported that the last observed unauthorized activity was on that same day – March 20, 2025. It did not detect further malicious activity in its IT environment after that date.

[51] Autism Services reported that data was likely exfiltrated by the threat actor and not recovered. Autism Services confirmed that the dark web was actively monitored and did not identify any evidence to suggest the copied data was published or otherwise exploited for any fraudulent purpose.

[52] Autism Services has taken reasonable steps in its containment of the privacy breach.

b. Notification of Affected Individuals

[53] Section 29.1 of *FOIP* requires government institutions, to take all reasonable steps to notify affected individuals when a privacy breach creates a real risk of significant harm to the affected individuals.[19]

> **29.1** A government institution shall take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the government institution if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

[54] Social Services did not offer a submission in this matter. Did Social Services consider the privacy breach in this instance as the real risk of significant harm that it was? A privacy breach involving data elements that included names, addresses and social insurance numbers can surely lead to the real risk of identity theft.[20] We are sadly in the dark as to

[19] Section 28.1 of *LA FOIP* has a similar provision to section 29.1 of *FOIP*. Section 28.1 of *LA FOIP* requires local authorities to notify individuals of an unauthorized use or disclosure of individuals' personal information by a local authority if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individuals.

the responses, if any, on the part of Social Services. We can only conclude that Social Services has not fulfilled its obligation pursuant to section 29.1 of *FOIP*.

[55] Even though *HIPA* does not have a similar provision as section 29.1 of *FOIP* or section 28.1 of *LA FOIP*, it is a best practice for trustees such as Autism Services, and Social Services, to inform affected individuals when their personal information and/or personal health information has been breached by threat actor(s).

[56] A notice to affected individuals should include the following:[21]

- 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 the affected individual because of the privacy breach.
- Steps taken and planned to mitigate the harm and 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).
- Contact information of an individual within the organization who can answer questions and provide further information.
- A notice that individuals have a right to complain to OIPC (provide OIPC's contact information).
- Recognition of the impacts of the breach on affected individuals and, an apology.

[57] Autism Services notified the affected individuals by letter and email on September 3, 2025. The letter contained almost all the essential elements of an effective notice, including an offer of 12-months of credit monitoring and identity protection services to the affected

[20] *Supra,* footnote 13 at paragraphs [37] and [38].

[21] *Supra,* footnote 16 at paragraph [42].

individuals. This is an appropriate and commendable move. The only element missing from the notice was a communication of the right to complain to OIPC along with OIPC's contact information. Autism Services' notice to affected individuals was deficient in this regard.

[58] Autism Services included its telephone number so that affected individuals could call for information or to express concerns regarding the privacy breach. Autism Services confirmed that approximately 49 individuals responded.

[59] Going forward any party that experiences a privacy breach should ensure its notices to affected individuals include information about their right to complain to OIPC and OIPC's contact information.

c. Investigation of the Breach

[60] Once containment has been addressed and appropriate notification to affected individuals has been given, the organization should conduct a thorough investigation. The investigation must address the incident on a systemic basis and include a root cause analysis and conclusion. The organization must consider its duty to protect personal information pursuant to section 24.1 of *FOIP* and section 23.1 of *LA FOIP* and to protect personal health information pursuant to section 16 of *HIPA*. Section 24.1 of *FOIP* provides:

> **24.1** Subject to the regulations, a government institution shall establish policies and procedures to maintain administrative, technical and physical safeguards that:
>
> (a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the personal information in its possession or under its control;
>
> (ii) loss of the personal information in its possession or under its control; or

(iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and

(c) otherwise ensure compliance with this Act by its employees.

[61] Section 23.1 of *LA FOIP* provides:

23.1 Subject to the regulations, a local authority shall establish policies and procedures to maintain administrative, technical and physical safeguards that:

(a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;

(b) protect against any reasonably anticipated:

(i) threat or hazard to the security or integrity of the personal information in its possession or under its control;

(ii) loss of the personal information in its possession or under its control; or

(iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and

(c) otherwise ensure compliance with this Act by its employees.

[62] 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;

(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.

[63] Social Services was silent on the duty to protect pursuant to section 29.1 of *FOIP* and section 16 of *HIPA*.

[64] Social Service required Autism Services to report privacy breaches as laid out in the *Service Agreement* as follows:

> 9.0 CONFIDENTIALITY
>
> 9.4 The Agency shall immediately advise the Minister:
>
> (a) if the Agency knows or suspects that confidential information may have been compromised;
>
> (b) if the Agency or an affiliated company of the Agency is served with an order, demand, warrant or any other document purporting to compel the production of any of the confidential information, including an order made pursuant to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT ACT); or
>
> (c) if the Agency becomes aware that any requirement of this Article 9.0 has been breached.

[65] Autism Services confirmed that Social Services was notified of the privacy breach on September 2, 2025.

[66] Beyond being notified of the privacy breach, it is unclear what role was played by Social Services in terms of the investigation or its assistance to Autism Services in relation to this privacy breach.

[67] As noted, Autism Services undertook a complete forensic investigation and hired outside legal counsel and cyber security experts in that respect.

[68] At the time of the attack, Autism Services had the following safeguards in place:

- Patch management for production systems;
- Multifactor authentication;
- Antivirus installed on endpoints and services; and

- Firewalls.

[69] A deficiency with Autism Services' firewall at the time of the attack was its limited capability to log activities such as network traffic. Overall, there were blind spots in the system that made it difficult if not impossible to detect or investigate security threats. As we explain below, Autism Services has now remedied this deficiency.

[70] As a result, the forensic cyber experts hired by Autism Services to investigate the breach concluded that the threat actor entry point was likely by means of a vulnerability within a firewall. Autism Services reported that on January 14, 2025 it was aware of the vulnerability and had it patched by February 24, 2025. The attack occurred a month later on March 20, 2025.

d. Preventative Measures Going Forward

[71] It is crucial that organizations implement measures to prevent privacy breaches in the future. Possible prevention measures include adding/enhancing safeguards already in place, the provision of additional training and the regular monitoring/auditing of systems and system users.

[72] Autism Services has greatly increased the system logging capacity. It will now be much easier to detect and investigate malicious attacks going forward. Further, Autism Services has engaged an outside expert agency, a Managed Service Provider (MSP), that manages, monitors, and guards its IT systems. Autism Services has taken reasonable steps to enhance the security of its network.

[73] We recommend that Autism Services ensure that regular vulnerability assessments and penetration testing continue in the future so any gaps in the security features are identified and remedied.

[74] Autism Services confirmed that it had monitored the dark web and did not identify any evidence to suggest the copied data was published or otherwise exploited for any fraudulent

purposes. We were not informed of the monitoring period. There is no guarantee that the information will not be used at any time in the future. We recommend that Autism Services remind all affected individuals to be vigilant in their efforts to protect themselves against fraud and identity theft.

[75] Finally, without a submission from Social Services, it is unclear what role Social Services assumed in this matter. We do not know if Social Services assisted Autism Services to secure the personal information of clients or if it assisted in the investigation of the privacy breach. At the very minimum, OIPC recommends that Social Services establish baseline IT security requirements and provide support for community based organizations, such as Autism Services, that engage in a service agreement with Social Services.

III FINDINGS

[76] OIPC undertakes this investigation pursuant to the jurisdiction as afforded by *HIPA*.

[77] OIPC has jurisdiction to investigate this matter pursuant to PART VII of *FOIP*.

[78] OIPC has jurisdiction to investigate this matter pursuant to PART VI of *LA FOIP*.

[79] A privacy breach occurred.

[80] Autism Services has taken reasonable steps to contain the privacy breach.

[81] Autism Services properly notified the affected individuals of the privacy breach;.

[82] Autism Services undertook a forensic investigation into the privacy breach but because of IT security deficiencies at the material time, Autism Services was unable to come to a final conclusion with respect to the root cause of the privacy breach.

[83] Autism Services has taken reasonable steps to enhance the security of its network.

IV RECOMMENDATIONS

[84] I recommend that in the event of a future privacy breach, the Autism Services' notices to affected individuals include information about the individuals' right to complain to OIPC and the OIPC office contact information.

[85] I recommend that Autism Services undertake regular vulnerability assessments and penetration testing in the future to identify gaps in its IT security.

[86] I recommend that Autism Services regularly remind affected individuals to be vigilant in their efforts to protect themselves against fraud and identity theft by checking their credit reports and credit scores on a regular basis.

[87] I recommend that Social Services establish baseline IT security requirements and provide support for community based organizations, such as Autism Services, that engage in a service agreement with Social Services.

Dated at Regina, in the Province of Saskatchewan, this 7th day of August, 2026.

Grace Hession David
Saskatchewan Information and Privacy Commissioner