# Review of Privacy Breach Recommendations made to Children's disAbility Services

## Case MO:00783

## Report on status of Recommendation Implementation

as of

May 25, 2023

# Introduction

On September 10, 2020, Manitoba Ombudsman initiated a systemic investigation into the circumstances surrounding the privacy breach of the personal health information of 8,900 service recipients, children and youth, of the Children's disAbility Services (CDS) program of Manitoba Families ("the department"). The August 26, 2020 privacy breach was the result of an accidental misdirected email to over 100 unintended recipients.

The systemic investigation considered the circumstances surrounding the privacy breach including the department's email practices, as well as some missed opportunities for early detection and prevention of the incident. The ombudsman explored the department's actions following the privacy breach with respect to containing the unauthorized disclosure, evaluating the risk to the affected individuals, and notification and prevention actions taken to avoid a recurrence. The investigation reviewed the measures taken by the department to adopt reasonable security safeguards to protect the sensitive personal health information in accordance with its responsibilities under the Personal Health Information Act (PHIA).

At the conclusion of the investigation of the privacy breach, we found that Manitoba Families has a long-standing history of incomplete security safeguards. We also determined that the department had only recently made significant progress in the development of PHIA security requirements including pledges of confidentiality, policies, procedures, and enhanced training and that fulfillment of these requirements was incomplete. Based on our findings, we made 9 recommendations to ensure that the required privacy safeguards were implemented and that a culture of privacy could be fostered in the department through the implementation of a privacy management program. A list of our recommendations is located in Appendix A of this document.

The public report with recommendations was released on April 29, 2021, with the department accepting all recommendations, advising on actions it would take to fulfill the recommendations.

In 2022, we notified Manitoba Families that we would review the actions taken since 2021 to fully implement the recommendations made in the report and to monitor its implementation of the security safeguards to ensure compliance with PHIA. We informed the department of our intent to make the results of our review available to the public. A summary of the results follows below, with additional details of our review and commentary contained in Appendix A.

# Follow-Up Review

The intent of our review was to determine the implementation status of the nine recommendations and to provide the public with assurance that Manitoba Families has

implemented privacy policies, procedures, processes, and program controls necessary to be in compliance with the security safeguard requirements of PHIA. We also wanted to determine the measures taken to develop an effective and accountable privacy management program. In the review, we examined the extent to which Manitoba Families completed the following:

- the implementation of PHIA policies and procedures
- the provision of privacy orientation and training to employees and agents/service providers
- the signing of employee, officer and agent/service provider pledges of confidentiality
- the implementation of a process for reporting, and central tracking of, privacy breaches
- the establishment of a privacy management program

We reviewed written policies, staff training curriculum, training logs, training databases, and other documents. We examined the department intranet for online privacy policies, and ease of accessibility for staff seeking guidance on privacy-related issues. During our review, we provided the department with feedback intended to improve clarity and strengthen its privacy policies and administration to reflect best practices. The most significant suggestions are reflected in Appendix A. We are pleased to report our suggestions were accepted and implemented.

We note that Manitoba Families has taken the following actions to improve compliance with legislation:

- Revamped and reorganized its PHIA policies
- Reviewed its policies to ensure consistency
- Updated its pledge of confidentiality to meet the requirements of PHIA
- Established new policies such as a policy for the recording of privacy breaches
- Ensured that its policies/procedures are incorporated into its employee training
- Provided PHIA training to 93% of its employees, and established a centralized training tracking system
- Developed a process to review PHIA pledge signing quarterly
- Established a Privacy Management Committee

Based on the materials reviewed and our assessment of the actions undertaken to date, we have determined that Manitoba Families has fulfilled recommendations 1-7. While we recognize that significant progress was made on all recommendations, we cannot conclude that recommendations 8 and 9 have been completely satisfied at this time.

Recommendation 8 requires that the department ensure that its employees and agents have received privacy training on policies and procedures, and that each employee and agent signs a pledge of confidentiality. These commitments are to be monitored and tracked regularly.

The department implemented this recommendation with its employees. However, as of May 2023, this has not occurred with the employees of the department's external service providers (agents).

In our April 2021 report, we noted the department's standard Service Purchase Agreement (SPA) with its agencies explicitly states that the department is responsible for ensuring that external service providers handle personal information appropriately.
Manitoba Families advised our office that various departmental areas (as outlined in Appendix A of this document) provide some oversight of agencies and their SPAs with the department. However, our review of the information indicates that Manitoba Families must take additional steps to ensure that agents/service providers comply with the requirements for protecting personal health information under the SPA and under PHIA. Given the volume, detail and sensitivity of the personal health information held and maintained by agents, we are of the view that the privacy obligations of agents need to be standardized and consistently monitored for the department to adequately fulfill it oversight responsibilities.

Recommendation 9 focuses on the implementation of a Privacy Management Program (PMP) within Manitoba Families. We believe that a strong privacy culture requires an organization to develop a program that demonstrates it is accountable for its privacy practices and to ensure its handling of personal and personal health information is compliant with legislation. Controls for each department program are an important and the foundational element of a strong privacy management program. Our review confirms that Manitoba Families made an organizational commitment to privacy management by creating a privacy management committee (PMC) (see details in Appendix A).

An essential initial step in ensuring that privacy requirements are met is understanding what personal information and personal health information the department collects, uses, discloses, and retains. An inventory of the personal and personal health information held by the department and its agents is a key program control in a PMP. We appreciate that the department states that it is in the process of compiling the inventory. Given its importance in protecting privacy, our office will monitor Manitoba Families' completion of its inventory and its progress toward full implementation of a privacy management program.

## Conclusion

Manitoba Families and its service providers possess an enormous amount of Manitobans' personal health information under various programs. Following the privacy breach in August 2020, the department has taken many steps to strengthen its PHIA security safeguards to protect personal health information. We find that the department has improved its PHIA policies, its staff training, its recording of security breaches, and its tracking of staff training and PHIA pledge compliance.

We also find that the department needs to take further actions in relation to the protection of personal health information in the custody of its agents/service providers. Manitoba Families needs to strengthen its oversight of service providers' compliance with privacy protection measures contained in its SPAs. Relatedly, we have determined that Manitoba Families needs

to strengthen its foundation to continue to build a culture of privacy by way of its Privacy Management Program. These steps are necessary to rebuild and maintain public trust in a system that collects some of the most sensitive personal health information of Manitobans. Given the significance of this issue, our office has advised Families that we will continue to actively monitor its implementation of recommendations 8 and 9.

Manitoba Ombudsman

# Appendix A

## Children's disAbility Services Privacy Breach Recommendations: Report on status of implementation

Objective: The objective of this review is to determine if Manitoba Families ("the department") has taken the necessary actions to fulfill the recommendations in Manitoba Ombudsman's 2021 Privacy Breach Report. This review includes ensuring that the department has implemented privacy policies, procedures, processes and controls to support compliance with The Personal Health Information Act (PHIA) security safeguard requirements.

| 2021 Recommendation | Evidence Reviewed in 2022-23 | Assessment | Status of Recommendation |
|---|---|---|---|
| ***1. We recommend that Manitoba Families finalize the manual to reflect "Policy and Procedures Manual" in the title, consistent with the contents, to provide employees with greater certainty about their obligations according to policy when required to sign the pledge of confidentiality.*** | Our office reviewed the department's finalized PHIA Policy and Procedures Manual ("the Manual") which had been implemented in July 2021.<br><br>We also reviewed changes made to procedure that reflected suggestions made by our office to strengthen policies or procedures and improve administrative practices. | The department's policies are consistent with the requirements of The Personal Health Information Act (PHIA).<br><br>We reviewed preliminary and final versions of the manual and made suggestions to update references to the provisions of the act to ensure recent amendments to PHIA were reflected in the policies. Other key suggestions to strengthen policy and practice include:<br>• that the department cross-reference its disclosure policy with its email policy to ensure that any disclosure via email follows the proper procedures.<br>• that the department include a specific procedure that addresses how personal health information is to be safeguarded when a record is removed from a secure area (clause 2(a)(i)) of The Personal Health Information Regulation).<br>• that it is a best practice to have a policy for that addresses an individual's right of access to, and correction of, their personal health information. | We assess this recommendation as implemented.<br><br>The department has accepted and implemented our suggestions for improvement to procedures. |

| 2021 Recommendation | Evidence Reviewed in 2022-23 | Assessment | Status of Recommendation |
|---|---|---|---|
| ***2. We recommend that Manitoba Families establish a written policy/procedure containing provisions for the recording of security breaches and specifically who will be responsible for receiving and maintaining this information. Our office suggests that as a best practice the record of security breaches be maintained in a central repository for the purpose of identifying systemic security/privacy incidents.*** | The department advised our office that its Privacy Breach Policy was approved February 18, 2022 and sent to all employees.<br><br>Our office reviewed the Privacy Breach Policy that is available to Families' employees on the departmental intranet.<br><br>Our office reviewed the department's privacy breach process flow-chart and its detailed privacy breach checklist for use by Access and Privacy Coordinators. | The department has made improvements to its recording of security breaches and to its procedures related to collating privacy breach information. The department has a central breach repository that now includes the cause of the breach to improve analysis of systemic issues. A privacy coordinator is assigned to each breach and is responsible to enter and track progress of actions taken in the central repository. These improvements will help the department to identify systemic security and privacy breach incidents.<br><br>Our office provided the department with administrative suggestions for improving its organization of breach-related information. Specifically, we suggested that:<br>• the department include the privacy breach policy in the PHIA Policy and Procedure Manual for ease of reference by staff.<br>• the department clarify departmental staff responsibilities in acting and communicating when privacy breaches occur in order to better respond to privacy breaches. | We assess this recommendation as implemented.<br><br>The department has accepted and implemented our suggestions for improvement. |

| 2021 Recommendation | Evidence Reviewed in 2022-23 | Assessment | Status of Recommendation |
|---|---|---|---|
| ***3. We recommend that Manitoba Families ensures that its PHIA policies and procedures are incorporated into the orientation and ongoing training.*** | Our office reviewed Families' updated PHIA training and compared it with its PHIA Policy and Procedure Manual.<br><br>Our office reviewed the department's PHIA training schedule. Training is available once a month. | We observed that the department's policies in the Manual are incorporated into its training. This helps to ensure that employees are aware of their responsibilities regarding the security of personal health information.<br><br>The training covers key requirements of the legislation and offers concrete examples of implementation of privacy principles in every day work.<br><br>Our office suggested incorporating links to the relevant PHIA policy on each slide for the online training to increase employee awareness of the corresponding policy and procedures.<br><br>Our office also suggested that the training would be strengthened by identifying who is responsible for what actions when a privacy breach occurs. | We assess this recommendation as implemented.<br><br>The department has accepted and implemented our suggestions for improvement. |

| 2021 Recommendation | Evidence Reviewed in 2022-23 | Assessment | Status of Recommendation |
|---|---|---|---|
| ***4. We recommend that Manitoba Families creates an inventory of the policies and guidelines described to our office, including those from Business Transformation and Technology (BTT) [now Digital and Technology Solutions] and the Community Service Delivery (CSD) Division so that employees have certainty about required obligations and guidelines during training and prior to signing of the pledges of confidentiality.*** | Families advised that an inventory of policies and guidelines are available to staff on the Families Intranet Access and Privacy site. Our office reviewed the inventory to ensure consistency with the PHIA Policy and Procedure Manual.<br><br>Our office reviewed the departmental site, the CDS-specific site, and government's digital services intranet site to ensure consistency. | Our office observed that the policies are easy to find on the intranet. The links to privacy-related internal (e.g., privacy breach reporting form) and external resources are easy to find and utilize.<br><br>Our office provided several suggestions to the department based upon our review. For instance, we asked the department to incorporate the privacy breach policy into its PHIA policy and procedures manual for ease of reference. We also asked the department to update/activate certain links on its intranet site to facilitate access by staff to resources, such as the privacy breach reporting form. | We assess this recommendation as implemented.<br><br>The department has accepted our suggestions for improvement. |

| 2021 Recommendation | Evidence Reviewed in 2022-23 | Assessment | Status of Recommendation |
|---|---|---|---|
| ***5. We recommend that Manitoba Families reviews the policies and guidelines listed on its intranet site and the Community Service Delivery intranet site, to ensure that they mirror information provided to employees in PHIA training and at the time of pledge signing.*** | Our office reviewed the policies and guidelines on Manitoba Families' intranet, including the Community Service Delivery Division's internet site.<br><br>We also reviewed Community Living disAbility (CLDS) Services' (who supports adults with intellectual disabilities) 'Protection of Personal Information Guidelines' on Manitoba Families' intranet site. | Our office observed that the policies and guidelines are consistent with its PHIA training.<br><br>Our office provided Manitoba Families with several administrative suggestions that would improve user experience, such as providing additional links to the new policies and forms and ensuring clarity about how the guideline applies to privacy breaches.<br><br>We also advised the following modifications were required:<br>• noting that PHIA pledge signing is mandatory.<br>• updating the CLDS guidelines to include references to personal health information. | We assess this recommendation as implemented.<br><br>The department has accepted and implemented our suggestions for improvement. |

| 2021 Recommendation | Evidence Reviewed in 2022-23 | Assessment | Status of Recommendation |
|---|---|---|---|
| ***6. We recommend that Manitoba Families finalizes the pledge of confidentiality to include reference to personal health information and the consequences for an employee who breaches the department's PHIA policies and procedures.*** | The department advised our office that the revised pledge of confidentiality was approved for use on March 25, 2021.<br><br>Our office reviewed the pledge in relation to the requirements of PHIA. | We observed that the revised pledge of confidentiality does have a statement that the employee is bound by the requirements of the Acts and the policies. It also outlines the consequences of unauthorized activity.<br><br>We further observed that the revised pledge still refers only to 'personal information', rather than 'personal health information' in some cases. We advised the department that the pledge must include:<br>• reference to personal health information.<br>• the statutory definition of personal health information. | We assess this recommendation as implemented.<br><br>The department has accepted and implemented our suggestions for improvement. |

| 2021 Recommendation | Evidence Reviewed in 2022-23 | Assessment | Status of Recommendation |
|---|---|---|---|
| ***7. We recommend that by May 1, 2021, the department implements orientation and training on existing policies and procedures for all new employees and that each employee has signed a pledge of confidentiality that includes an acknowledgment that he or she is bound by the trustee's PHIA policies and procedures and is aware of the consequences of breaching them.*** | Manitoba Families advised our office that its revamped two-hour access and privacy training course is mandatory for all new employees and that each employee signs a pledge of confidentiality following completion of the training. The department stated that new staff are required to take this training prior to working with personal health information. This mandatory course replaces the one-hour orientation session that was previously held quarterly.<br><br>We reviewed the department's training intranet site. We also reviewed a list of employees who took the mandatory training between September 2020 and December 31,2021.<br><br>The department advised that employees are provided with the pledge of confidentiality to sign following completion of training. Employees must provide a signed pledge to their managers, and a copy is maintained in the employee's human resource file. | We observe that the department provided 13 mandatory trainings from May 1, 2021 to December 31, 2021 and note that 887 individuals took the training.<br><br>Although there is no differentiation of new employees in the information provided by Families, we observe that 93% of the department's employees have received the training.<br><br>It is our view that the training of staff is an ongoing activity and will require continued review and oversight by the department. | We assess the creation of the orientation and training program as implemented.<br><br>Progress on training is assessed as ongoing. |

| 2021 Recommendation | Evidence Reviewed in 2022-23 | Assessment | Status of Recommendation |
|---|---|---|---|
| ***8. We also recommend that by December 31, 2021, all existing departmental employees and agents have received privacy training on the policies and procedures and that each employee and agent has signed a pledge of confidentiality that includes an acknowledgment that he or she is bound by the trustee's PHIA policies and procedures and is aware of the consequences of breaching them. The results of these activities for every departmental employee and agent must be logged and tracked, so that timely retraining can occur.*** | **Employees**<br>As stated previously, Families advised that 2632 of 2833,or 93%, of its new and existing employees completed the privacy training as of December 31, 2021. Families stated that all attendees receive an email link to the Pledge and are told they must provide a signed copy to their supervisor. Each quarter, senior management reminds the divisions of the responsibilities in terms of training and PHIA pledges. This also includes a copy of an updated training completion report.<br><br>**Agents/Service Providers**<br>In April 2022 the department sent its training and PHIA pledge template to external service providers (agents). The department states that the objective was for service providers to tailor the training to its unique organizational needs. We reviewed the list of service providers who received the training and pledges.<br><br>Manitoba Families advised our office that program staff work with agencies to ensure that services are provided per the department's service purchase agreement (SPA). The department stated that it can investigate service providers in relation to the SPA under the Residential Care Licensing Manual.<br><br>The department stated that the Agency Accountability and Support Unit (AASU) may review policies if it conducts a financial audit of an agency. The AASU also provides an orientation session to agencies when drafting new SPAs. | Although Manitoba Families states that it is unable to track PHIA pledges centrally, it has taken steps to strengthen its tracking of employee training and pledge-signing by using a quarterly review mechanism that reminds supervisors to ensure that each employee has met their obligations.<br><br>We note that general orientation about the SPA is provided to agents with a focus on program, service delivery, and financial responsibilities. There is not a specific orientation related to their PHIA privacy obligations under the agreement.<br><br>The department is responsible under the SPA to ensure that agents are complying with the requirements for protecting personal health information. It is our view that Manitoba Families must take additional steps to standardize and consistently monitor agents' compliance with the SPA and PHIA for the department to adequately fulfill its oversight responsibilities. | We assess that Manitoba Families has partially implemented this recommendation.<br><br>The department has taken adequate steps to train its existing staff and to track the training. The department has developed an alternate solution for tracking PHIA pledge-signing.<br><br>We assess that the aspect of the recommendation relating to agent/service provider oversight as partially implemented. |

| 2021 Recommendation | Evidence Reviewed 2022-23 | Assessment | Status of Recommendation |
|---|---|---|---|
| ***9. We recommend that Manitoba Families implements a Privacy Management Program.*** | Manitoba Families advised that a privacy management committee (PMC) has been formed. Our office reviewed the PMC's terms of reference. Manitoba Families states that the purpose of the PMC is to ensure that existing policies and procedures are compliant with legislation, to revise and create new policies, and to conduct audits to ensure compliance.<br><br>The department stated that it has initiated its first program-area audit.<br><br>The department stated that it is beginning its process to inventory the personal information/personal health information in its custody or control. | While a privacy management program is not required by PHIA, it is a best practice. As we noted in our investigation report, as a trustee, Manitoba Families is one of the largest holders of personal health information outside of the health system. As such, our view remains that the implementation of an effective and accountable privacy management program would help promote ongoing compliance with PHIA and instill public confidence in the practices employed by Families to safeguard the personal and personal health information of thousands of Manitobans. Our view is that the PMC also provides an important vehicle for the department to outline its procedure for agent/service provider oversight.<br><br>While we agree that the activities noted by Families are critical, we observe that Families has not yet completed appropriate program controls to ensure the requirements of PHIA are implemented throughout the department and with its agents. Development of program controls will enable the PMC to develop the foundation of a privacy respectful culture in the department. The following elements of a Privacy Management Program are still in development:<br>• A complete personal information/personal health information inventory.<br>• Procedures for agent/service provider oversight.<br>• Privacy and security risk assessment tools.<br>• An oversight and review plan to assess and revise program controls on an ongoing basis. The plan should include a review of Families' personal information/personal health information inventory, policies, security risk assessments, training & communication with staff, and service provider oversight. | We assess this recommendation as partially implemented.<br><br>The department has formed a privacy management committee (PMC) and included several key activities of a privacy management program in its PMC terms of reference.<br><br>The department continues to work on implementing other necessary elements of an effective privacy management program. |