

Personal Health Information Act Privacy Breach Report

Case 2020-1304: Manitoba Families, Children's disAbility Services



April 2021

Manitoba  Ombudsman

TABLE OF CONTENTS

OMBUDSMAN'S MESSAGE	3
EXECUTIVE SUMMARY	5
BACKGROUND AND OVERVIEW	8
The discovery of the privacy breach and decision to investigate	8
Ombudsman jurisdiction to investigate	8
Purpose and scope of the review	10
Methodology	10
Manitoba Families	11
LEGISLATIVE CONTEXT	13
Purpose of the Personal Health Information Act	13
PHIA: Applicable sections for the investigation	14
Manitoba Advocate for Children and Youth	17
INVESTIGATION	21
The events leading up to and including the privacy breach	21
Variables impacting the breach	22
Manitoba Families response to the CDS privacy breach	26
Security safeguards: before and after the privacy breach	38
Privacy laws and government-funded external service providers	45
A ROADMAP FOR THE FUTURE: THE CASE FOR A PRIVACY MANAGEMENT PROGRAM	47
CONCLUSION	49
SUMMARY OF RECOMMENDATIONS AND DEPARTMENT RESPONSES	51
APPENDICES	55

Available in alternate formats upon request

Mailing address: Manitoba Ombudsman
 750-500 Portage Avenue
 Winnipeg, MB R3C 3X1

Phone: 204-982-9130

Toll-free phone: 1-800-665-0531

Email: ombudsman@ombudsman.mb.ca

Website: www.ombudsman.mb.ca



OMBUDSMAN'S MESSAGE

Personal health information is some of our most sensitive and private information. We entrust it to government for many reasons, but most often for the purpose of receiving specific benefits or services. Those who are receiving services have the expectation that the government department or program that gathered their personal and personal health information will take all measures to protect and safeguard it. When that information is accidentally shared with the wrong people, or in privacy language, when an unauthorized disclosure happens, the public's trust in government can be damaged. When those affected are vulnerable children and youth, the impact of a privacy breach of sensitive personal health information for those children and their families can be devastating.

On August 26, 2020, a privacy breach occurred when an email containing the personal health information of 8,900 children receiving services from the Children's disAbility Services (CDS) program of Manitoba Families ("the department") was sent in error to approximately 100 service agencies and community advocates, all unintended recipients. The information in the email included such details as the child's name, gender, date of birth, address, the nature of their disability and dates and types of medical or psychological assessments conducted.

This privacy breach, affecting thousands of Manitoba children and their families, was unprecedented in its scope for this province. When Manitoba Families recognized that this privacy breach posed a risk to many vulnerable individuals they immediately reported this breach to my office. While there is no legal obligation to report a privacy breach to my office, proactive reporting is one of the most important steps an organization can take to demonstrate accountability and restore confidence in public programs. It is important that the public, and specifically the citizens who raised concerns to my office, fully understand how the breach happened. In addition, understanding the extent to which the department was meeting its obligations under Manitoba's health privacy legislation is vital to ensuring its accountability for the protection and responsible management of personal health information. For these reasons, under my authority as Manitoba Ombudsman, my office began an investigation of the CDS privacy breach under the Personal Health Information Act (PHIA).

Once privacy is lost, it cannot be remedied for those affected, only improvements can be made to prevent similar breaches from affecting other citizens.

I wish to convey my appreciation to Manitoba Families for their immediate notification of the privacy breach to my office. Their employees cooperated fully with ombudsman investigators in the completion of this review, while continuing to provide supports and services to children and families, made even more challenging during a global pandemic. In our contact with CDS we

saw and heard their commitment to the children and families in the program, and a genuine concern about any loss of trust engendered as a result of the unauthorized disclosure of client health information, however accidental and unintended.

Acknowledgements and commendations are also extended to those unintended recipients of the personal health information – service providers and community advocates – who quickly brought the issue of the misdirected email to the attention of CDS and took immediate steps to provide the program with assurances that the email messages and attachments were securely destroyed.

“We trusted that all our information would be kept private and confidential.”

Above all, I am sincerely grateful to those callers, complainants, affected families and concerned citizens who contacted my office and shared their experiences and concerns in the days after the privacy breach. The information they provided, and their worries about where their children’s personal health information was sent and what was done to secure it after the email breach, were essential components in our investigation of the breach and our review of the department’s existing policies, procedures and safeguards to protect the personal health information of those they serve now and into the future.

It is my honour to provide this report to you.

Jill Perron
Manitoba Ombudsman



EXECUTIVE SUMMARY

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 privacy breach occurred on August 26, 2020.

Under the ombudsman's authority pursuant to part 4 of the Personal Health Information Act (PHIA), the ombudsman may conduct investigations to ensure trustees are in compliance with the act. In completing the investigation of the CDS privacy breach, the office considered the circumstances surrounding the privacy breach including the email practices at issue, 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, approaches to notification and prevention measures taken to avoid a recurrence. The report provides a detailed description of the type of personal health information at the heart of this matter.

The format of the discussions and findings in this report reflects the same sequence of the investigation undertaken. Our intent is for the reader to learn about and understand the circumstances of the privacy breach, as we did.

The ombudsman found that service providers and community advocates, regularly copied on newsletters and other information from CDS, were accidentally blind copied on confidential emails intended only for the Manitoba Advocate for Children and Youth (MACY). The following report discusses the pitfalls of using blind copying which precipitated the privacy breach and the resulting difficulties it presented in detecting errors in emailing.

Highlighting discussions with the department over the months following the privacy breach about concerns expressed by affected individuals, Manitoba Ombudsman strongly advocated for the release of the names of the service providers and community advocates to the individuals affected by the privacy breach. As a result, Manitoba Families developed a process for individuals to receive the names of the agency service providers and community advocates.

The report notes the role of the service providers and advocates who quickly came forward to alert the department of the wrongly received emails, and provided assurance of the steps taken to fully delete the personal health information received. The involvement of these organizations and groups prompted us to consider the vast amount of personal and personal health information of children and adults service agencies must also manage on a day-to-day basis. As we considered the privacy obligations of Manitoba Families through a broader lens and the need for a privacy culture within government, it raised the question of service provider

understanding and compliance with the privacy laws, not as specific trustees as defined under PHIA, but as the service partners of government, and how this is developed and maintained.

The report provides detailed analysis of the department's work with the email recipients to ensure secure destruction of the personal health information received in error and the factors considered in evaluating the risks associated with the unauthorized disclosure. The ombudsman found that the department, at various levels, took extensive measures to notify the affected individuals and to keep the public informed through resources placed on the CDS website.

With respect to preventative measures, CDS assured the ombudsman of the discontinuance of the blind copying practice, of the use of specific instructions for complex communication tasks and the implementation of the revised protocol for data transmission established specific to the MACY operational review.

In addition to an analysis of the circumstances which impacted the privacy breach, the primary focus of the investigation was to assess the measures taken by the department to adopt reasonable security safeguards to protect the sensitive personal health information in accordance with its responsibilities under sections 18 and 19 of PHIA and sections 2-8 of the Personal Health Information Regulation.

A long outstanding issue in previous investigations by Manitoba Ombudsman, the office reviewed the security safeguards (privacy policies and procedures, training, and pledges of confidentiality) implemented to date by the department to assist CDS and all Manitoba Families' employees in their day-to-day handling and transmission of sensitive personal and personal health information of their client populations.

Finding that the department has only recently made significant progress in the development of security safeguards required to be in place, the ombudsman makes several recommendations to Manitoba Families to make certain that privacy safeguards are implemented, including that the department implement a privacy management program. While a component of a privacy management program ensures that there is compliance with privacy legislation, it also seeks to consider and develop knowledge and skill in interpreting privacy legislation in conjunction with other legislation under which a program or department must operate and helps to build and entrench a culture of privacy. A privacy culture cannot fully prevent privacy breaches from occurring, but is a component of a strong defense.

A privacy management program ensures that privacy is built into all initiatives, programs or services.

The report emphasizes that implementation of these safeguards is not solely necessary in order for the department to meet its obligations as a trustee under PHIA, but even more critical to

protect the personal health information of citizens collected for the purpose of service delivery from unauthorized collection, use and disclosure – such as a privacy breach of the magnitude which occurred on August 26, 2020. Manitoba Ombudsman asserts that it is imperative that the work of Manitoba Families in this area remains a priority.

On March 18, 2021, Manitoba Families accepted the nine recommendations made as a result of this investigation. Mindful of the history of concerns about the absence of implemented security safeguards to protect personal health information collected and maintained within the department – policies, procedures, training and pledges of confidentiality – we sought further evidence of the department’s plan to achieve compliance with PHIA and to demonstrate how it would undertake completion of the recommendations. We believe that individuals who receive services from the programs of Manitoba Families must receive more than promises that their personal health information will be protected. The department must be able to provide evidence to verify that it has developed and fully implemented the required safeguards and that its employees receive regular training on the department’s privacy policies and practices.

In a further response to our office on April 7, 2021, the department provided communication and implementation plans showing how it intends to put security safeguards in place. We have notified Manitoba Families of our intent to audit and publicly report in 2022 on the department’s compliance with the security requirements of PHIA and the actions taken to fully implement the recommendations made in this report.



BACKGROUND AND OVERVIEW

The discovery of the privacy breach and the decision to investigate

On August 26, 2020, a privacy breach occurred when email containing the personal health information of 8,900 children receiving services from the Children's disAbility Services (CDS) program of Manitoba Families was sent in error to over 100 service agencies and community advocates, all unintended recipients. The breach was related to a data request from the Manitoba Advocate for Children and Youth, for the purpose of a wide-scale review and investigation of the delivery of children's disability services in Manitoba.

The department proactively contacted Manitoba Ombudsman to notify us of the privacy breach on the date it occurred. While breach reporting is not currently mandatory in Manitoba, our office encourages public bodies and trustees to report privacy breaches when there is significant impact to affected individuals, there are risks resulting from the breach, and/or there are large numbers of people impacted. Such was the case with the CDS incident, where there were thousands of vulnerable children and youth affected and sensitive personal health information was disclosed in error to recipients who had no apparent authorized purpose under PHIA for receiving it.

We began an investigation to review the circumstances of the breach, to examine the department's compliance with the requirements of PHIA and to identify areas where administrative improvements could occur related to the protection and security of personal health information in the care of Manitoba Families. One of the primary purposes for our investigation was to assess the measures taken by Manitoba Families to prevent such a breach of privacy from happening again.

With these goals in mind, on September 10, 2020, we formally notified the minister of Manitoba Families and the public that we had begun a systemic investigation of the CDS privacy breach under the Personal Health Information Act.

Manitoba Ombudsman jurisdiction to investigate

Manitoba Ombudsman is an independent office of the Legislative Assembly of Manitoba and is not part of any government department or agency. In Manitoba, the ombudsman conducts investigations about: access to information and privacy matters (under the Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Health Information Act (PHIA)); the fairness of government actions or decisions (under the Ombudsman Act), or serious "wrongdoings" that a citizen believes may have occurred (under the Public Interest Disclosure (Whistleblower Protection) Act).

Under PHIA and FIPPA, the ombudsman investigates complaints from people who have concerns about any decision, act or failure to act that relates to their requests for information from public bodies or trustees, or a privacy concern about the way their personal or personal health information was handled.

The ombudsman has additional duties and powers under FIPPA and PHIA, and these include:

- conducting audits to monitor and ensure compliance with FIPPA and PHIA
- commenting on the implications of proposed legislation or programs affecting access and privacy rights
- commenting on the implications of the use of information technology in the collection, storage, use or transfer of personal and personal health information
- informing the public about FIPPA and PHIA and receiving comments from the public

In light of these duties and powers, and as a result of the concerns expressed to our office from affected individuals, Manitoba Ombudsman determined the need for a systemic investigation into the CDS privacy breach. The authority for the ombudsman's investigation of the CDS privacy breach is found under part 4 of PHIA within clause 28(a), under which the ombudsman may conduct investigations to ensure trustees comply with the act:

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;

In addition to over 30 intake inquiries, our office also received four formal privacy complaints from individuals whose children were directly affected by this breach under subsection 39(2) of PHIA:

Right to make a complaint about privacy

39(2) An individual may make a complaint to the Ombudsman alleging that a trustee

(a) has collected, used or disclosed his or her personal health information contrary to this Act; or

(b) has failed to protect his or her personal health information in a secure manner as required by this Act.

We investigated these individual complaints simultaneously and this report serves as an outcome to those families.

The purpose and scope of the ombudsman's review of the CDS privacy breach

In our notification to the minister of families, we committed to investigating the following:

- The details, scope and circumstances giving rise to the breach reported on August 26, 2020.
- The dates and details of any breaches of the same information which occurred prior to August 26, 2020.
- The actions taken by the department to investigate, contain and respond to the privacy breach(es).
- The measures taken by the department to limit the disclosure of personal health information in accordance with sections 20 and 22 of PHIA.
- The measures taken by the department to adopt reasonable security safeguards to protect the sensitive personal health information of Manitobans, in accordance with its responsibilities under sections 18 and 19 of PHIA and sections 2-8 of the Personal Health Information Regulation. This includes review of security safeguards (privacy policies and procedures, training, and pledges of confidentiality) implemented by the department to assist CDS staff in their day-to-day handling and transmission of sensitive personal and personal health information of their client populations.
- Additional measures taken by the department or CDS to prevent future privacy breaches.
- Gaps or areas of concern regarding departmental compliance with PHIA if revealed in the course of investigation.

Methodology

The investigation into the CDS privacy breach included completion of over 20 interviews; a review and analysis of all the concerns raised to our office by citizens, and all correspondence received from the department about the privacy breach. We examined the format and type of personal health information at issue in this matter, and considered the audit results of the emails leading up to and at the time of the privacy breach. Previous ombudsman privacy investigation files related to the department were also considered. The team reviewed the department's policies, procedures, and the content of orientation and training. For complete details of the investigation methodology, please see Appendix 3.

Manitoba Families, Community Service Delivery Division and disability programs

This report will refer to Manitoba Families or the department, which includes the divisions and program areas involved in the privacy breach and responsible for actions taken to address and prevent a recurrence. It is important to clarify the service roles and responsibilities of these various departmental structures. The following is a brief description found on the department's website: ¹

The Department of Families is responsible for a wide range of programs and social services that are delivered by the Department, or by community-based partner organizations.

The Community Service Delivery (CSD) division delivers many of the Department's programs through a province-wide network of community-based offices.

The division helps adults with intellectual disabilities to live and participate in the community through Community Living disAbility Services (CLdS), which includes funding and supports for residential services, day services, and transportation. The division helps children with disabilities, their families and caregivers through Children's disAbility Services (CDS), and provides funding for the Children's Therapy Initiative, early intervention autism services, and external agencies that deliver specialized services.

The Corporate Services division provides centralized internal services to the Department in the areas of corporate services, accessibility, legislation and strategic policy, intergovernmental relations and information services. It is also accountable for the effective operations of the Adult Abuse Registry Committee and supports three independent offices: The Social Services Appeal Board, the Fair Practices Office, and the Office of the Vulnerable Persons' Commissioner. The division also houses the Disabilities Issues Office (DIO), responsible for supporting the implementation of The Accessibility for Manitobans Act. The DIO supports the Accessibility Advisory Council and works with community organizations to improve accessibility and inclusion for Manitobans who are disabled by barriers.

The Manitoba Families organizational chart can also be found in Appendix 5.

The community-based partners, funded by the province of Manitoba, noted in the description above are those external agency service providers referred to in this report. These agencies provide support, respite, residential services and a range of resources for families of children

¹ <https://www.gov.mb.ca/fs/about/index.html#csd>

with disabilities. It is these agencies, along with those that provide services to adults with disabilities and some community advocates, that received the email with personal health information of CDS clients on August 26, 2020.



LEGISLATIVE CONTEXT

The purpose of the Personal Health Information Act

A privacy breach occurs when there is unauthorized collection, use, disclosure or disposal of personal or personal health information. Such activity is “unauthorized” if it is not permitted by the Personal Health Information Act (PHIA) or its companion legislation, the Freedom of Information and Protection of Privacy Act (FIPPA).

All privacy laws are based on internationally recognized principles or fair information practices.² These principles are based on accountability, identifying purposes, consent, limiting collection, limiting use, disclosure and retention, accuracy, safeguards, openness, individual access and challenging compliance. Reference to these principles can be found throughout this report.

PHIA is a health privacy law that sets rules and governs the handling of personal health information. The act describes those that collect and maintain personal health information as trustees. Trustees have a responsibility to protect the privacy of those whom they serve. PHIA also requires trustees to protect personal health information by adopting reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information.

Manitoba Families, including all of its service delivery programs such as CDS, is a public body under FIPPA and all public bodies who hold personal health information are also trustees under PHIA. PHIA defines these terms as follows:

"trustee" means a health professional, health care facility, public body, or health services agency that collects or maintains personal health information.

"public body" means a public body as defined in The Freedom of Information and Protection of Privacy Act, and for the purpose of this definition, the definitions of "department", "educational body", "government agency", "health care body", "local government body" and "local public body" in that Act apply;

External organizations provide services on behalf of a public body, and by legal agreement are obligated to comply with the PHIA requirements for the protection of privacy and the

² See Appendix 4, Fair Information Practices

collection, use, disclosure and security of personal and personal health information. A discussion of the privacy obligations of service providers who extend services under contractual agreement with the province of Manitoba and the government responsibilities for privacy management of these service providers follows in a later section of the report, *Privacy laws and government-funded external service providers*.

PHIA: applicable sections

In order to report on our analysis of the evidence gathered and our investigation findings, it is important to identify the relevant provisions of PHIA that were considered in our review. This section of the report is also intended to explain, in plain terms, what these provisions mean for the protection of personal health information.

Defining personal health information

Personal health information is broad in scope and can vary in type and sensitivity. PHIA defines personal health information as follows:

"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**, (emphasis added)*
- (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*

The information sent in error to unintended recipients by CDS included the child's name, gender, date of birth, address, along with the nature of their disability and dates and types of medical or psychological assessments. This is information that relates to the child's health and health-care history and in some cases may be genetic information. This is, therefore, personal health information under PHIA.

Further discussion of the format and type of personal health information disclosed in this case follows later in the report.

Obligations for trustees: authorized disclosure

PHIA places controls on how and when trustees, like Manitoba Families, may collect, use and disclose personal health information. As the CDS privacy breach involves the sharing of personal health information with organizations outside of government, this is referred to as disclosure. PHIA permits the disclosure of personal health information only when authorized and limits the disclosure to the minimal amount of information necessary to accomplish the purpose for which it is disclosed under section 20 of the act:

General duty of trustees re use and disclosure

20(1) A trustee shall not use or disclose personal health information except as authorized under this Division.

Limit on amount of information used or disclosed

20(2) Every use and disclosure by a trustee of personal health information must be limited to the minimum amount of information necessary to accomplish the purpose for which it is used or disclosed.

What these provisions mean is that health records cannot be shown to anyone outside of the trustee who maintains that personal health information, unless for a specific and authorized purpose under PHIA. It also means that even if sharing the health information is authorized or permitted under the act, the trustee must share as little of that health information as possible to achieve the purpose.

It is clear, in this circumstance, that there was no authorized purpose for the disclosure of the aggregated health information of 8,900 children to agency service providers or community advocates, all of whom received the data in error. This is why the release of this information about the children is considered a breach of privacy under PHIA.

Authorization for disclosure can be established in a number of ways, first through the consent of the individual the personal health information is about, under clause 22(1)(b) of PHIA:

Individual's consent to disclosure

22(1) Except as permitted by subsection (2), a trustee may disclose personal health information only if
(b) the individual the information is about has consented to the disclosure.

PHIA also sets out a number of circumstances where disclosure can happen without consent under subsection 22(2) of the act. The provision that is relevant in this situation, clause 22(2)(o), permits a trustee to disclose personal health information when another law or enactment authorizes or requires the disclosure:

Disclosure without individual's consent

*22(2) A trustee may disclose personal health information without the consent of the individual the information is about if the disclosure is
(o) authorized or required by an enactment of Manitoba or Canada.*

The Advocate for Children and Youth Act, which mandates the powers and duties of the Manitoba Advocate for Children and Youth (MACY), is such an enactment. A description of MACY, the context for the advocate's operational review of CDS, and the legislative authority for the CDS disclosure of personal health information to that office will be discussed later in this report.

The obligations of trustees to ensure security safeguards

PHIA also directs trustees to ensure the security of the personal health information under subsection 18(1) of the act:

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.

The specific requirements for these security safeguards are set out under the Personal Health Information Regulation:

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.*

Orientation and training for employees

6 A trustee shall provide orientation and ongoing training for its employees and agents about the trustee's policy and procedures referred to in section 2.

Pledge of confidentiality for employees

7 A trustee shall ensure that each employee and agent signs a pledge of confidentiality that includes an acknowledgment that he or she is bound by the policy and procedures referred to in section 2 and is aware of the consequences of breaching them.

Our review of the security safeguards of Manitoba Families in place at the time of, and subsequent to, the privacy breach can be found on page 38 of this report.

The Manitoba Advocate for Children and Youth (MACY)

We noted earlier in this report that the privacy breach occurred in the course of CDS responding to an information request from MACY.

MACY is an oversight body responsible for reviewing and investigating “designated services” under section 1 of the Advocate for Children and Youth Act, provided to children, youth, young adults, and their families. Like the ombudsman, the advocate is an independent officer of the Legislative Assembly of Manitoba. Further details of the advocate’s office, her role and mandate can be found on her website.³

None of the officers of the legislative assembly (the ombudsman, the advocate, the auditor general, the chief electoral officer, the information and privacy adjudicator and the conflict of

³ <https://manitobaadvocate.ca/>

interest commissioner) are subject to the provisions of PHIA as these offices are not trustees of personal health information under that act or public bodies under the Freedom of Information and Protection of Privacy Act (FIPPA). While not subject to Manitoba's privacy laws, it is our opinion that all public sector organizations, regardless of mandate or governance, should embrace and adhere to the privacy principles referred to at the beginning of this report.⁴

To understand the context of the privacy breach and the sequence of events leading up to it, it is first necessary to understand the reasons why detailed program information was being provided by CDS to MACY. We invited the advocate to provide us with her comments for our report, on the purpose for the MACY operational review of CDS. In a letter to our office on December 14, 2020, the advocate stated:

The Advocate's review has emerged from stories of children and youth who have struggled to access appropriate disAbility services, including stories of children who have died while receiving services or waiting for disAbility services that met their needs.

A review of a child death under Part IV of the ACYA (The Advocate for Children and Youth Act) informed the launch of an investigation under part IV and a special report under Part V of the ACYA, which included a systemic review of the children disAbility services.

The Advocate is studying and analyzing how these systems currently work for children and youth in Manitoba, with the goal of providing recommendations to the government in order to improve the effectiveness and responsiveness of services for children and their families.

In the early days following the privacy breach, some of the callers to our office questioned CDS' authorization to disclose the personal health information of clients to MACY without the consent of those individuals who the information was about. The advocate provided us with the following explanation of her statutory authority to collect information under the Advocate for Children and Youth Act (ACYA):

The following sections of the ACYA governs access to information from a plain language perspective:

*Section 17(1) - provides the Advocate with the right to obtain any information--including **personal information or personal health information** necessary to enable the Advocate to carry out responsibilities under the ACYA (section 11(1(b))). (emphasis added)*

⁴ See Appendix 4, Fair Information Practices.

Section 17(2) - Despite any other provincial legislation (including PHIA), any person receiving a request for information is under a duty “to provide the Advocate with the information and assistance that the Advocate requires.”

Among the designated services under the advocate’s authority, Children’s disAbility Services (CDS), would therefore be required to comply with a request for information made by the independent officer as the subject of a review in accordance with MACY’s legislation.

As we note in our discussion of the relevant provisions of PHIA, clause 22(2)(o), allows a trustee to disclose personal health information when another law or enactment of Manitoba, such as the Advocate for Children and Youth Act, requires the disclosure.

While clause 22(2)(o) provides authorization for the disclosure to occur, trustees must still consider how much personal health information is necessary. Subsection 20(2) of PHIA directs trustees, such as CDS, about the requirement to limit the amount of personal health information to that which is necessary for the purpose of the disclosure.

In our discussions with CDS, we heard about the preliminary meeting held on June 24, 2020, between MACY staff, CDS staff and department leadership, to consider the nature and format of information held by CDS that would be required for MACY’s operational review. Such a meeting helped to ensure that the information requested by the advocate, and disclosed by CDS, was limited to the amount and type of personal health information and related data necessary for the purposes of the operational review. MACY provided us with the following summary for inclusion in our report to explain the goal of the meeting and to explain the basis for the decision to include person-based, non-anonymized personal health information in the data requested for review:

The objective of this meeting (on June 24, 2020) was to communicate our process, the scope of our review, and understand how they collect information in order to develop the information request. This meeting was essential for assessing information requirements in compliance with Section 17(4) of the ACYA.

At this meeting, CDS staff reported relevant changes in operations over the last five years. Due to information provided it was determined that a short view would not give us an accurate depiction of the data. This is particularly important also since information reviewed through the investigation is historical and findings might not accurately reflect current practices. The five-year scope of the review was required for the development of relevant and effective recommendations.

The tracking of children that transition from CDS to CFS is an important component of this review and it was discussed at this meeting. It was stated that the information in the

InFACT database (information management system at CDS) is not reliable, and that CFSIS (the information management system at CFS) and inFACT are not connected in a systematic way, for instance through a common code or case file number that would allow for analysis of anonymous data. Following this meeting, it was apparent that in order to identify people in both systems personal information would be needed to understand the extent of the overlap between the two systems (names, addresses, and dates of birth). ⁵

Any references to MACY in this report are made solely to explain the events leading up to the privacy breach or to establish the context for the actions of CDS. Any findings, conclusions or recommendations in this report do not pertain to the advocate.

We must also emphasize that while the CDS privacy breach occurred in the course of transmitting requested information to MACY (as will be discussed in detail in a subsequent section of this report), the error in disclosing the requested information to agency service providers and community advocates was not caused by MACY.

⁵ MACY correspondence to ombudsman, December 14, 2020



INVESTIGATION

The events leading up to and including the privacy breach

The timeline leading up to and including the privacy breach of August 26, 2020, is based on the formally submitted privacy breach report received by our office on September 10, 2020, consideration of the internal audit conducted by the department, our own review of 200 email messages, and interviews with CDS and departmental leaders. Please see the chart below for a depiction of the relevant dates and events from June 24, 2020 to August 26, 2020.



Variables impacting the breach

In reviewing this incident, there is no question that the August 26, 2020, sharing of client personal health information with agency service providers and community advocates was an unintended administrative error. This accident, however, emphasizes the obligations of all trustees who collect and maintain highly personal and sensitive details of individuals, in this case vulnerable children and youth. Our primary goal is to understand how the accident occurred and to assist the department to identify and implement improvements to prevent it from happening again.

The pandemic

In August 2020, Manitobans were enduring the health crisis brought on by the COVID-19 virus, numbers of cases were rising and there was increasing concern about transmission of the virus in congregated living settings. Plans regarding the coming school year were being formulated, and families with children in receipt of CDS services, and the support services for those families and children were significantly impacted by a situation in constant change. We were advised that timely and detailed updates, guidance and COVID-related physical management strategies for the agencies and services that provide supports on behalf of CDS and Community Living disAbility Services (CLdS) were imperative. This was the environment described to us in our discussions with the department.

Blind carbon or courtesy copying

With the onset of COVID-19 in March 2020, we heard that CDS began to use the practice of blind copying (bcc) their roster of agencies and disability community advocates, to quickly disseminate critical information about COVID-related matters of concern regarding children with disabilities.

We were advised by CDS that in August 2020 frequent updates and general information about COVID-related matters were still needed to inform the large group of agencies and community advocates providing services to CDS clients. This was also the month that the clusters of data requested by MACY was due. From all explanations, it appears that in the volume of information required for each of these distinctly separate email tasks, the lists of recipients for the agencies and community advocates and MACY were confused, resulting in the blind copying of the wrong recipients on the data meant solely for MACY.

Organizations use blind copying for two reasons. It protects an email recipient from knowing the identity of others as the recipient cannot see the names of others who were blind copied. It

is also used in cases where there are a large number of recipients, to prevent an email recipient from accidentally clicking reply all, setting off an unmanageable volume of email.

When blind copying, it is only the sender who can see the recipients that are blind copied on an email. The risk is that if there is an error in the recipient list, there is no one else who can see that there are unintended recipients on an email once it is sent. Such is the case in this circumstance. Department leadership copied on the email were unable to see there were also unintended recipients blind copied.

Early warnings

The privacy breach that occurred on August 26, 2020, was not the first administrative error in this case involving email to the same list of unintended recipients.

A transmission of information on August 13, 2020, was also blind copied to service providers and community advocates. In this instance, the email did not contain personal or personal health information. Multiple investigations by the program and the department, reviewed later by our office, concluded that the information sent to the agencies and community advocates on that date included only policies and an informational circular.

Our investigation noted the number and timeliness of attempts to recall the emails sent in error on August 13. As depicted in the timeline on page 21, messages were received by the sender that indicated the recalls failed and yet others that indicated success. This would be confusing to the individual sending the requests for recall to know with certainty that the problem was fixed.

We found that there was no breach of privacy of personal health information on August 13, 2020, and that Manitoba Families exercised due diligence in investigating the emails sent on this date to rule out a possible privacy breach on that date.

From our review of the events of this date, although the use of blind copying would have prevented senior leaders at CDS and Manitoba Families from seeing that the agency service providers and community advocates were copied in error, they did receive the subsequent and numerous recall messages. Management from CDS were also copied on an email from a service provider sent at 11:39 a.m. on August 13, in which the agency director advised of receiving email that they were concerned about. The recall messages and the email received from an agency almost immediately after 11:35 a.m. alerting to the misdirected email of the MACY data, should have been a red flag that information was sent to the wrong people in error, albeit that no personal health information was disclosed.

We find that this represented a significant missed opportunity, on or shortly after August 13, for program management to identify and stop the blind copying of the agency service providers and community advocates on email messages sent to MACY. If identified and corrected, it may have prevented the error from recurring on August 26, resulting in the unauthorized disclosure of client personal health information on that later date.

We wish to acknowledge the service providers who reacted quickly and contacted CDS within minutes alerting the program to the email received in error at 11:35 a.m. on August 13.

We note that all the messages sent in error were confidential. On August 13, the program should have instructed the recipients that the messages were confidential, sent in error and should immediately be deleted, rather than instructing recipients to just disregard the errant email. CDS' later messages to the agency service providers and advocates when the breach occurred, advising of the error in sending the confidential information, with the instruction to immediately delete the email and attachments, was a clearer and more appropriate response.

The use of passwords

The Manitoba government's Information Security Centre intranet website guides employees on general use of passwords and encryption. Comments about creating strong passwords, limiting the sharing of passwords and methods by which to encrypt documents and email for transmission are included. The intranet site also contains a 2012 policy, *Data Classification Guideline*, which guides employees on determining the level of risk involved with disclosure of the information they are working with.⁶

The password to the encrypted data was sent via email to the same recipients on August 26 as in the August 13 email. However, it is important to note that the password to gain access to the email meant for the advocate was appropriately never sent in the same email with the encrypted attachments in the email sent on August 26, 2020. The department created policy on emailing (specifically for programs under Community Service Delivery) in November 2020, after the occurrence of the breach, noting that passwords can be sent over the telephone if there are not a volume of receivers. Were that method to have been used in this case, the privacy breach of August 26 may have been prevented. None of the unintended recipients would have been called and given the password to open the encrypted files and the risk of unauthorized disclosure would have been mitigated.

⁶ <http://intranet.mbgov.ca/btt/information-security/Pages/Encryption>

The use of the original email to send or forward

We reviewed the emails sent from August 7 to August 26, 2020, about the MACY request. We observed the frequency in which an original email of June 30, 2020, to MACY (also copied to Families and MACY management) was used to forward the subsequent email messages and data sets throughout the month of August. The department advised us that this is a common practice used to provide intended recipients the original context for the communication.

The program's use of the original email as the "base" would make it less likely that further verification of the correct recipients occurred before pressing send. Once the emailing errors were made, as noted above, a series of recalls were attempted which would have made the volume of email to be considered overwhelming.

The result of using the original email to MACY was that agency service providers and advocates who were blind copied on both August 13 and 26, 2020, would have viewed the email and email addresses of MACY staff with respect to the operational review. We note that this type of correspondence between independent offices and the departments under their jurisdiction is confidential and protected under legislation.

Bulk disclosures

Previous investigations by the ombudsman involving other trustees have commented on the practice of bulk disclosure.⁷ We have noted that bulk disclosures of highly sensitive information and/or disclosures made to non-trustees should be carefully considered by a trustee. Trustees that are larger institutions generally have experience with respect to such disclosures particularly when disclosing for research purposes. In our discussions with the department, we were advised that the advocate's request was reviewed by other divisions of Manitoba Families from a legal and privacy perspective as the department did not have a protocol for the disclosure of information which applied in this circumstance. We understand that the decision regarding specific contents of the data and the method of transmission were provided to CDS by MACY under her legislated authority. In view of the requirement for this bulk disclosure, CDS informed us that going forward, they would follow the protocol issued by MACY in October 2020 (see page 36 for a further description of this security safeguard) because it sets out a revised process for CDS to ensure security of all data, including personal and personal health information, during transport to the independent office.

⁷ <https://www.ombudsman.mb.ca/uploads/document/files/case-2017-0143-en.pdf>

Manitoba Families' response to the CDS privacy breach

When a privacy breach occurs, our office expects trustees to take swift action in response. To assist trustees, our office has published a practice note titled *Key Steps in Responding to Privacy Breaches*.⁸ This guidance document outlines four key steps: containing the breach, evaluating the risks associated with the breach, notifying affected individuals and preventing a recurrence.

We considered the actions taken by Manitoba Families, Community Service Delivery (CSD) Division and CDS following the privacy breach in relation to these key steps.

Containing the breach

The first and most critical step following a privacy breach of personal or personal health information is to take all measures to “re-secure” the information that has been disclosed and to prevent further disclosure. This is commonly referred to as containment.

As noted previously, the privacy breach of August 26, 2020, occurred at 8:11 a.m. when one email with two attachments containing detailed personal health information of 8,900 clients of CDS was blind copied to agencies and community advocates in error, along with the password to the attachments which was sent in a second email. Attempts at recalling the email began minutes later at 8:29 a.m. and continued at various intervals. Also, at 8:35 a.m., CDS sent an email to all unintended recipients noting in bold that they were incorrectly included on a confidential email from Children’s disAbility Services and requested immediate deletion of the email and any attachments. Follow up calls to the unintended recipients by CDS program staff began to occur that morning to request deletion of the emails and a list was created to track these calls and the outcomes. A communication outline was created for these calls which included a request to delete emails, a further request that emails be deleted from the deleted folder and that any emails that went to a junk email folder also be deleted.

Based upon the calls and complaints our office received from individuals affected by the privacy breach, there was great interest in understanding what was done with the personal health information that was received in error. We wrote to Manitoba Families on December 17, 2020, to seek a further update on the actions taken to secure the personal health information disclosed on August 26, 2020. In a formal reply to our office, the department stated:

Immediately following the breach, CDS called all agency and advocate groups directing them to delete the unauthorized emails. CDS found most

⁸ <https://www.ombudsman.mb.ca/uploads/document/files/practice-note-keys-steps-in-responding-to-privacy-breaches-2018-en.pdf>

agencies and groups had already adhered. A few smaller agencies/offices were closed due to staff summer vacation. CDS followed up with them a week or two later when the offices re-opened.

In late September/early October, CDS leadership reached out again to agencies via Abilities Manitoba. This was to ensure emails that may have been sent to the agency mailbox and/or forwarded to another email account due to staff coverages at agencies were also completely deleted from computers.

In January 2021, we received additional written communication from the program stating that all agency service providers and advocates were contacted and verified deletion of the personal health information received in error. The log form created to track and monitor the name of the organization, the date and details of the contact was provided to our office.

Agencies were also the first to alert CDS to the error. In the letter sent to affected families, the department clarified that most of those who received the personal health information in error provide services on behalf of CDS and CLdS and therefore would be aware of their legal/contractual obligations to protect personal health information.⁹ We find that the actions of CDS in contacting the agencies and community advocates, to ensure that full deletion of the emails had occurred, were timely and complete.

In the course of our investigation, we had many discussions with the department about the two continuing worries of families who were directly affected by the privacy breach – not knowing who received their child’s health information and what was done with it. Families who called our office expressed concern about not knowing whether their child’s health information could ever be fully “erased” off the recipients’ computers, and their frustration was whether this information could be accessed years in the future and cause reputational harm or difficulty for those children as adults. These fears are understandable. While it is unlikely the health data disclosed will be accessed, it is impossible to be completely assured that this cannot occur.

“I want to ensure that my child’s information is not used or leaked to the public...I am worried about what this means for her future.”

In addition to assuring families about the deletion of the email, additional information such as who viewed the email, if the attachment was opened and read, whether it was forwarded to anyone else or printed, whether it was stored in any other network drive or paper file or,

⁹ See *Privacy laws and government-funded external service providers* on page 45

conversely, that no records exist – can be helpful information to provide those affected by a privacy breach. It is best practice, therefore, to provide families with as much assurance as possible about the security of their child’s health information.

We shared the above noted elements to CDS as examples of further considerations when assuring individuals of the security of their personal or personal health information following a privacy breach. The program advised us of their continued commitment to the children and families they serve including monitoring and responding to any individual additional concerns about the containment measures taken.

Evaluation of risk

Before making decisions regarding notification of the affected individuals, the public and others, a trustee must evaluate the risks of the personal health information that was disclosed in a privacy breach. This evaluation could include determinations about the sensitivity of the health information disclosed, the impact on those to whom the information belongs, whether the disclosure may result in physical harm or further emotional distress, criminal or fraudulent activity, the number of affected individuals and whether the disclosure was accidental or deliberate, for example in the case of a ransomware attack. All of these factors impact the assessment of the risk associated with a privacy breach.

Our office provides a matrix for trustees and public bodies to help them make determinations regarding the risk incurred following a privacy breach, which in turn guides the decision of whether to inform those affected and others.¹⁰

We find that Manitoba Families fully considered all relevant factors in its evaluation of risk including the vulnerability of those affected and the volume of those whose privacy was breached.

Notification

Informing affected individuals when there has been a breach of their privacy should always occur if it is necessary to avoid or mitigate harm to them. There may be other factors that influence a decision to notify individuals, such as wanting to be transparent about the breach.

An individual whose privacy has been breached through an unauthorized collection, use or disclosure of personal or personal health information may also be in the best position to better inform a public body or trustee of the risks related to that breach. Notification can also be a

¹⁰ <https://www.ombudsman.mb.ca/uploads/document/files/practice-note-keys-steps-in-responding-to-privacy-breaches-2018-en.pdf>

first step in helping to restore an affected individual's confidence that their personal or personal health information has been secured and renews public trust.

As of the date of this investigation report, mandatory reporting of privacy breaches to the ombudsman is not currently the law in Manitoba.¹¹ Our office, however, encourages this practice when there is a risk of harm, the information disclosed is sensitive and/or there are a significant number of affected individuals. To assist trustees and public bodies, we have developed a privacy breach reporting form, which can be found on our website.¹²

Manitoba Families proactively and voluntarily notified our office of the CDS privacy breach on August 26, 2020, the same date on which the breach occurred and the department and CDS provided frequent and detailed updates thereafter including completion of a privacy breach reporting form.

The department advised us of a number of strategies to notify those individuals directly affected by the breach or their parents or guardians, in addition to a public notice to all provincial citizens. On August 28, 2020, within two days of the privacy breach, notification began as follows:

- A provincial public media release described the circumstances of the breach, the type of information involved and the types of organizations who received the personal health information in error. The release assured the public that no financial, social insurance or health numbers were in the disclosed information, that the spreadsheet was password protected but that a password was disclosed, the actions taken to date to delete, and other details. The bulletin noted that all affected families were being contacted directly. The bulletin also advised of a report to the ombudsman. A second media release following on September 10, 2020, following the announcement of the investigation by Manitoba Ombudsman.
- Affected families were contacted by phone and the calls were followed by a letter, which included similar information and provided a phone number and email address for further questions.

¹¹ As of the release of this report, there are proposed amendments to PHIA and FIPPA that would require the reporting of privacy breaches. These are contained in Bill 54, The Personal Health Information Amendment Act and Bill 49, The Freedom of Information and Protection of Privacy Amendment Act, which are currently before the legislature and have not yet been passed into law.

¹² <https://www.ombudsman.mb.ca/breaches/privacy-breach-reporting-form.html>

- The letter to families, a questions and answers fact sheet, a description of MACY and the reason for the request of the personal health information, and a contact number for the ombudsman were posted on the CDS website as resources for families.¹³
- CDS immediately established a full-time staffed and dedicated phone line to receive calls and questions about the privacy breach. We were advised that the deployment of a staff member to respond to phone calls continued until September 30, 2020. In our discussions with CDS they noted that this was set up with the intent that a CDS representative would always be available to receive, or quickly return, calls about the privacy breach. The program also noted that this allowed existing program staff and service providers to continue to deliver needed services to clients and families. CDS also informed us that the special phone line continued to be monitored by program staff until January 21, 2021, when no further calls about the privacy breach were being received.

In the course of our contact with CDS during this period, we advised the program that following any privacy breach, it was not unusual for affected individuals to contact the trustee or public body asking to receive copies of their own actual personal health information that was involved in the privacy breach. Responding to such requests is a best practice as it can provide further assurance to affected individuals when they are able to view their specific personal health information which has been disclosed. We note that the following actions were undertaken:

- CDS prepared a further letter of explanation for families who requested more information about the information disclosed and also responded to requests from adults who received CDS services as children, or parents or guardians of children who currently or previously received CDS services, who asked to obtain their child specific health information involved in the breach. Following verification of identity and guardianship status, we were advised that the identifying personal health records disclosed in the privacy breach were securely sent to affected individuals who made a specific request.

All samples of the letters and communications with families were provided to our office in the course of this review.

CDS also sought feedback to check on the types of concerns raised by individuals who contacted our office and the perceived effectiveness of the notification activities undertaken.

We find that Manitoba Families' and Children's disAbility Services' notification actions were fully-considered, thorough and responsive to many of the concerns raised from the affected

¹³ https://www.gov.mb.ca/fs/cds/privacy_breach.html

individuals, families and the public. The department considered the sheer volume and vulnerability of those affected by the breach when using various methods to both notify and keep families informed. These actions demonstrated that the department took the privacy breach and its impact on affected children and their families very seriously.

Our review noted one exception to the immediate responsiveness of the department, regarding release of the names of the agency service providers and community advocates.

The recipients of the personal health information sent in error – agency service providers and advocates

As we noted earlier, the primary concern we heard from families was not knowing who received their child's health information and what was done with it. Despite the fulsome description by CDS that the recipients were agency service providers and community advocates and that most have legal service agreements to provide services on behalf of CDS and Community Living disAbility Services (CLdS), it appears from those who contacted our office, that the uncertainty of knowing precisely which organizations or individuals received their child's personal health information is a source of stress for families. Many of these concerned families have described this as the one remaining piece of information that would provide them with closure over this incident and that the decision by the department not to divulge the names caused those affected to speculate about the exact organizations involved.

This was a key area of focus in our investigation. We requested a list of the names and email addresses of those agencies and community advocates who were recipients of the "breached" personal health information of CDS on August 26, 2020. Our review noted 114 agencies and community advocates, divided into the following categories:

- Community advocacy groups (12)
- Service providers funded to provide services to children with disabilities (6)
- Service providers funded to provide services to adults with disabilities (94)
- Service providers funded to provide services to both children and adults with disabilities (2)

CDS clarified that the community advocates are key stakeholders in the disability community with whom they consult on issues, trends or possible options for future services.¹⁴

¹⁴ These community advocates are separate and unrelated to the Manitoba Advocate for Children and Youth (MACY), who has statutory authority as advocate under the Advocate for Children and Youth Act.

With regard to notifying affected individuals and their families of the names of these services and advocates, we advised CDS of the above-noted concerns of those who had contacted our office. It was our position that CDS should provide the names of the organizations to those directly affected by the privacy breach that wanted that information.

In our discussions with CDS, we heard of the struggle with wanting to support their clients and families by providing the names, but at the same time observing the demands and stresses on their service providers and not wanting to inflict more with the possibility of having to receive many calls from the public about the breach.

Our office monitored the position of the department in this matter and inquired about any changes throughout the months following the breach. Within our office, we considered the list provided and determined that most of the 114 names are funded service providers with legal service purchase agreements (SPA) signed with the province of Manitoba to provide services on behalf of CDS and/or CLdS. We examined portions of the service purchase agreements related to confidentiality and the protection of personal and personal health information, in particular the appendix to the agreement.¹⁵ While not directly subject to FIPPA and PHIA, service providers who are not trustees under the act must comply with the requirements of the privacy statutes for the Manitoba government, including protecting personal and personal health information collected, used or disclosed in the course of serving the public, in agreeing to provide services on behalf of the government.

We also considered that the names of funded service providers are published annually in the vendor payments related to public accounts.¹⁶ It is our view that many of the names of the providers are, therefore, in the public domain and would also be known to many of the affected individuals and families. While we acknowledge and respect the worries of the agencies about their ability to manage inquiries about the privacy breach, our office believes that the interests of citizens must be paramount. Governments must make decisions on behalf of those they serve with the perspective of fairness and transparency. Advising affected individuals of the names of the organizations who received their personal health information disclosed in error can help allay fear and worry about the intentions of the unintended recipients and would be best practice.

As a result, for the reasons noted above, we strongly urged Manitoba Families to reconsider their position regarding the release of the agency and advocate names and requested a formal written response. On January 11, 2021, we received the department's details of planned

¹⁵ See Appendix 2

¹⁶ <https://www.gov.mb.ca/government/finances/print,annualreports-publicaccounts.html>

discussions with the agencies and the timelines for a plan to make available the agency and service provider names to affected families who request the information through the CDS website. Updates to the CDS website with directions for individuals to obtain access to the agency and advocates names were implemented on February 18, 2020.¹⁷ The website summary stated:

The Department of Families has worked closely with the Ombudsman during the investigation regarding the email that was sent in error in August 2020, to ensure that recommended steps are taken in response to the breach and towards implementing additional safeguards. The Children's disAbility Services program and the Department take all privacy issues seriously, and implement reasonable measures to prevent similar mistakes from happening again.

As a response to the recommendation from the Ombudsman and request from families impacted by the email that was sent in error in August 2020, the Department will provide to parents, upon request, the list of agencies and advocacy groups who mistakenly received the email. Please contact ADS@gov.mb.ca for next steps.

The written response to our office also noted that the agencies and advocates would receive prepared information from CDS to assist them in responding to any calls from affected families.

It is our office's approach, whenever possible, to assist public bodies and trustees to resolve issues informally. We acknowledge the department's collaboration with its agencies and advocates to resolve this matter that resulted in the decision to release the names of these organizations. We are hopeful that the availability of these names brings some closure for the impacted families. Our office will continue to encourage families to forward their concerns and questions about the privacy breach to the department, the trustee responsible for the emailing error, reserving contact with the agencies for service related inquiries to avoid service disruption.

The personal health information disclosed in the privacy breach

In the Q&A on the CDS website, the program described the personal health information disclosed about 8,900 children served as follows:

The attachment in the email contained your child's name, address, date of birth, gender, first language, region of the province, case worker's name, the assessment type (for example, neurodevelopmental, Child Development Clinic, Newborn Follow-up Program),

¹⁷ https://www.gov.mb.ca/fs/cds/privacy_breach.html

the source of your child's referral to Children's disAbility Services (physician, parent, school) and if applicable, the date of and reason for program closure. If applicable, the attachment also contained services that your child or family received during the years of 2015-16 to 2019-20, including respite, after school care, summer skills maintenance, equipment and supplies, behavioural psychology and child development. The name of the diagnosis was only included for children who received child development services in Winnipeg.

In our investigation of this matter, we requested and viewed all of the types of personal health information disclosed in the privacy breach. It is important to state that at no time did we examine the identifiable personal health information of any CDS service recipients and took all measures to ensure that this information remained protected by the program. Like those affected, however, we sought to understand the nature of the personal health information at issue.

At our request CDS provided the data spreadsheets describing the type of personal health information that was disclosed in error to the agency service providers and community advocates.¹⁸ For those individuals, or their guardians, who requested copies of their own personal health information disclosed, these sheets with identifying information were provided by CDS. Our review noted that while the volume of personal health information disclosed in spreadsheets was large, there were no actual medical or assessment reports included.

We noticed that there was more information disclosed in the datasets relating to children who had received child and family services (CFS), than in those who were solely involved with the CDS program. We contacted the acting executive director of the Child and Family Services Branch and received a copy of the branch's early notification to the CFS authorities on August 27, 2020, advising them of the privacy breach for 170 children, who had received services from CFS and were deemed as eligible for CDS services. We understand that the CFS authorities later received lists of the children for their respective agencies whose personal health information was disclosed in the privacy breach. In the notification to the CFS authorities, the Child and Family Services Branch stated that the families affected had been contacted by CDS.

The notification to the CFS authorities described the more detailed data set prepared for MACY that was disclosed in the breach. This subset of personal information related to 61 children eligible for children's disability services who were admitted to a child and family service agency during the years during 2017/18 and 2018/19. We were told that this analysis was completed by the department's Legislation and Strategic Policy Branch and comprised information from both CDS and CFS programs including details of the child and their family (family status at time

¹⁸ See Appendix 1, for copies of the format of the spreadsheets

of placement, number of siblings and number of siblings in care, primary disability, indigenous); the CDS case workers' assessment of the reason for placement (protection or non-protection); factors that contributed to placement – case worker notes on the contributing factors and preceding events; placement details – date, age at time of placement, legal status, status of parent, type and number of placements, current placement, agency, whether siblings are in care, CFS notes, and CFS ID number, CDS and CFS funding amounts.

We asked to review deidentified samples of this personal health information, concerned that by description, the personal information disclosed was far greater than for the larger “non-CFS” group of CDS clients. The spreadsheets we reviewed captured lists of data fields which included those items described above, and while clearly personal and personal health information of those 61 children, there were no narrative assessment reports. We specifically asked about the portion of the information relating to factors that contributed to placement, unsure as to how this might be reflected as simply data. The samples we examined were chosen and identified by CDS as examples of the “most” amount of personal information disclosed. We noted that this field in the spreadsheet was very brief, often one or two sentences.

This is not to minimize that the information in all of this subset is a child's personal and personal health information, and reflects details about much of that child's personal, family and CFS agency history. It is important to note that personal and personal health information of children under CFS agency care, or who are receiving the mandated services of an a CFS agency, is protected under the Child and Family Services Act and disclosure of such information is prohibited by that act. The CDS privacy breach, therefore, was not solely a breach of PHIA, it also contravened the Child and Family Services Act.

In considering the unauthorized disclosure of all of the health information described in this section in relation to the definitions under PHIA, we find that the information disclosed without authorization to agencies and community advocates is clearly personal health information under the act. The information is recorded information about an individual's health, health-care history or the provision of health care to that individual. We also found that other information disclosed about identifiable children, while not health information, would be considered personal information pursuant to the Freedom of Information and Protection of Privacy Act (FIPPA) and that information about children receiving services from child and family services agencies is protected from disclosure, except in specific circumstances, under the Child and Family Services Act.

Prevention

A final consideration in assessing a trustee's response to a breach of personal health information concerns the measures that have or will be taken to prevent a similar privacy breach from happening again. In a recent investigation, the Saskatchewan Information and

Privacy Commissioner identified the fundamental questions a trustee should consider following a privacy breach:¹⁹

- Can the organization create or make changes to policies and procedures relevant to this privacy breach?
- Are additional safeguards needed?
- Is additional training needed?
- Should a practice be stopped?

Within CDS, we heard about the following steps to help prevent a recurrence of emailing errors:

The CDS Branch is now providing staff with directions when emailing personal or personal health information. For each separate email, CDS management provides a list of persons who should receive the email communication. The list of recipients ensures staff can accurately and confidently send emails to only those persons who should receive the sensitive personal and personal health information, based on privacy legislations need to know basis.

In our discussions with CDS, we also inquired about the practice of blind copying emails and were advised that this practice is no longer being used.

With respect to the transmission of information to MACY required for the purposes of her operational review of the CDS program, on October 14, 2020, the advocate informed us of the revised protocol developed by her office, *MACY Data Procedure for the Disabilities Investigation and Special Report*. The procedure requires that remaining data be provided from CDS to MACY on encrypted, password protected flash drives that are hand-delivered to the MACY office by CDS staff. CDS has advised our office that they will comply with the revised protocol established by MACY as it provides greater security for any personal or personal health information contained in the requested data. For further information about the advocate's revised data procedures, please contact MACY directly.

The department also advised that requests for information by external organizations or independent offices would be more formally reviewed by the department's privacy unit to better protect clients' personal information. In view of the minister's response to our office committing to working to ensure that appropriate safeguards are in place when the Manitoba government is required to disclose personal and personal health information to external organizations, including independent officers – this revision to practice is a critical step toward

¹⁹ <https://oipc.sk.ca/assets/foip-hipa-investigation-009-2020-053-2020-224-2020.pdf>, p.38

developing privacy practices which protect the personal health information held by the department.

We find that Children's disAbility Services has taken reasonable and appropriate measures with regard to ceasing the practice of electronic transmission of bulk disclosures of highly sensitive, personal and personal health information.

Increasing information privacy protection practices in the administration of public programs is an opportunity to strengthen and demonstrate transparency and accountability in service delivery systems.

Preventing unauthorized collection, use and disclosure of personal and personal health information, however, is far more than ensuring day to day privacy-focused administrative safeguards. Prevention includes the creation of a privacy respectful organizational culture which places the protection of personal and personal health information as a primary consideration in every facet of service. Security safeguards are a building block in the creation of that privacy culture.

The security safeguards required by PHIA are the legislative framework under which every trustee of health information in Manitoba must operate and comply. In keeping with the plan for this investigation, we wanted to fully examine what security safeguards the department had established and implemented before the privacy breach of August 26, 2020, whether the existence or absence of those safeguards impacted the breach and what safeguards have since been put in place following or as a result of the privacy breach.

In *PHIA: applicable sections*, we described the relevant legislated requirements for trustees who maintain personal health information. We noted that these security measures are set out under the act and by regulation. To reiterate, PHIA directs trustees to ensure the security of personal health information is maintained through security policies, training and pledges of confidentiality. These requirements include:

- provide orientation and ongoing training for employees and agents about the trustee's PHIA policies and procedures
- ensure that each employee and agent signs 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
- establish a written policy/procedure containing provisions for the recording of security breaches

Security safeguards: before and after the privacy breach

Security safeguards act as the strongest reminders to trustees and their employees about their obligations to guard and protect the personal health information in their custody and control. These safeguards require trustees to carefully consider the sensitivity of the personal health information that they manage on a day to day basis. Policies, procedures, practices and other safeguards minimize the risk of unauthorized access, use, disclosure, or destruction of personal health information simply by raising employee awareness. Pledges of confidentiality ensure that an employee understands and moreover, commits, to protecting personal health information.

We asked to receive comments from the department regarding what privacy resources, policies, guidance or instructions were in place for employees prior to August 2020. We were advised as follows:

. . .All Government of Manitoba employees are required to sign-off on an Oath of Office and the Oath of Allegiance or Affirmations of same, subject to the provisions of The Civil Service Act, Section 41 (a) (b) and the Civil Service Act Regulation 11. The Oath of Office is a solemn promise by government employees to discharge their duties responsibly and to refrain from disclosing any information, in any form, which may come to them by reason of their employment in the government service and includes responsibilities under FIPPA and PHIA.

Employees must ensure confidentiality of participant's personal and personal health information and protect information against unauthorized collection, use and disclosure as set out in The Freedom of Information and Protection of Privacy Act (FIPPA) and The Personal Health Information Act (PHIA). These guidelines apply when information is transmitted outside the Department. Employees are directed to follow the policies on the Business, Transformation and Technology (BTT) Information Security website, specifically, the Employee Network Usage Policy and the Guideline on Sensitive Information. Employees must adhere to appropriate safeguards, taking into consideration the levels of risk and the necessary risk mitigating measures.

The Department has a policy titled Recommendations and Privacy Considerations When Using Email. The document includes deidentifying information to the greatest extent possible before emailing the information, emailing only over the secured government network unless the attachment is encrypted, and instructions on how to encrypt email attachments.

We also reviewed the 34 privacy breach reports from Manitoba Families (and its departmental predecessors) received by our office from 2005 to present. While perhaps not significant from the viewpoint of the span of 16 years, any reported privacy breach causes us to consider the state of the trustee's security safeguards. The delayed implementation of the statutory security requirements required under PHIA by Manitoba Families' has been the specific subject of commentary in a number of investigation files relating to these breach reports.

In a 2008 investigation we concluded that the department had made substantial progress in developing PHIA policies. While we relied on the department's stated commitment to completion and implementation of the PHIA policies, we subsequently discovered that these policies were never implemented. During a privacy breach investigation of Families that began in 2017, the department later developed a PHIA policy framework dated July 2018. We found, however, that the department was not fully compliant with the PHIA regulation as it had not implemented department-wide PHIA policies, procedures, training and pledges of confidentiality. As a result, in 2019, our office opened a new systemic investigation to monitor the implementation of PHIA policies and procedures, training and pledges. This file remained active at the time the CDS breach was reported with continuing dialogue between our office and the department about its failure to implement these required minimal safeguards in order to comply with PHIA.

We asked to receive comments from the department regarding what privacy resources, guidance or instructions were in place for employees *after* August 2020. It is important to acknowledge that the department's comments above regarding the security safeguards in place before the breach continue to apply. The following information provided by Manitoba Families notes the additional measures taken immediately following the breach to increase security safeguards:

The CDS Branch has incorporated additional privacy resources on the branch's intranet website in an effort to provide readily accessible information for divisional staff and privacy related expectations.

Recognizing a detailed guideline on emailing sensitive information including personal health information was necessary, the Community Service Delivery division was in the process of developing its guideline in conjunction with BTT on external emailing (outside the secured network) when the breach occurred. The Community Service Delivery division guideline was finalized and distributed to divisional staff in November 2020. The guidelines indicate how staff determine the sensitivity level of the information and to consider the best means of transmitting the information.

We can further inform you that the Department is committed to expanding the Department-wide email guideline document, including a tip sheet, to assist staff in their day to day responsibilities.

As a result of the breach, the Department sped up its considerations related to training existing staff, and developed the privacy webinar so all Departmental employees throughout the province could partake in privacy training. A training webinar open to all Department of Families staff on privacy requirements and privacy breaches were developed and held September 9, 2020.

This training is being offered regularly to Departmental staff as indicated above. The Department's executive management committee is directing management to remind their employees about their obligations to safeguard personal and personal health information. Departmental staff are being encouraged to attend the privacy webinar

The Department requires that all staff complete mandatory training courses, one of which includes staff responsibilities on Information Security Awareness. Additionally, resources on safeguards, in particular emailing of personal information, are available for all employees on the BTT Information Security website, the Guideline on Sensitive Information, and Departmental emailing guideline.

Many safeguards, while in development, were not in place at the time of the breach. However, Manitoba Families continued to make progress in developing more safeguards and increasing its compliance with the requirements of the PHIA regulation after the breach of August 26. In October 2020, Manitoba Families provided us with a draft of the department's PHIA policies and procedures, draft PHIA pledge and a revised training module. The following section contains an assessment of the adequacy of security safeguards (policies, training and pledges) in place for CDS program employees at the time of the breach as well as the adequacy of administrative improvements made following the breach to prevent a similar occurrence and to strengthen its compliance with the legislation.

Policies and procedure manual

The department's PHIA policy on collection, use and disclosure of personal health information (2018) is a good legislative framework and instructs readers to comply with the legislation; however, detailed guidance about how these legal requirements could be put into practice and actual policy guidance was limited. The draft PHIA Procedure Manual provided to our office in October 2020, provides a broader range of guidance and direction about the management of

personal health information including sections on collection, use, disclosure, consent, retention and destruction, security and orientation and training. We observe that each section quotes departmental policy and is followed with procedural guidance. The manual also contains a section on the recording of security or privacy breaches.

As noted previously, the Personal Health Information Regulation under PHIA requires that a trustee establish a written policy/procedure containing provisions for the recording of security breaches.

In the Families' PHIA policies and procedures, under the section named *Procedures Involving Security Breaches*, it advises that if an investigation into a privacy breach is warranted, information about the breach would be collected. However, there is no indication who is responsible for recording when a privacy breach occurs or whether these records are maintained centrally. While PHIA does not require that records of security breaches be maintained centrally, it is considered a best practice. Maintaining a central repository of security breaches assists the department as a whole to detect and proactively address any systemic security concerns.

We find that Manitoba Families' draft PHIA Procedures Manual (2020) provides additional policy and procedural guidance reflecting the range of obligations required for trustees of personal health information.

Based on our review of the draft policies, the ombudsman makes the following recommendations:

- 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.**
- 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.**

Training

A trustee is required to provide orientation and ongoing training for its employees and agents about its PHIA policies and procedures. Orientation and training should not be confused as the same, and therefore, the content of information provided to employees in each of these

processes should differ in scope and depth. Orientation is an introduction to the workplace, the requirements for new employees and should provide a basic understanding of the legislation of which a public body or trustee must comply. Training is the forum in which a greater depth of skills, knowledge and competence is gained. Respecting privacy law, training is indeed the correct forum at which to operationalize how the protection of privacy occurs in daily work.

At the time of the breach, the department had been providing a webinar regarding the legislative requirements of both PHIA and FIPPA, access and privacy, in general orientation for new employees and as a refresher. The training in policies and procedures focused on the department's PHIA policy framework developed in 2018, included minimal practical guidance to meet the varied responsibilities of the staff providing the service. We were advised that this webinar was the basis for a revised version for ongoing training to include more content related to privacy obligations and scenarios for discussion which assist employees in understanding how PHIA and FIPPA impacts their daily work. Based on our review of the revised webinar content provided to our office, we are of the view that providing practical guidance on how privacy is considered in the daily work will help prevent the future occurrence of an unauthorized disclosure arising from human error.

As a requirement of PHIA, orientation and ongoing training needs to include a review of the department's PHIA policies and procedures. Employees are then aware of their day to day responsibilities regarding collection, use, disclosure and security of personal and personal health information. The policies and procedures should be reviewed frequently and updated to reflect the most current practice and guidance, which also means that training is never "one and done." We acknowledge that offering such a tailored FIPPA/PHIA webinar allows for greater accessibility for an employee to participate in the training and may help the department reach greater numbers of staff in a shorter period.

The department indicated that it is considering expanding the PHIA webinar to incorporate their PHIA policies and procedures. As this is a requirement under PHIA, the department's PHIA policies and procedures should be included in their orientation and ongoing training.

- 3. We recommend that Manitoba Families ensure that its PHIA policies and procedures are incorporated into the orientation and ongoing training.**
- 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) 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.**

Pledges of confidentiality

PHIA requires that a trustee must ensure that each employee and agent sign a pledge of confidentiality that includes an acknowledgment that they are bound by the trustee's PHIA policies and procedures and is aware of the consequences of breaching them.

We noted that the department's draft pledge of confidentiality does not include a statement that the employee is bound by the policies and procedures and the potential consequences of breaching them. For example, some trustees have added a statement in their pledge of confidentiality similar to this:

I also understand that unauthorized use or disclosure of such information may result in a disciplinary action up to and including termination of employment / contract /association /appointment, the imposition of fines pursuant to The Personal Health Information Act, and where applicable, a report to my professional regulatory body (if applicable).

Samples of a pledge of confidentiality and PHIA guidance can be found on the website of Manitoba Health and Seniors Care.²⁰

We also noted that while the Families' draft pledge is titled as "required under *The Personal Health Information Act*," the language in the draft speaks of personal information and not personal health information. While the department may wish to use the pledge to ensure employees read and agree to comply with the requirements of both FIPPA and PHIA, the pledge of confidentiality is a specific requirement under health privacy legislation and the language of personal health information should also be reflected in the content.

We appreciated receiving the department's communication plan for roll-out of the revised training, revised policies and final approval for implementation of the pledges of confidentiality in 2021. It is critically important that new employees receive orientation on privacy policies in order to inform the signing of the pledge of confidentiality and that existing employees are retrained as new policies are developed. It is our opinion that Manitoba Families must start training on the policies currently in draft form and commit to the completion of these activities.

Our review found that the procedure manual of 2020 provided good basic privacy policy guidance to employees. While we acknowledge that additional details required for privacy breach notification still need to be added, the policies in this manual must be included in the training so that signing of pledges of confidentiality can then be completed.

²⁰ <https://www.gov.mb.ca/health/phia/docs/poc.pdf>

Overall, we find that while the department has made progress toward PHIA compliance by developing security policies and a draft pledge of confidentiality, and making improvements to the training program, at the time of this report, it is incomplete and the department is non-compliant. Manitoba Families will only be in compliance with the legislation once it has approved and implemented all the necessary security safeguards required under PHIA.

Based on this review and in view of the challenges to implementation of basic security safeguards by the department noted in previous ombudsman privacy investigations, the ombudsman makes the following recommendations:

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.
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.
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.
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.

Privacy laws and government-funded external service providers

Throughout this report, we described the role of agency service providers in relation to the department's disability programs. We noted that these agencies, which are external to government, provide support services to CDS and CLdS clients under legal service agreements signed with the province of Manitoba. The personal and personal health information managed by these external providers mirrors that which is held and maintained by the government disability programs, in volume, detail and sensitivity of the information with the trust of clients and service recipients.

The unauthorized disclosure, albeit accidental, of personal health information to agency service providers in the case of the CDS privacy breach raises the question of how Manitoba Families ensures that service providers handle personal and personal health information appropriately. We earlier acknowledged those service providers who came forward within minutes to alert CDS to the error and question the purpose for the information received. These messages were critical to the identification and containment of the privacy breach and prevented further breaches from occurring. We noticed, however, that these messages were provided from a very small number of the 114 agencies and advocates who received the email and attachments containing personal health information. Assuming that other agencies opened the email, we wondered if they understood their obligations and whether they would have questioned the receipt of the errant emails or considered the implications for the privacy of individual children whose health information was contained in the email.

While not the focus of our investigation, in Appendix 2 of this report, we included a portion of the service purchase agreement setting out the requirements for agency providers under FIPPA and PHIA. These expectations for agencies include those for the collection, use, disclosure, retention and security of personal and personal health information.

The wording of the service purchase agreement reflects the complex relationship that government and service providers may have in abiding by Manitoba privacy laws. The agreement states that agency service providers who are external to government may not be directly subject to FIPPA or PHIA, but they are "brought under" these laws through the Access and Privacy Regulation under FIPPA or are required to comply with the acts through the conditions and terms of the service purchase agreement with government. The appendix to the agreement states that government is responsible for ensuring that external service providers handle personal information appropriately in accordance with FIPPA.

The service purchase agreement also vests similar responsibilities with the governing board of the agency:

It is the responsibility of the governing Board to ensure that the Service Provider takes all reasonable steps to protect the privacy of individuals receiving Services from the Service Provider. This shall include protecting personal information respecting these individuals from risks such as inappropriate collection, use, or disclosure. It is also the responsibility of the Board to ensure that the requirements set out in this Appendix are communicated to all Board members, employees and volunteers of the Service Provider and to establish policy and procedures for ensuring compliance with these requirements.

Agency boards are responsible for setting policy and procedures for ensuring compliance with these requirements. To understand the obligations for authorized collection, use and disclosure under PHIA and FIPPA, and as follows, to quickly identify when unauthorized disclosure has occurred, means that service providers, like government employees, must receive orientation, training and oversight from both their government and agency leaders. The obligations of external service providers under privacy legislation differ based on the structure of their organization and the nature of the services they provide. Some providers may be trustees directly subject to PHIA while others may be required by an agreement to act in accordance with PHIA. It is the responsibility of the department to determine each of their service provider's obligations under PHIA and FIPPA.

We have acknowledged the recent work by the department in developing policies and procedures, training, and pledges of confidentiality. We have noted that all of this work is in various stages of implementation and Manitoba Families has not yet complied with the requirements of PHIA. We are concerned about how agency boards might go about establishing policy and procedures for ensuring compliance without clear and established policy direction from the department, to whom they are accountable. This being the case, it is possible that service providers may not be in full compliance with PHIA if they are reliant on the department for direction on safeguards to ensure the appropriate handling of personal and personal health information.

Much can be learned from the external service providers in this situation about orientation and training of the privacy laws and the policies and procedures put into place by their leadership. Those who alerted CDS to the potential privacy breach may well be able to describe privacy management at their respective agencies, in order to inform others and to identify gaps in learning and opportunities for improved privacy practices for all external service providers.



A ROADMAP FOR THE FUTURE: THE CASE FOR A PRIVACY MANAGEMENT PROGRAM

The CDS privacy breach illustrates the volume, depth and sensitivity of personal and personal health information maintained by one departmental program alone. When considering the amount and type of personal and personal health information collected and maintained by all the service delivery programs under Manitoba Families, it is very likely that this department is the largest trustee of health information in the province, outside of the health sector. Moreover, the health information entrusted to Manitoba Families belongs to the most vulnerable of the province's citizens, who often have no other place to go for assistance.

As a trustee of the personal health information of the most vulnerable Manitobans, the department has a greater responsibility to secure and protect the health information of those receiving its services. It is imperative, therefore, that all employees of the department have more than a basic understanding and ability to manage personal and personal health information including its collection, use, disclosure, retention and security in performing their job duties. There must be advanced knowledge of the requirements of PHIA and FIPPA and the complex interface between those laws and the myriad of legislation under which Families' service programs are administered. This is fundamental to the daily work of departmental employees. It is also imperative, as noted in the previous section of the report, that the department ensures that its service providers are equally knowledgeable and equipped to manage these demands.

Simply complying with the security requirements of FIPPA and PHIA is not enough. The risk for addressing the privacy needs of those citizens served by the department in a piecemeal approach which focuses on basic compliance with privacy law is that considerable resources are then expended in reacting to privacy breaches, in particular one of the magnitude and severity of the CDS breach, rather than preventing them.

In a digital age, in employing technology, governments are constantly striving to provide and administer programs and services in the most effective and efficient ways. With greater technological advancement, opportunities for the transmission, storage and management of data by third party managers are viable options, but only if government has its own established structures to make sound determinations that privacy is protected and the privacy impact of new technology has been considered. A strong privacy culture is the foundation for using new technology. Without significant commitment to ensuring that advanced knowledge of privacy principles is embedded within the organizational culture, breaches of privacy, such as in this case, are more and more likely to occur. The commitment to privacy must be at the "front-end," not solely as a reaction when something has gone wrong.

In the written response to Manitoba Ombudsman of September 10, 2020, the minister of families, at the time, stated that the department was working to improve its safeguards to prevent future breaches. The minister also committed to working with our office to ensure that appropriate safeguards are in place when the Manitoba government is required to disclose personal and personal health information to external organizations, including independent officers of the Legislative Assembly of Manitoba.

Regardless of who the department needs to share information with, a good privacy management program is a foundation to safeguarding personal and personal health information in the delivery of services, now and into the future and demonstrates a much needed “front end” approach.

A trustee, such as Manitoba Families, must proactively ensure that the protection of privacy is a primary consideration in every action taken by every program when managing personal or personal health information. A privacy-focused organization must demonstrate a top-down, comprehensive, strategic, forward-thinking approach to the development of a privacy culture. This can best be accomplished through the adoption of a privacy management program which embraces the privacy principles referred to at the beginning of this report. An approach advocated by many information and privacy commissioners internationally, Manitoba Ombudsman published *Guidelines for Implementing a Privacy Management Program for Privacy Accountability in Manitoba's Public Sector* in 2017.²¹

The guide provides step-by-step guidance for public bodies and trustees on how to implement an effective and accountable privacy management program. While a component of a privacy management program ensures that there is compliance with privacy legislation, it also seeks to consider and develop knowledge and skill in interpreting privacy legislation in conjunction with other legislation under which a program or department must operate. As noted above, this is particularly necessary for the programs and services provided by Manitoba Families.

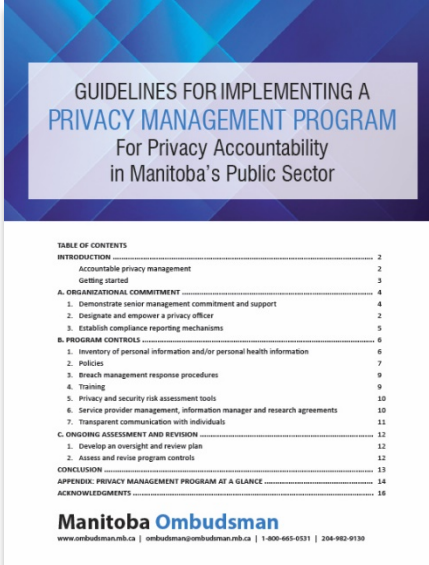


TABLE OF CONTENTS	
INTRODUCTION	2
Accountable privacy management	2
Getting started	3
A. ORGANIZATIONAL COMMITMENT	4
1. Demonstrate senior management commitment and support	4
2. Designate and empower a privacy officer	2
3. Establish compliance reporting mechanisms	5
B. PROGRAM CONTROLS	6
1. Inventory of personal information and/or personal health information	6
2. Policies	7
3. Breach management response procedures	9
4. Training	9
5. Privacy and security risk assessment tools	10
6. Service provider management, information manager and research agreements	10
7. Transparent communication with individuals	11
C. ONGOING ASSESSMENT AND REVISION	12
1. Develop an oversight and review plan	12
2. Assess and revise program controls	12
CONCLUSION	13
APPENDIX: PRIVACY MANAGEMENT PROGRAM AT A GLANCE	14
ACKNOWLEDGEMENTS	16

Manitoba Ombudsman
www.ombudsman.mb.ca | ombudsman@ombudsman.mb.ca | 1-800-665-0331 | 204-982-0130

Based on our review of this matter, the ombudsman makes the following recommendation:

9. We recommend that Manitoba Families commits to implementation of a privacy management program.

²¹ <https://www.ombudsman.mb.ca/uploads/document/files/privacy-management-program-guidelines-en.pdf>



CONCLUSION

The CDS privacy breach of August 26, 2020, is a prime example of how one administrative error can have an immediate impact on the security of the personal health information of 8,900 children and young adults, in addition to their families. The disclosure of this health information, while unintended, was nonetheless unauthorized under PHIA and non-compliant with the act. It serves as a reminder to all trustees about the critical need to protect personal and personal health information held in its custody and to fully consider the consequences of collection, use, disclosure, retention and security at all times.

Human error will never be fully eradicated. However, organizations can take steps to mitigate the risk of that error, and to be well positioned to take immediate action and make administrative improvements in the event error occurs.

Manitoba Families has a strong and coordinated privacy breach response system and quickly mobilized a multi-level approach to address the CDS breach after it occurred. We found that the department, in particular the Community Service Delivery and Corporate Services Divisions and the Children's disAbility Services program, took extensive and appropriate actions to respond to the privacy breach in containing the breach, evaluating risk, notifying affected individuals and taking practical preventative measures. We also noted the missed opportunities for identifying the error of blind copying which might have prevented the subsequent privacy breach.

The significant time and resources expended to address a privacy breach after it occurs, although necessary, must be allocated proactively to ensure that required privacy safeguards are in place before a privacy breach happens.

The CDS privacy breach caused our office to again question and review the state of required PHIA security safeguards within Manitoba Families and revealed a longstanding void of completed and implemented policies, procedures, training and pledges of confidentiality.

We found that Manitoba Families has recently made significant progress in the development of PHIA security requirements including a pledge of confidentiality, policies and procedures and enhanced training. It is imperative that the department continues this progress toward full implementation of these safeguards, not solely to ensure compliance with legislation, but in order to achieve a privacy respectful environment, one in which awareness of privacy and protection of personal health information is a paramount concern.

Based on our findings, we have made a number of recommendations regarding the implementation of security safeguards that were required under PHIA upon its enactment years

earlier. Considering the extent of the personal and personal health information collected from thousands of citizens receiving services under various department programs, service recipients need assurances that their information will be maintained and handled in a manner that fosters trust with service programs. This is the basis for our recommendation to the department to implement a privacy management program.

On March 18, 2021, the deputy minister of families wrote to our office accepting the nine recommendations. Details of the department's response to each recommendation can be found in the *Summary of Recommendations and Department Responses* section. The responses received were promising but some referenced "communication plans" and did not provide sufficient detail as to *how* the required actions would be realized. Given the importance of a demonstrated commitment on the part of Manitoba Families to completing the actions set out in the recommendations, we contacted the department to determine whether a detailed plan had been developed to implement the recommended actions for improved privacy practices. On April 7, 2021, Manitoba Families provided communication and implementation plans detailing the actions to be undertaken to deliver on its promise that appropriate security safeguards required under PHIA are fully put into place.

In issuing this report, we have notified Manitoba Families that in 2022 we will audit its compliance with PHIA to ensure that the department is meeting minimal legislative security requirements as well as to assess the actions taken to fully implement the recommendations made in this report. The results of the audit, Manitoba Families' compliance with PHIA and details of the actions taken by the department to implement the recommendations will be reported publicly.



SUMMARY OF RECOMMENDATIONS AND DEPARTMENT RESPONSES

In light of the investigation findings, Manitoba Ombudsman made several recommendations to Manitoba Families. The following incorporates the department's responses to our recommendations:

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.

Department's response: The department is in the process of vetting the Policy and Procedure Manual through Executive Management for feedback and final approval. Once approved we plan to make it available to all Department of Families employees through inclusion in the Mandatory Training Course and via the Families Live Intranet site.

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.

Department's response: The department will work towards developing and/or enhancing our policies and procedures on the recording of privacy breaches and designating staff to fulfill the associated responsibilities. We are currently exploring the possibility of a centralized location for all documentation related to privacy information, including a repository related to breaches that can be accessed by appropriate staff.

3. We recommend that Manitoba Families ensures that its PHIA policies and procedures are incorporated into the orientation and ongoing training.

Department's response: The department is updating our Mandatory Training Presentation to ensure our policies and procedures align with the training that will be delivered to employees.

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) 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.

Department's response: The development of a centralized location for all privacy information will be made available to employees on the Families Live Intranet site and will include a more user-friendly location and will house all policies and guidelines from various divisions across the department.

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.

Department's response: We will review our various policies and guidelines housed by the department to ensure that our approach is consistent across all programs as it relates to PHIA training and the pledge.

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.

Department's response: The department has updated the pledge to include reference to personal health information. Furthermore, the following consequences for an employee who breaches the department's PHIA policies and procedures have been included:

I also understand that unauthorized use or disclosure of such information may be subject to a disciplinary action up to and including termination of employment/contract/association/appointment, the imposition of fines pursuant to the Personal Health Information Act and, where applicable, a report to my professional regulatory body (if applicable).

In addition, the following statement has been updated to affirm the pledge signed by the employee continues after employment with the department.

I am bound by the PHIA and FIPPA Acts and regulations and any other applicable regulations, as amended or replaced from time to time, and by the PHIA and FIPPA policies and procedures of the department, respecting the collection, use, disclosure, protection, retention and destruction of any personal information that I may collect or have access to in the course of my employment, or after my employment ends with the department.

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.

Department's response: The department will develop a communication plan, with the target of May 1, 2021. This will ensure that all new employees complete the departmental Mandatory Training Course and upon completion, they must sign the PHIA Pledge of Confidentiality. The communication will stress the importance of the employee's obligations and be made aware of their responsibilities under PHIA to complete the Mandatory Training Course.

Moreover, we will continue to offer an abridged version of the New Employee Orientation, providing an overview of privacy legislation and the responsibilities as employees of the public body.

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.

Department's response: As part of the communication plan, employees will be made aware that any employee who has not yet completed the New Employee Orientation, or the Privacy Webinar are required to complete the Mandatory Training Course. Furthermore, employees will be required to complete a refresher of the course at a minimum of every 3 years.

The department will ensure that employee participation in the Mandatory Training Course is tracked. Quarterly reports will be completed so that employee attendance can be monitored and verified. The department will also verify those employees who have completed the New Employee Orientation, or the Privacy Webinar in the last three years and require that the PHIA Pledge of Confidentiality be signed.

While the department is committed to meeting your deadline of December 31, 2021, for all departmental employees, we respectfully ask that the deadline be extended somewhat for us to meet this obligation with our agents.

9. We recommend that Manitoba Families implements a privacy management program.

Department's response: The department recognizes that it houses an extensive amount of personal and personal health information regarding individuals who receive services through the various programs we administer. We will explore how department privacy management could be augmented to form a fulsome privacy management program.

Appendix 1: CDS Information Fields

Participant List

Month Of Extract	2020-03-31
Participant ID	0
Participant Name	
Address 1	123 Fake St
Postal Code 1	
City/Town/Municipality 1	WINNIPEG
Participant Details Status	Open
Date of Birth	2003-01-01
Age at March 31	17
Gender	Female
First Language	English
Funding Region	Winnipeg
Primary Case Worker	NAME, CSW
Program Status	Eligible
Supervisor Elig Decision	Eligible
Referred From	Family
Letter of Elig/Inelig Sent	
Reason for Program Closure	
Date of Program Closure	
Open to Program This Month	Yes
Assessment Type 1	Psychology
Assessment Type 2	
Assessment Date 1	2003-08-21
Assessment Date 2	
Data Collection Date	2020-05-31
Running Date	2020-06-04

Family Supports 2019-20

Participant ID			
Participant Name			
Funding Region	Westman	Westman	Westman
Service	Exceptional Circumstances	Self Managed	Self Managed
Sub-service	Child Care	After School Care	Respite
Plan Start Date	2020-03-23	2019-04-01	2019-04-01
Plan End Date	2020-03-31	2019-06-30	2019-09-30
Service Provider Name	ABC	ABC	ABC
Service Provider ID			
Plan ID			
Unit Type	Once over months	Once over months	Once over months
No. of Units	-1	-1	-1
Rate	273	1176.5	2704
Is Ongoing	No	No	No
No. of CF Units	-1	-3	-6
INVOICE: April	0	351	468
INVOICE: May	0	390	416
INVOICE: June	0	195	468
INVOICE: July	0	0	468
INVOICE: August	0	0	468
INVOICE: September	0	0	416
INVOICE: October	0	0	0
INVOICE: November	0	0	0
INVOICE: December	0	0	0
INVOICE: January	0	0	0
INVOICE: February	0	0	0
INVOICE: March	273	0	0
Annual Invoiced Total	273	936	2704

Appendix 2: Excerpt, Service Purchase Agreement, Appendix 2, Province of Manitoba

The Province of 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) the Government is responsible for ensuring that personal information is handled appropriately by external service providers.

Certain external service providers that do not fall under The Freedom of Information and Protection of Privacy Act and The Personal Health Information Act (C.C.S.M. c. P33.5) are brought under both Acts by virtue of the Access and Privacy Regulation under The Freedom of Information and Protection of Privacy Act.

Where the Service Provider does not fall under The Freedom of Information and Protection of Privacy Act and The Personal Health Information Act , the Service Provider shall comply with the requirements respecting the collection, use, protection and disclosure of personal information. These requirements reflect the principles of The Freedom of Information and Protection of Privacy Act.

It is the responsibility of the governing Board to ensure that the Service Provider takes all reasonable steps to protect the privacy of individuals receiving Services from the Service Provider. This shall include protecting personal information respecting these individuals from risks such as inappropriate collection, use, or disclosure.

It is also the responsibility of the Board to ensure that the requirements set out in this Appendix are communicated to all Board members, employees and volunteers of the Service Provider and to establish policy and procedures for ensuring compliance with these requirements.

Definition of Personal Information

1.01 “Personal information” has the meaning given to that term in The Freedom of Information and Protection of Privacy Act of Manitoba (C.C.S.M. c. F175) (as amended from time to time), and includes:

- (a) personal information about an identifiable individual which is recorded in any manner, form or medium; and
- (b) personal health information about an identifiable individual as defined in The Personal Health Information Act of Manitoba (C.C.S.M. c. P33.5) (as amended from time to time).

These statutory definitions are attached at the end of this Appendix.

1.02 The requirements and obligations in this Appendix:

- (a) apply to all personal information received, collected or otherwise acquired by the Service Provider in the course of carrying out its obligations under this Agreement, in whatever manner, form or medium;
- (b) apply whether the personal information was received, collected or acquired before or after the commencement of this Agreement; and (c) continue to apply after the termination or expiration of this Agreement.

Collection of personal information by the Service Provider

1.03 The Service Provider recognizes that, in the course of carrying out its obligations under this Agreement, the Service Provider may receive personal information from Manitoba and may collect, acquire, be given access to and may otherwise come into possession of personal information about individuals participating in the programs operated by or receiving Services from the Service Provider under this Agreement.

1.04 Where the Service Provider receives, collects, acquires, is given access to or otherwise comes into possession of personal information, the Service Provider shall receive, collect or acquire only as much personal information about an individual as is reasonably necessary to carry out the Service Provider's obligations under this Agreement.

1.05 Where the Service Provider collects or acquires personal information directly from the individual it is about, the Service Provider shall ensure that the individual is informed of:

- (a) the purpose for which the personal information is collected;
- (b) how the information is to be used and disclosed;
- (c) who can answer questions the individual may have about his or her personal information; and
- (d) the individual's right of access to the personal information about himself or herself, as set out in the Service Provider's policies established in accordance with subsection 1.06 of this Appendix.

Appendix 3: Methodology

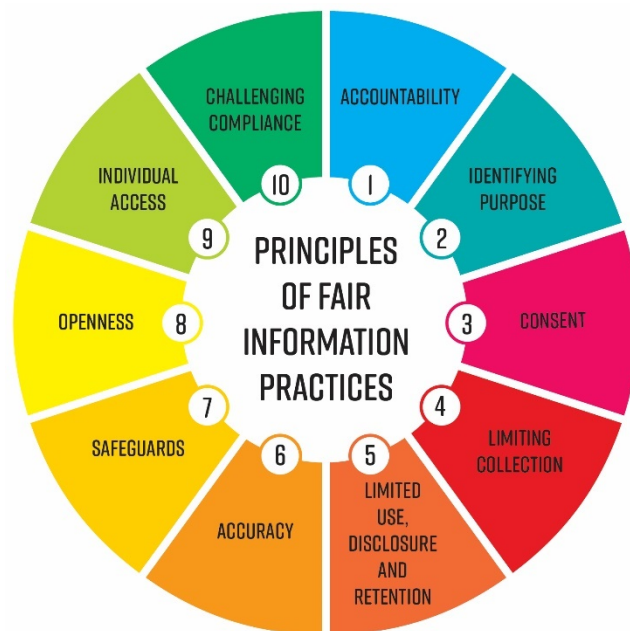
The review was conducted by a two-person investigative team under the direction of the ombudsman and deputy ombudsman. The team reviewed over 500 pages of documents including the following:

- Records of complaints and calls from affected individuals and families
- Formal correspondence from the department
- A privacy breach reporting form
- Records and notes of actions taken by Manitoba Families following discovery of the privacy breach related to containment, risk assessment, notification and prevention
- All emails sent from and to CDS in response to the MACY request for information
- All emails sent and received from the unintended recipients
 - Records depicting the format and nature of personal and personal health information and other data disclosed about CDS clients
 - Records depicting the format and nature of personal and personal health information and other data disclosed for CFS clients
- An analysis of email communications considered by Manitoba Families
- An audit of all email communications from August 7 to 26, 2020 related to transmission of personal health information at issue – requested by our office
- Listing of all advocacy groups and services providers and their respective email addresses (the email recipients)
- Departmental privacy requirements - privacy and security policies, pledges of confidentiality, FIPPA and PHIA training materials, other website privacy resources
- CDS staff privacy training completed
- Training schedules for 2019/2020, 2020/2021 and planned schedule for 2020/2021
- PHIA/FIPPA privacy resources on Families' and Community Service Delivery intranet sites
- PHIA/FIPPA privacy resources on the Manitoba government Business Transformation and Technology (BTT) website
- MACY Revised Data Protection Procedures, October 14, 2020

The team also reviewed previous ombudsman investigation files relating to Manitoba Families' privacy policies, procedures, pledges and training.

The investigation team conducted interviews with over 20 employees and executive management of Manitoba Families, Community Service Delivery, Corporate Services and Children's disAbility Services, the Child and Family Services Branch, select Child and Family Services authorities/agencies, CDS/CLdS agency service providers, and complainants (affected individuals) to our office. As noted previously, our office intake investigator spoke with over 30 individuals who contacted us to relay concerns about the breach or were seeking further information or assistance.

Appendix 4: Principles of Fair Information Practices, Canadian Standards Association Principles in Summary Model, Code for the Protection of Personal Information (1996)



1. ACCOUNTABILITY A public body is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the public body's compliance with the following principles.

2. IDENTIFYING PURPOSES The purpose for which personal information is collected shall be identified by the public body at or before the time the information is collected.

3. CONSENT The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4. LIMITING COLLECTION The collection of personal information shall be limited to that which is necessary for the purposes identified by the public body. Information shall be collected by lawful means.

5. LIMITED USE, DISCLOSURE AND RETENTION Personal information shall not be used or disclosed for purposes other than those which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

6. ACCURACY Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. SAFEGUARDS Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. OPENNESS A public body shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. INDIVIDUAL ACCESS Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. CHALLENGING COMPLIANCE An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the public body's compliance.

Adapted with permission from 10 Privacy Principles by the B.C. government.

Appendix 5: Manitoba Families Organizational Chart

