MANITOBA OMBUDSMAN

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT & PERSONAL HEATH INFORMATION ACT INVESTIGATION REPORT

Manitoba Families

Privacy Breach: Use, Disclosure and Security of Information

CASE# MO-09540

Final Report with Recommendations & Response

Issued to Public Body:
May 7, 2026

Published with Response:
May 28, 2026

Provisions considered:
FIPPA – 41, 41.1, 49(a)(i)
PHIA – 1(1), 18(1), 19, 19.0.1, 28(a)

SUMMARY

In November 2024, Manitoba Families (Families or the public body or trustee) submitted a privacy breach report to our office after its service provider experienced a cybersecurity incident that resulted in unauthorized access to personal information (PI) and personal health information (PHI) belonging to 1,361 Manitoba residents (affected individuals). The affected individuals received service from the Community Living disABILITY Services program of Families, through a community-based service provider (the Service Provider) funded and contracted by Families under a service purchase agreement.

Our office investigated the circumstances of the incident, the Service Provider's response, and Families' obligations as a trustee under The Personal Health Information Act (PHIA) and as a public body under The Freedom of Information and Protection of Privacy Act (FIPPA) (collectively, the Acts) with respect to the protection of PI and PHI held by the Service Provider on its behalf. Our investigation was conducted under Part 4 of the Acts.

Our office found that Families did not have service provider management policies, security control guidelines, or an active audit program in place to oversee the Service Provider's privacy practices, including cybersecurity.

Our office issued five recommendations to Families to address these gaps, and requested that Families provides an implementation plan within 60 days of its acceptance. Families responded to our report and recommendations on May 25, 2026. It accepted the recommendations and stated that it would provide the implementation plan within 60 days of its acceptance.

PURPOSE AND SCOPE OF THE REPORT

The purpose of this report is to inform the public about the cybersecurity incident involving Families and to provide transparency regarding the nature of the incident and the actions taken in response.

In preparing this report, our office withheld the name of the third-party service provider involved in this incident and deliberately generalized certain technical, operational, and security-related details. This approach is intended to avoid disclosing sensitive information that could reasonably be exploited by threat actors, while still providing sufficient information to meet the public interest in transparency and accountability.

TABLE OF CONTENTS

INTRODUCTION

The Department of Families (Families) Community Living disABILITY Services (CLDS) program provides support and services to adults living with an intellectual disability to live satisfying and independent lives in the community.[1] In this CLDS program, Families refers eligible adults, providing their personal and personal health information to contracted external service providers who deliver program services directly to these Manitobans, on behalf of Families. The funding, program parameters and accountabilities are outlined in Families' service purchase agreements.

This report concerns an investigation of a privacy breach under Part 4 of both The Personal Health Information Act and The Freedom of Information and Protection of Privacy Act.

Our office received notification of the incident from Families on October 28, 2024, followed by a formal privacy breach report on November 20, 2024. The incident resulted in unauthorized access to personal information (PI) and personal health information (PHI) of 1,361 adults receiving services through an external service provider (the Service Provider).

The information on the Service Provider's systems that was compromised included legal names, addresses, day program information, emergency contacts, level of support required, Social Insurance Numbers (SIN), sources of income, Personal Health Identification Numbers (PHIN), medical professional contact information, medical needs, plans of care, and medication information.

Our office investigated this matter in accordance with our powers under Part 4 of the Acts. In particular, clause 28(a) of PHIA enables the Ombudsman to conduct investigations and make recommendations to monitor and ensure compliance with PHIA.

> ***General powers and duties***
> ***28*** *In addition to the Ombudsman's powers and duties under Part 5 respecting complaints, the Ombudsman may*
>
> *(a) conduct investigations and audits and make recommendations to monitor and ensure compliance with this Act;*

[1] Manitoba Families, *Community Living disABILITY Services*, online: https://www.gov.mb.ca/fs/clds/index.html; *Are you Eligible?*, online: https://www.gov.mb.ca/fs/clds/eligible.html (retrieved on 2026-04-09).

Subclause 49(a)(i) of FIPPA enables the Ombudsman with the same authority in substantially similar terms.

> ***General powers and duties***
> ***49*** *In addition to the Ombudsman's powers and duties under Part 5 respecting complaints, the Ombudsman may*
> *(a) conduct investigations and audits and make recommendations to monitor and ensure compliance*
> *(i) with this Act and the regulations,*

The investigation looked at the circumstances of the breach, the Service Provider and Families' response to it, and whether the actions of Families were in compliance with the requirements of FIPPA and PHIA. We also sought to understand what safeguards Families has in place to protect the privacy of program participants receiving services from its Service Provider.

Our office requested written representations from both Families and the Service Provider, both of which provided detailed information in response. Our office also conducted an interview with Families to discuss its approach to service provider oversight and its existing practices in relation to the Service Provider.

DUTY TO ADOPT SECURITY SAFEGUARDS

Section 41 of FIPPA sets out a public body's obligations for the protection of PI in the custody or control of the public body.

> ***Protection of personal information***
>
> ***41*** *The head of a public body shall, in accordance with any requirements set out in the regulations, protect personal information by adopting reasonable administrative, technical and physical safeguards against such risks as unauthorized access, use, disclosure or destruction.*

PHIA contains similar but more stringent requirements for protection of PHI. It sets out that the reasonableness of security safeguards to protect personal health information in a trustee's custody or control shall take into account the degree of sensitivity of such personal health information.

Definitions

1(1) *In this Act,*

[…]

"personal health information" *means recorded information about an identifiable individual that relates to*

(a) the individual's health, or health care history, including genetic information about the individual,

(b) the provision of health care to the individual, or

(c) payment for health care provided to the individual,

and includes

(d) the PHIN and any other identifying number, symbol or particular assigned to an individual, and

(e) any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care;

Duty to adopt security safeguards

18(1) *In accordance with any requirements of the regulations, a trustee shall protect personal health information by adopting reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information.*

Safeguards for sensitive information

19 *In determining the reasonableness of security safeguards required under section 18, a trustee shall take into account the degree of sensitivity of the personal health information to be protected.*

The Personal Health Information Regulation (the Regulation) further requires trustees to establish and comply with their policy and procedures.

Written security policy and procedures

2 *A trustee shall establish and comply with a written policy and procedures containing the following:*

(a) provisions for the security of personal health information during its collection, use, disclosure, storage, and destruction, including measures

(i) to ensure the security of the personal health information when a record of the information is removed from a secure designated area, and

(ii) to ensure the security of personal health information in electronic form when the computer hardware or removable electronic storage media on which it has been recorded is being disposed of or used for another purpose;

(b) provisions for the recording of security breaches;

(c) corrective procedures to address security breaches.

Subsections 8(1) and (2) of the Regulation further require trustees to audit their security safeguards and to take corrective action where deficiencies are identified.

Audit

8(1) *A trustee shall conduct an audit of its security safeguards at least every two years.*

8(2) *If an audit identifies deficiencies in the trustee's security safeguards, the trustee shall take steps to correct the deficiencies as soon as practicable.*

PART 1: OVERVIEW OF THE INCIDENT

Part 1.1: Incident identification and containment

On October 8, 2024, the Service Provider identified suspicious activity on its systems. On the same day, the Service Provider engaged third-party cybersecurity specialists to assist with containment, remediation, and forensic investigation. The Service Provider confirmed that it isolated affected systems, implemented countermeasures to prevent further unauthorized activities, reset credentials, hardened systems, and rebuilt servers, and enhanced firewall, VPN, domain controller, server, endpoint, and Microsoft 365 security configurations.

On October 9, 2024, the Service Provider notified Families of the incident.

The forensic investigation concluded on October 21, 2024. The investigation determined that unauthorized access and data exfiltration had occurred. The investigation could not conclusively determine the attack vector due to insufficient available evidence. Based on the information available, the most likely attack vector was the Service Provider's virtual

private network (VPN). An attack vector refers to the method or pathway used by the threat actor to gain unauthorized access to the Service Provider's systems. The Service Provider reported the incident to law enforcement and to the National Cybercrime Coordination Centre.

Based on our review of the information reported to us by the Service Provider, our view is that the Service Provider responded promptly to the incident and took reasonable steps to contain and remediate the breach.

Part 1.2: Evaluate the risks associated with the breach

Under both FIPPA and PHIA, when a public body determines that a privacy breach creates a real risk of significant harm to affected individuals, the public body must provide notification of the breach to the affected individuals and to the ombudsman. Subsection 41.1(1) of FIPPA and subsection 19.0.1(1) of PHIA define "significant harm" identically as follows:

> ***"significant harm"*** *includes, in relation to an individual, bodily harm, humiliation, damage to the individual's reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the individual's credit rating or report, and damage to or loss of the individual's property.*

As explained in our practice note,[2] assessing whether a breach creates a real risk of significant harm requires considering both the sensitivity of the personal or personal health information involved and the likelihood that it could be misused, based on the cause and extent of the breach, the number and vulnerability of affected individuals, the security and recovery of the information, and any evidence that harm has already occurred. The practice note also emphasizes that "real" and "significant" require more than a vague possibility, and that public bodies must complete a breach-specific assessment using the regulatory risk factors and available tools as guidance, recognizing that the tools are not exhaustive and the assessment drives notification and other required response steps.

---

[2] Manitoba Ombudsman, *Key Steps in Responding to Privacy Breaches under the Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Health Information Act (PHIA)*, online: https://www.ombudsman.mb.ca/wp-content/uploads/2025/11/PN-FIPPA-PHIA-breach-key-steps-EN.pdf, [*Key Steps in Responding to Privacy Breaches*].

Families advised our office that it conducted a risk assessment on October 23 and 24, 2024, to evaluate whether the incident created real risk of significant harm (RROSH) to the affected individuals. Based on the sensitivity of the PI and PHI involved, the vulnerability of the affected individuals, and the fact that the information remained potentially accessible and could be misused by the threat actor(s), Families determined that the incident met the definition of RROSH. Our office finds that Families considered the required factors and is in compliance with the legislation and the Regulation in assessing the risk of harm.

The sensitivity of the information involved warrants emphasis. The compromised information included SINs, PHINs, medical needs, plans of care, and medication information. SINs and PHINs are unique government-issued identifiers that can be used to facilitate identity theft or fraudulent access to government services. Financial information, including sources of income, and detailed medical information, including medication information and care plans, are among the most sensitive categories of personal information. The exposure of these categories of information creates a heightened risk of financial loss, identity theft, and damage to reputation or relationships, as contemplated under the definition of significant harm in the Acts.

Part 1.3: Notification

Under section 41.1 of FIPPA and section 19.0.1 of PHIA, public bodies have a duty to notify affected individuals and our office of a privacy breach, as soon as practicable after the breach becomes known to the head of the public body, if the breach creates a real risk of significant harm to affected individuals. See Appendix A for notification requirements.

As noted above, the incident was discovered on October 8, 2024. The forensic investigation concluded on October 21 and determined that unauthorized access and data exfiltration had occurred. Families confirmed that this incident met the definition of RROSH on October 24 and provided direct notification to affected individuals on November 24 by letter, approximately one month after the RROSH determination.

Families advised our office that its Community Support Workers provided in-person notification to certain, but not all, vulnerable individuals. Families also advised our office that notification was delayed by a month for several reasons:

- The forensic investigation was still ongoing at the time of the RROSH determination which required time to work with its third-party cybersecurity specialists to

determine the full nature and scope of the incident before notifying affected individuals;

- The Service Provider was working with external legal counsel to ensure that all legal obligations were met;
- The Service Provider had to report the incident to law enforcement and to the National Cybercrime Coordination Centre; and
- Delivery of the notification letters was further affected by the Canada Post postal strike, which ran from November 15 to December 17, 2024.

Our office acknowledges the reasons provided for the delay. However, as explained in our office's practice note, *Key Steps in Responding to Privacy Breaches Under FIPPA and PHIA,*[3] notification should occur as soon as is practicable following a RROSH determination, and prompt notification can serve as an important risk mitigation strategy, enabling affected individuals to take steps to protect themselves and allowing them to share information about possible harms that the public body may not otherwise be aware of.[4] Given the acute sensitivity of the information involved and the RROSH determination in late October 2024, consideration could have been given to some form of earlier preliminary notification (such as a media alert or direct contact by phone or email, followed by formal written notification) to affected individuals or those who provide support to them.

We note where direct notification is impracticable because of the large number of individuals affected by the privacy breach, subclause 3.3(1)(c)(i) of the Access and Privacy Regulation and subclause 8.9(1)(c)(i) of the Personal Health Information Regulation both provide that indirect notification may be given to affected individuals.

Given that 1,361 Manitobans were affected, and the practical challenges of direct written notification, Families should have considered providing indirect notification through public announcement on the Service Provider and/or Families website. An earlier notification would have allowed individuals and their caregivers to take protective steps at an earlier stage, including monitoring financial accounts and taking steps to secure their SINs and PHINs.

When Manitobans receive services through government programs and entrust their highly sensitive PI and PHI to a public body or trustee, they also rely on that public body or trustee to protect their information. This obligation does not diminish when the

[3] *Ibid* at 5–6.
[4] *Ibid.*

services of the public body or trustee are delivered through contracted third parties, as explained below in Part 2 of this report.

In the present case, Families funded and contracted the Service Provider to serve these individuals on its behalf. Accordingly, Families continues to hold the duty to adopt security safeguards for the PI and PHI of those individuals including when the Service Provider processes and stores that information in the course of service delivery. Where a privacy breach occurs, prompt notification of affected individuals is required under the Acts, allowing them and those who support them to take protective measures without delay.

In terms of the content of notification, our office reviewed the notification template provided by Families and assessed it against the requirements of section 8.8(1) of the *Personal Health Information Regulation* and section 3.2(1) of the *Access and Privacy Regulation*. We are satisfied that the notification addressed all mandatory elements by describing (i) the circumstances of the breach and the date on which the unauthorized access was detected, (ii) the categories of PI and PHI compromised, (iii) the steps taken by the Service Provider to contain and remediate the breach as well as measures intended to reduce the risk of recurrence, (iv) the protective steps available to affected individuals, (v) our office's contact information, (vi) Families' contact person available to answer questions, etc.

Part 1.4: Prevention

Following the containment of the incident, the Service Provider implemented a series of preventive measures on its network, identity and access management, server infrastructure, endpoints, and cloud environment. We also reviewed the post-incident security assessment dated December 9, 2024, completed by a third-party consultant which contained recommendations to address common issues associated with ransomware incidents,[5] including weak perimeter controls, inadequate authentication requirements, excessive privilege, and insufficient endpoint monitoring. The Service Provider confirmed that it has accepted all recommendations in that report. We acknowledge the Service Provider's efforts in implementing such preventive measures, and we also view that its deployment of two-factor authentication specifically on VPN

[5] Canadian Centre for Cyber Security, *Ransomware Playbook*, online: https://www.cyber.gc.ca/sites/default/files/itsm00099-ransomware-playbook-e.pdf, at 10-14.

access is an appropriate measure, given that the VPN was identified as a possible attack vector. However, we also note that the forensic investigation could not conclusively confirm the attack vector due to insufficient available evidence, and some recommendations remain outstanding.

The Service Provider advised some recommendations remain in progress due to financial constraints. It explained that it is a non-profit organization with limited cybersecurity funding and that it faces challenges implementing certain long-term measures.

In its representations, Families acknowledged that resources to fully implement the outstanding recommendations remain a challenge, noting that the Service Provider is a non-profit organization with minimal funding available for cybersecurity.

These funding constraints highlight the importance of Families establishing clear minimum cybersecurity standards and providing proactive guidance to its service providers, so that service providers are well-equipped to identify and prioritize the resources necessary to meet those standards. As discussed below in Part 2, Families did not have such standards or guidance in place at the time of the incident.

Notwithstanding these resource limitations, we acknowledge the Service Provider's efforts to implement preventative measures to mitigate risks to privacy. We would expect Families, in the exercise of its oversight responsibilities, to work with the Service Provider to establish a timeline for the completion of the outstanding recommendations.

PART 2: FAMILIES' OBLIGATIONS REGARDING SERVICE PROVIDER PRIVACY AND CYBERSECURITY CONTROLS

When a trustee or public body contracts with a third-party service provider to deliver services on its behalf, it continues to hold its responsibilities under the Act to ensure the protection of the PI or PHI of its clients served under the agreement. In the present case, the Service Provider is an external agency funded and contracted by Families under a service purchase agreement to deliver services to Families clients. Families provides PI and PHI to the service provider, and, through the course of providing daily supports and services to the individual, the Service Provider also collects, uses, and retains PI and PHI belonging to those individuals. Although the PI and PHI is stored on the Service Provider's systems, it remains under the control of Families at all times.

The principle that an organization continues to be responsible for PI and PHI under its control, including when that information has been provided to a third party for the purpose of delivering services, is one of the foundational principles of privacy protection recognized internationally[6] and adopted by Canadian courts and privacy oversight bodies across public sector, health privacy, and private sector frameworks.[7]

The Manitoba Ombudsman previously examined the service provider oversight obligation in the 2021 Privacy report on Manitoba's Families, Children's Disability Services[8] (the 2021 CDS Report). That investigation found that external service providers funded and contracted by Families under service purchase agreements are brought under the requirements of FIPPA and PHIA either by the Access and Privacy Regulation under FIPPA, or through the terms of the service purchase agreement itself. The report also emphasized that public bodies and trustees are responsible for ensuring external service providers handle PI and PHI appropriately, determining each service provider's obligations under the Acts and ensuring those obligations are met.[9]

Similarly, The Saskatchewan Information and Privacy Commissioner found that a local authority cannot shift responsibility for the protection of PI to a service provider, as the public body retains care and control of that information at all times, and that merely having a contractual framework in place without actual implementation and verification is insufficient.[10] The Information and Privacy Commissioner of Alberta also found that public bodies are accountable for the actions or inaction of their contracted service providers in

---

[6] Organisation for Economic Co-operation and Development, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (23 September 1980, revised 11 July 2013), online: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188, at paras 14, 16; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (*General Data Protection Regulation*), [2016] OJ L 119/1, arts 24, 28.

[7] *Prairie Spirit School Division (Re)*, 2025 CanLII 81113 (SK IPC), <https://canlii.ca/t/kdv75>, retrieved on 2025-11-28, at para 24; *Edge Imaging (Re)*, 2024 CanLII 90510 (SK IPC), <https://canlii.ca/t/k6zxj>, retrieved on 2025-11-28, at para 24; *Toronto District School Board (Re)*, 2025 CanLII 117835 (ON IPC), <https://canlii.ca/t/kgj9b>, retrieved on 2026-03-24, at para 43; *Canada (Privacy Commissioner) v. Facebook, Inc.,* 2024 FCA 140 (CanLII), <https://canlii.ca/t/k6pn1>, at paras 92-98, 114-118, retrieved on 2026-03-26 [*Facebook 2024*]. Note: leave to appeal to the Supreme Court of Canada was granted; the appeal was heard on March 19, 2026, and judgment was reserved as of the date of this report.

[8] Manitoba Ombudsman, *PHIA Case 2020-1304: Privacy Breach Report – Manitoba Families, Children's disABILITY Services,* online (pdf): https://www.ombudsman.mb.ca/wp-content/uploads/2025/03/case-2020-1304-en.pdf, at 45-46 [*2021 CDS Report*].

[9] *Ibid*.

[10] *eHealth Saskatchewan Saskatchewan Health Authority Ministry of Health (Re)*, 2021 CanLII 214 (SK IPC), <https://canlii.ca/t/jcgk0>, retrieved on 2026-03-29, at para 50.

relation to the protection of PI, and that accountability for compliance rests with the public body, not the service provider.[11] In the context of Canada's federal private sector privacy legislation, the Federal Court of Appeal affirmed that an organization's safeguarding obligations do not end when PI is shared with or transferred to a third party, and that an organization must implement proactive oversight measures rather than rely solely on contractual terms to discharge those obligations[12].

In the Manitoba Ombudsman's 2023 follow-up report on the implementation of recommendations from the 2021 CDS report, it confirmed that Families' oversight obligations remained only partially implemented,[13] noting Families must take additional steps to standardize and consistently monitor service providers' compliance with the service purchase agreements and PHIA, and to adequately fulfill its oversight responsibilities.[14]

In addition to establishing a policy specifying cybersecurity requirements on third-party service providers, public bodies and trustees should also exercise their due diligence and due care by assessing and reviewing the service providers' security controls, rather than accepting their claims[15] or simply assuming such measures are in place because they are required in an agreement.

As noted in the 2021 CDS Report, the Ombudsman published the *Guidelines for Implementing a Privacy Management Program for Privacy Accountability in Manitoba's Public Sector* in 2017 which established the following necessary controls, among other things, for an effective and accountable privacy management program.[16]

---

[11] *Investigation into the PowerSchool Breach* (F2025-IR-02), Office of the Information and Privacy Commissioner of Alberta, online (pdf): https://oipc.ab.ca/wp-content/uploads/2025/11/FINAL-Investigation-Report-Regarding-PowerSchool-Breach-FOIP2025-IR-02.pdf, at paras 18, 29, 45.
[12] *Facebook 2024, supra* note 7 at paras 92-98, 114-118.
[13] Manitoba Ombudsman, *Review of Privacy Breach Recommendations made to Children's disAbility Services*, online: https://www.ombudsman.mb.ca/wp-content/uploads/2025/03/case-mo-00783-en-en.pdf, at 3 [*2023 CDS Follow-Up*].
[14] *Ibid* at 13.
[15] National Institute of Standards and Technology, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, online (pdf): https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf, at 41 and 158 [*NIST SP 800-161r1*].
[16] Manitoba Ombudsman, *Guidelines for Implementing a Privacy Management Program for Privacy Accountability in Manitoba's Public Sector,* online(pdf): https://www.ombudsman.mb.ca/wp-content/uploads/2025/03/privacy-management-program-guidelines-en.pdf, at 2 [*PMP Guidelines*].

- Privacy and security risk assessment, encompassing security threat and risk assessments for new projects, services, or systems involving personal information and for significant changes to existing ones;
- Service provider management, specifying that a privacy management program must include standard contractual clauses to ensure service provider compliance with privacy obligations; and
- Procedures that ensure the privacy officer of the public body is involved in procurement and contracting processes that relate to services involving personal information.

Accordingly, our office reiterates that trustees and public bodies in Manitoba must establish and enforce internal policies and standards that ensure third-party service providers comply with the Acts. Such policies should set out the privacy and cybersecurity risks, requirements and responsibility, among other things, from the executive level.[17] This includes defined practices for (i) vendor management, (ii) audit and oversight of third-party security safeguards, and (iii) review of security documentation and incident response capabilities.

During this investigation, Families confirmed in writing and during the interview that it had relied primarily on the service purchase agreement as the mechanism for ensuring the Service Provider's compliance with its duty to adopt security safeguards, without having conducted any independent monitoring, inspection, or audit of the Service Provider's security practices.

Although the findings of the 2021 CDS Report and the 2023 CDS Follow-Up arose in the context of a children's disability program and a different type of breach, the service provider oversight obligation described in these reports remains the same. Families has a duty to provide guidance on and oversight of its service providers' privacy practices and security safeguards, including cybersecurity, to ensure compliance with the Acts. Families' accountability for ensuring its service providers protect the PI and PHI of program participants in compliance with the Acts is acknowledged in the preamble of the service purchase agreement between Families and the Service Provider. Nevertheless, Families relied solely on those contractual provisions without actively providing guidance or oversight of the Service Provider's privacy practices and security safeguards.

[17] *NIST SP 800-161r1, supra* note 15 at 19.

Part 2.1: Written Agreement Between Families and the Service Provider

During the investigation, our office requested a copy of the agreement between Families and the Service Provider. Families provided the Service Purchase Agreement (SPA) and its appendices.

In reviewing the SPA, our office notes the following provisions as relevant to this investigation as well as the Service Provider's obligations regarding privacy and security safeguards:

- Section 8.03 grants Families the rights to audit the Service Provider.
- Section 12.02 acknowledges that personal information provided by the Service Provider to Families respecting individuals receiving services provided by the Service Provider will be collected, used, disclosed and protected by Manitoba and its officers and employees in accordance with the provisions of FIPPA, PHIA and all other applicable legislation.
- Section 12.03 requires the Service Provider to take all reasonable steps to protect PI and comply with Appendix 2.
- Section 12.04 requires the Service Provider to notify Families of any breach or possible breach of privacy.
- Appendix 2
    - The preamble states:
        - *Manitoba recognizes that funded, external service providers may receive, collect, acquire, be given access to, and may otherwise come into possession of personal information about individuals receiving Services from the Service Provider under this Agreement. Under The Freedom of Information and Protection of Privacy Act, (C.C.S.M. c. F175) and The Personal Health Information Act (C.C.S.M. c. P33.5) Manitoba is responsible for ensuring that personal information is handled appropriately by external service providers.*
    - Section 1.01 defines both PI and PHI under the above noted Acts.
    - Section 1.12 requires the Service Provider to implement reasonable administrative, technical and physical security arrangements to protect PI. The standard of protection shall take into account the PI's sensitivity and the medium in which the PI is stored and processed.
    - Section 1.13(b) requires the Service Provider to maintain its system and network security, and to implement need-to-know access control, and password protection.

- Section 1.19 provides Families with the right to inspect and audit the Service Provider at all reasonable times.
- Section 1.20 requires the Service Provider to take reasonable steps to promptly correct the deficiencies identified in an inspection or investigation to Families' satisfaction.

Part 2.2: Guidance Provided to the Service Provider

During the investigation interview, Families advised our office that it recently provided guidance to its service providers on privacy and security matters on two occasions: in 2022 and again in 2025. On both occasions, Families shared information with service providers through a privacy awareness training presentation covering the following topics:

- The definition and types of privacy breaches;
- The security safeguards requirements under the Acts, categorized as administrative (policies, procedures, tsraining, pledges of confidentiality, etc.), technical (passwords, secure networks, encryption software, firewalls, etc.), and physical (keycard access, locked rooms and areas, lockable filing cabinets, etc.);
- Encryption of sensitive information, portable devices,
- Auto-lock on devices;
- Information security awareness resources, including the Manitoba government's Employee Network Usage Policy and guidance on emails, internet, passwords, and portable devices;
- Safeguard best practices, including locking computers when leaving a workstation, clean desk practices, and creating complex passwords, and
- The key steps in responding to a privacy breach: containment, evaluation, notification, and prevention.

The materials shared with service providers on both occasions were general privacy awareness presentations. While they promote privacy compliance of the Acts, they are not a substitute for clear guidance to service providers on the types of administrative, technical, and physical safeguards Families expects them to implement to meet their obligations under section 1.12 of the SPA.

The materials shared with service providers are general in nature and do not establish any minimum cybersecurity standards, technical requirements, or performance expectations against which Families could assess or enforce compliance. They do not address the specific cybersecurity risks faced by service providers when maintaining PI

and PHI in electronic systems. They do not create any mechanism by which Families can verify that appropriate measures are actually in place at the service provider level.

Our review of the SPA noted that the technical requirements are limited. Section 1.13(b) of Appendix 2 of the SPA establishes a general security baseline limited to (i) secure computer systems, (ii) password protection, and (iii) need-to-know access controls. As cybersecurity threats continue to evolve, this baseline no longer addresses modern cybersecurity threats, including ransomware and phishing attacks, nor does it require preventive measures that the Canadian Centre for Cyber Security[18] identifies as baseline cybersecurity hygiene for Canadian organizations, such as multi-factor authentication and endpoint protection. These gaps were also identified by the Service Provider's third-party cybersecurity specialists in the post-incident security assessment of December 2024. Without clear direction from Families on the minimum cybersecurity measures expected of its service providers, the Service Provider did not have sufficient guidance to understand what specific protections it was required to implement in order to fulfill its obligations under the service purchase agreement to adopt reasonable security safeguards proportionate to the sensitivity of the PI and PHI in its custody.
This gap is made more significant by the factors described in Part 2.3 below. Families does not have its own internal security baseline, cybersecurity policies, or vendor management guidelines. It is difficult for an organization that has not established a security standard for itself to establish or enforce a security standard for its service providers.

Part 2.3: Families' Internal Guidelines and Policies

Our office also requested Families to provide copies of its own vendor/service provider management policy, and any guidelines in relation to security controls. Families advised that it did not maintain any such policies or guidelines. Instead, it relies on the SPA as the primary mechanism governing the Service Provider's obligations under the Acts in relation to the protection of PI and PHI.

The Manitoba Ombudsman Privacy Management Program Guidelines provide that privacy management programs must include procedures for ensuring compliance with the Acts with respect to service providers, and that the privacy officer is involved in procurement and contracting processes relating to services involving PI and

[18] Canadian Centre for Cyber Security, *Cyber security hygiene best practices for your organization - ITSAP.10.102*, online: https://www.cyber.gc.ca/en/guidance/cyber-security-hygiene-best-practices-your-organization-itsap10102.

PHI.[19]Security risk assessment tools, including security threat and risk assessments, are also required program controls under the Manitoba Ombudsman guidelines.[20]

The absence of vendor and service-provider management policies and security control guidelines has significant implications for Families' ability to fulfill its obligations under the Acts.

Without a vendor/service provider management policy, Families has no framework to conduct due care or due diligence of the Service Provider's obligation to protect PI and PHI. Such obligation, as noted above, remains Families' responsibility under the Acts which cannot be satisfied solely by the existence of contractual language.

Likewise, without security control guidelines, Families has no defined standards against which to assess the Service Provider's security safeguards. The SPA cannot serve as a substitute because its security requirements rest on a standard of "reasonableness" without specifying the details by which the parties establish and agree on the minimum technical and administrative measures expected.

As a result, Families lacks internal processes to verify, monitor, or evaluate the Service Provider's compliance with the terms of the agreement, leaving it without the tools necessary to assess whether appropriate safeguards are in place. This falls short of Families' duty to adopt security safeguards under the Acts and creates systemic vulnerabilities when service providers collect, use, retain, and disclose PI and PHI when delivering services to clients on Families' behalf.

Part 2.4: Audit Practices and Third-Party Security Oversight

As PI and PHI are increasingly collected, used, retained, and transmitted in electronic form, the security safeguards applied to that information must be proportionate to its sensitivity as required under section 19 of PHIA. Subsection 18(2) of PHIA identifies a number of specific security safeguards that are required. Subsection 18(3) of PHIA also requires trustees to implement additional safeguards for PHI maintained in electronic form as required by the regulations.

Subsections 8(1) and (2) of the Regulation require trustees to audit their security safeguards and take corrective action where deficiencies are identified. This requirement

[19] *PMP Guidelines, supra* note 16 at 10–11.
[20] *Ibid.*

applies to all types of security safeguards, including but not limited to the specific safeguards described in the Act and the Regulation.

As noted above, the SPA between Families and the Service Provider explicitly grants Families audit and inspection rights under section 8.03 and Appendix section 1.19. Appendix section 1.20 further requires the Service Provider to take prompt corrective steps to remediate any deficiencies identified through inspection or investigation, to Families' satisfaction.

As a trustee under PHIA, Families is bound by these obligations. The SPA's audit provisions give effect to those obligations under PHIA and the Regulation in the contractual relationship with the Service Provider.

During this investigation, our office asked Families whether it had exercised those audit or inspection rights; in particular, whether it had audited the Service Provider's security safeguards, reviewed its incident response plan, or verified its compliance with the Acts. Families confirmed that none of these steps were ever taken. Instead, Families indicated that it relied solely on the contractual framework to bind the Service Provider to the obligations under the Acts.[21] Despite having the authority under the legislative obligation to do so, Families did not conduct any audit, inspection, or technical review of the Service Provider's security safeguards at any time prior to the incident. This is particularly significant given that the Service Provider holds highly sensitive PI and PHI, including medical records and government issued unique identifiers of adults living with an intellectual disability.

The absence of an audit program is compounded by the gap identified in Part 2.3 – Families does not have an internal security baseline or minimum standards of its own against which to measure the Service Provider's controls. The SPA's requirement that the Service Provider implement "reasonable" security arrangements does not provide a sufficient benchmark. It establishes an obligation without defining its content. Without an internal security standard or practical guidance to the Service Provider, Families is not in a position to determine whether the Service Provider's safeguards are adequate, to identify deficiencies, or to enforce remediation under its contractual rights.

[21] In its representations of November 13, 2025, the public body also provided two factors it relied on to ensure compliance: the Service Provider's Residential Care Licensing, and Community Support Workers' ongoing monitoring of service delivery. However, these factors do not assess the security safeguards of PHI or technical security controls.

In establishing a standard or guidance, Families could draw from established cybersecurity supply chain risk management (C-SCRM) models, such as those developed by the International Organization for Standardization (ISO) or the National Institute of Standards and Technology (NIST).[22]

The absence of these program controls at Families meant that it had no structured mechanism to oversee the Service Provider's compliance with its privacy and cybersecurity obligations under the service purchase agreement.

The Information and Privacy Commissioner of Ontario has similarly observed that while it is necessary for public bodies to have a binding agreement with service providers, that alone is not sufficient, and that public bodies must also have sufficient oversight measures in place to ensure that service providers comply with their obligations under the agreement.[23]

The Office of the Privacy Commissioner of Canada reached the same conclusion, observing that there is a strong nexus between contracting and privacy, that outsourcing raises additional privacy risks, and that contracts must be accompanied by active oversight to be effective.[24]

This principle reflects the broader obligation that the public body or trustee remains responsible for protecting PI and PHI under its control by ensuring its service provider actually complies with the contract through periodic audit, inspection, and technical assessments of their security safeguards. In the present case, Families has the contractual rights to audit and inspect the Service Provider, but an internal security standard is required for Families to conduct a meaningful audit.

Our office finds that Families' reliance on the SPA and general privacy awareness guidance, without an internal security baseline, and technical inspection, review, or audit

---

[22] Relevant ISO standards include *ISO/IEC 27001* and *27002* for information security management and controls, and *ISO/IEC 27036* that specifically addresses supplier security and supply chain risk. Relevant NIST frameworks include *NIST SP 800-53* on security and privacy controls, and *NIST SP 800-161* on C-SCRM.

[23] Information and Privacy Commissioner of Ontario, *Privacy and Access in Public Sector Contracting with Third Party Service Providers*, online: https://www.ipc.on.ca/en/media/4297/download?attachment, at 3.

[24] Office of the Privacy Commissioner of Canada, *Investigation into the Contracting Practices of the Canada Border Services Agency Related to the Development of the ArriveCAN Application*, Special Report to Parliament, online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202526/sr_pa_20260312_arrivecan/, at paras 19, 53, 94.

of the Service Provider's actual privacy practices, limited its ability to identify security risks or ensure that reasonable security safeguards were in place in relation to the Service Provider's protection of PI and PHI.

PART 3: CONCLUSION

Our review of the cybersecurity incident found that the Service Provider took appropriate steps to contain the breach, assess the risk, and adopted a range of upgraded technical security safeguards on its network, identity and access management, server infrastructure, endpoints, and cloud environment to prevent recurrence of a breach. Other recommended measures remain in progress and require additional resourcing and guidance from Families.

We found that Families' notification to affected individuals was provided 30 days after it concluded its RROSH assessment and the notification contained all the mandatory elements required by the Personal Health Information Regulation and section 3.2(1) of the Access and Privacy Regulation. Nevertheless, we believe earlier notification to affected individuals could have allowed them to take more timely steps to protect themselves from any potential consequences of the breach.

Consistent with the internationally recognized principles for privacy protection, Families continues to hold responsibility for ensuring that the PI and PHI of the clients it serves are protected, including when that information is held by a service provider on its behalf. We found that Families relied solely on those contractual provisions of its service purchase agreements and general privacy awareness guidance shared with the Service Providers but did not provide active oversight of its privacy practices.

We also found that Families did not have vendor/service provider management policies, security control guidelines, or an active audit and oversight program in place to oversee the Service Provider's privacy practices, including those for cybersecurity at the time of the incident. The general privacy awareness guidance shared with service providers in 2022 and 2025, while helpful, does not constitute the department-defined minimum cybersecurity standards that would be necessary to allow service providers to assess and refresh their own security safeguard policies, including their technical safeguards, or to allow Families to exercise meaningful oversight of those practices.

Concerns regarding Families' oversight of service providers in relation to the requirements of the Acts were identified in our 2021 CDS Report and confirmed as outstanding in our 2023 CDS Follow-Up Report. As we noted in the 2021 CDS Report, Families must provide clear and established policy direction to its service providers to enable their boards to develop and implement policies and procedures ensuring compliance with the Acts.[25]

The same principle applies in the present case. PHIA requires trustees to adopt reasonable administrative, technical and physical safeguards to protect personal health information. Its regulation also requires a trustee to establish "and comply with a written policy and procedures" to ensure the security of that information and to audit those safeguards. Without department-defined technical safeguards standards and guidance for PI and PHI, service providers have no clear baseline against which to develop their own practices, and Families has no defined standards against which to ensure their compliance.

Given that service purchase agreements are not updated frequently and that cybersecurity requirements evolve with the threat landscape, Families should consider setting out its minimum technical safeguards in a separate policy incorporated by reference into the service purchase agreement rather than in the agreement itself. This separate policy should also be embedded in Families' general guidance for its service providers, so that service providers are able to refresh their security safeguard policies, including their technical safeguards, in alignment with Families' expectations over time. This approach would allow Families' minimum cybersecurity standards to be updated to reflect the changing nature of cybersecurity threats and enable ongoing oversight of service providers' compliance with those standards.

Our office has made recommendations to assist Families in establishing the vendor/service provider management framework, audit and oversight program, and updated contractual requirements necessary to meet its obligations going forward.

[25] *2021 CDS Report,* supra note 8 at 46.

PART 4: RECOMMENDATIONS

In light of our findings in this investigation, the Manitoba Ombudsman makes five recommendations to enhance Families' management of third-party service providers' security safeguards for the protection of PI and PHI.

Recommendation 1:

That Families develop and communicate to its service providers clear guidance and minimum standards for the protection of PI and PHI, including the administrative, technical, and physical safeguards Families expects service providers to implement to meet their obligations under the service purchase agreement and the Acts.

Recommendation 2:

That Families develop and enforce a structured framework for managing the cybersecurity risks associated with third-party service providers.

Recommendation 3:

That Families review and update its service purchase agreements with all service providers to ensure alignment with current privacy and cybersecurity expectations. This includes:

(i) having explicit contract language requiring service providers to observe all the requirements of the Acts that Families itself is bound by, and
(ii) requiring compliance with Families' minimum cybersecurity (and other) standards, once established.

Recommendation 4:

That Families develop and enforce a formal audit and oversight process for all third-party service providers handling PI and PHI.

Recommendation 5:

That Families, in the exercise of its oversight responsibilities, follow up with the Service Provider to confirm the status of the outstanding recommendations contained in the post-incident security assessment dated December 9, 2024, and to establish a timeline for their completion.

PART 5: HEAD'S RESPONSE TO THE RECOMMENDATIONS

On May 25, 2026, Families notified our office that it fully accepted the five recommendations, and that it would provide the implementation plan within 60 days of its acceptance. Families' indicated its acceptance as follows:

Response to Recommendation 1:

The department accepts the recommendation and will enhance its practices by working to develop and communicate more specific guidance for third party service providers that outlines expected safeguards under FIPPA and PHIA. This work will build on existing policies and contractual approaches.

Implementation will be undertaken in a collaborative manner, considering operational needs, evolving risks, and resources considerations. The department will also consider appropriate mechanisms for communicating guidance to the service providers to promote clarity, consistency, and compliance,

Response to Recommendation 2:

The department accepts the recommendation and agrees that managing cybersecurity risks related to third party service providers is critical given the rapidly evolving cyber threat landscape. Processes to support and assess risks, and opportunities to enhance their practices will be considered through established governance mechanisms subject to operational priorities and available resources.

Response to Recommendation 3:

The department accepts the recommendation and is currently undertaking a review of the service purchase agreement, in particular the appendix addressing the confidentiality of the protection of personal information requirements and will address the compliance requirements with minimum standards.

Response to Recommendation 4:

The department accepts the recommendation and will consider opportunities to enhance existing practices related to service provider oversight, considering operational priorities, risk levels, and available resources.

Response to Recommendation 5:

The department accepts the recommendations and will continue to follow up with the service provider to confirm appropriate measures have been implemented, consistent with legislation and contractual requirements. Where appropriate, the department will establish reasonable timelines for the service provider to complete any required corrective actions, considering the nature, scope, and risks associated with the breach. These timelines will be communicated as part of the post-incident response process, and progress will be monitored to support accountability and ongoing risk management.

Our office will monitor receipt of the implementation plan and the subsequent implementation of the recommendations.

This report concludes Manitoba Ombudsman's review of this matter.

APPENDIX

The Freedom of Information and Protection of Privacy Act, C.C.S.M. c. F175

Notifying individual of privacy breach

41.1(2) *The head of a public body that has custody or control of personal information about an individual must notify the individual about a privacy breach relating to the information if, after considering the relevant factors prescribed by regulation, the breach could reasonably be expected to create a real risk of significant harm to the individual.*

Notice requirements

41.1(3) *Notice to the individual must*

(a) *be given as soon as practicable after the privacy breach becomes known to the head of the public body;*

(b) *be given in the form and manner, and include the information, required by the regulations; and*

(c) *be given directly to the individual except in circumstances set out in the regulations, in which case it may be given indirectly in the form and manner required by the regulations.*

Notifying Ombudsman

41.1(4) *If the head of a public body is required to notify an individual about a privacy breach under subsection (2), the head must also notify the Ombudsman at the time and in the form and manner that the Ombudsman requires.*

The Personal Health Information Act, C.C.S.M. c. P33.5

Notifying individual of privacy breach

19.0.1(2) *A trustee who maintains personal health information about an individual must notify the individual about a privacy breach relating to the information if, after considering the relevant factors prescribed in the regulations, the breach could reasonably be expected to create a real risk of significant harm to the individual.*

Notice requirements

19.0.1(3) *Notice to the individual must*

(a) *be given as soon as practicable after the privacy breach becomes known to the trustee;*

(b) *be given in the form and manner, and include the information, required by the regulations; and*

(c) *be given directly to the individual except in circumstances set out in the regulations, in which case it may be given indirectly in the form and manner required by the regulations.*

Notifying Ombudsman

19.0.1(4) *If the trustee is required to notify an individual about a privacy breach under subsection (2), the trustee must also notify the Ombudsman at the time and in the form and manner that the Ombudsman requires.*

Access and Privacy Regulation, M.R. 64/98

Form and manner of direct notice to individuals

3.2(1) When notice of a privacy breach is to be given to an individual as required under section 41.1 of the Act, the notice must be given in writing and must include

(a) a description of the circumstances of the privacy breach;

(b) the date or period of time that the privacy breach occurred, or is believed to have occurred;

(c) the name of the public body who had custody or control of the personal information at the time of the privacy breach;

(d) a description of the personal information that was the subject of the privacy breach;

(e) a description of the steps that the public body has taken or is intending to take, as of the date of the notice,

(i) to reduce the risk of harm to the individual as a result of the privacy breach, and

(ii) to reduce the risk of a similar privacy breach in the future;

(f) a description of the steps that the individual can take to reduce the risk of harm that can result from the privacy breach or to mitigate that harm;

(g) a statement that the Ombudsman has been or will be given notice of the privacy breach, as required under subsection 41.1(4) of the Act;

(h) the name and contact information of an officer or employee of the public body who is able to answer questions about the privacy breach; and

(i) any other information that the public body considers relevant.

Personal Health Information Regulation, M.R. 245/97

Form and manner of direct notice to individuals

8.8(1) When notice of a privacy breach is to be given to an individual as required under section 19.0.1 of the Act, the notice must be given in writing and must include

(a) a description of the circumstances of the privacy breach;

(b) the date or period of time that the privacy breach occurred, or is believed to have occurred;

(c) the name of the trustee who had custody or control of the personal health information at the time of the privacy breach;

(d) a description of the personal health information that was the subject of the privacy breach;

(e) a description of the steps that the trustee has taken or is intending to take, as of the date of the notice,

(i) to reduce the risk of harm to the individual as a result of the privacy breach, and

(ii) to reduce the risk of a similar privacy breach in the future;

(f) a description of the steps that the individual can take to reduce the risk of harm that can result from the privacy breach or to mitigate that harm;

(g) a statement that the Ombudsman has been or will be given notice of the privacy breach, as required under subsection 19.0.1(4) of the Act;

(h) the name and contact information of an officer or employee of the trustee who is able to answer questions about the privacy breach; and

(i) any other information that the trustee considers relevant.

This report is available in alternate formats upon request.

MANITOBA OMBUDSMAN
300 - 5 Donald Street, Winnipeg, MB R3L 2T4
204-982-9130 | 1-800-665-0531 | ombudsman@ombudsman.mb.ca
www.ombudsman.mb.ca