REPORT OF THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

APRIL 11, 2024

Review of the Practices and Procedures of the Ministry of Children, Community and Social Services Inter-ministerial Data Integration Unit

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

CONTENTS

Executive Summary

This report concludes the Information and Privacy Commissioner of Ontario's (IPC or the Commissioner) review of the inter-ministerial data integration unit located within the Business Intelligence and Practice Division of the Ministry of Children, Community and Social Services (MCCSS IMDIU). The review was conducted under Part III.1 of the *Freedom of Information and Protection of Privacy Act* (Part III.1).

A major objective of Part III.1 is to enable the Ontario government to join data sets and to use the combined data for the public good while protecting the privacy of individuals. Part III.1 establishes the authority for data integration units to indirectly collect personal information for the purpose of analysis to support government decision-making. This authority involves linking different sets of personal information together and disclosing de-identified information for the purposes of managing or allocating resources; planning delivery of programs and services; and evaluating those programs and services. Data integration units are held to high transparency, privacy, and security standards. Data integration units must develop practices and procedures that comply with the Ontario Public Service Data Integration Data Standards.

Part III.1 requires that the IPC conduct reviews of certain classes of data integration units before they can begin collecting personal information. Now that the review is complete, the MCCSS IMDIU may begin its work with personal information. However, it must comply with the orders in this report and report back to the IPC on several recommendations made within the time periods specified.

During its review, the IPC assessed the MCCSS IMDIU's practices and procedures. The practices and procedures establish a framework that governs the lifecycle of information collected by the MCCSS IMDIU. They cover subjects including collecting, using and disclosing personal information; linking and de-identifying personal information; security; retention periods; and public reporting.

In general, the MCCSS IMDIU has been very responsive and has amended — or agreed to amend — its practices and procedures in accordance with the IPC's comments. Where the MCCSS IMDIU has demonstrated compliance with the standards, or has made the necessary adjustments to bring itself into compliance with the standards at the time of issuing this report, the IPC has found compliance has been met.

Where necessary adjustments are relatively minor, present low risk and can be achieved in short order, the IPC has accepted the MCCSS IMDIU's commitment to address these as indicating compliance with the applicable Data Requirement.

In three instances, the IPC has found more significant gaps likely to require more time and effort to address and has recommended that the MCCSS IMDIU remain engaged with the IPC and report back on their implementation within one year following the date of this report. These three recommendations are to:

1. describe how its practices and procedures have been changed to address the re-use of personal information and coded information;
2. revise its Methodologies and Risk Evaluation Framework to expand upon its practices and procedures, including how its de-identification and risk methodology have been revised to account for all considerations related to disclosures using the Secure Research Lab; and

3. revise its practices and procedures to:

    a. address business roles and access controls for the BIPDDE high sensitivity file server and SFTP/file transfer tools, in compliance with all elements set out in requirement 7; and

    b. address its relationship with individuals who supply services (whether on their own behalf or on behalf of another person, entity or organization) related to the collection, linkage, use, disclosure, de-identification, retention, transfer, disposal, or destruction of PI, coded information, or de-identified information, and who are not members in accordance with requirement 7.8.

Where the IPC has found higher risk issues that remain outstanding as at the date of this report and warrant the greatest level of assurance of compliance to protect Ontarians' privacy, the Commissioner has decided to issue binding orders ordering the MCCSS IMDIU. Specifically, the Commissioner has ordered the MCCSS IMDIU to:

1. ensure that an up-to-date privacy impact assessment (PIA) has been conducted of all systems and tools utilized;
2. ensure that an up-to-date threat risk assessment (TRA) has been conducted of all systems and tools utilized; and
3. implement a detailed business continuity and disaster recovery plan.

See Appendix A for the complete text of orders and recommendations to report back on.

1. Introduction

In 2019, the *Freedom of Information and Protection of Privacy Act* (FIPPA) was amended to add Part III.1 Data Integration (Part III.1).

Part III.1 created new authorities allowing designated data integration units to collect and link personal information to create de-identified datasets. These datasets are to be used for the purposes of analysis in relation to the Ontario government's:

- management or allocation of resources;
- planning for the delivery of programs and services provided or funded by the Government of Ontario; and
- evaluation of those programs and services.

This represented a significant change in Ontario's approach to using publicly held information for the public good. Part III.1 created a path for breaking down barriers to information sharing for analytics purposes in the public sector.

However, the new authorities created by Part III.1 came with an expanded regulatory regime and oversight role for the Information and Privacy Commissioner of Ontario. Among other things, Part III.1 *requires* that the IPC conduct reviews of certain data integration units *before* they can begin collecting personal information.

In this report, the IPC summarizes its review process, findings, recommendations, and orders relating to the inter-ministerial data integration unit located in the Business Intelligence and Practice Division of the MCCSS.

2. Data Integration Units

Part III.1 defines three types of data integration units and assigns different levels of authority to collect, use, and disclose personal information for each of these types.

The three types of data integration units are as follows:

- **Ministry data integration units (MDIUs)** are located within a ministry and permitted to indirectly collect personal information from within the ministry and entities that receive funding from the ministry or administer a program or service on its behalf.
- **Inter-ministerial data integration units (IMDIUs**) are located within a ministry and permitted to indirectly collect personal information from Ontario or municipal institutions[1], as well as MDIUs, other IMDIUs, and extra-ministerial data integration units.
- **Extra-ministerial data integration units (EMDIUs)** are outside of a ministry and are permitted to indirectly collect personal information from Ontario or municipal institutions, MDIUs, IMDIUs, and other EMDIUs, as well as the extra-ministerial unit itself if it is also a prescribed entity under section 45 of the *Personal Health Information Protection Act* (PHIPA).[2]

1 "Ontario or municipal institutions" means "institutions" as defined under FIPPA and its municipal equivalent, the *Municipal Freedom of Information and Protection of Privacy Act*.

2 EMDIUs were not included in the original amendments creating Part III.1. FIPPA was amended in 2020 to create a role for EMDIUs.

IMDIUs and EMDIUs can collect more broadly than MDIUS and, as such, are required to be reviewed by the IPC before they can begin to collect personal information under Part III.1.[3]

To date, the following data integration units have been prescribed in Regulation 366/19 under FIPPA:

MDIUs	IMDIUs	EMDIUs
– The Analytics and Evidence Branch of the Ministry of the Attorney General – The Business Intelligence and Practice Division of the Ministry of Children, Community and Social Services – The Education Statistics and Analysis Branch of the Ministry of Education – Digital and Analytics Strategy Division of the Ministry of Health (formerly the Capacity Planning and Analytics Division) – Digital and Analytics Strategy Division of the Ministry of Long-Term Care (formerly the Capacity Planning and Analytics Division) – The Analytics Unit of the Ministry of the Solicitor General	– The Business Intelligence and Practice Division of the Ministry of Children, Community and Social Services – The Ontario Statistics Office of the Ministry of Finance – Digital and Analytics Strategy Division of the Ministry of Health (formerly the Capacity Planning and Analytics Division)[4]	– The Institute for Clinical and Evaluative Sciences (ICES)[5]

To fully regulate the activities of data integration units, Part III.1 also applies to their officers, employees, or agents who work in the unit. These officers, employees, or agents are referred to as a "member" of the data integration unit.[6]

3 S. 49.5(1)1.ii.of FIPPA

4 The IPC completed its review of the MOH IMDIU March 29, 2022. The report can be found here: https://www.ipc.on.ca/wp-content/uploads/2022/05/review-practices-and-procedures_ministry-of-healths-inter-ministerial-data-integration-unit.pdf.

5 Pending review by the IPC.

6 See the definition of "member" in 49.1 which also slightly distinguishes between MDIUs/IMDIUs and EMDIUs.

3. Ontario Public Service Data Integration Data Standards

Part III.1 requires the Minister of Public and Business Service Delivery (the Responsible Minister), or a designated person, to prepare draft data standards that address, among other things, practices and procedures for use by data integration units when:

- collecting, using, and disclosing personal information,
- linking and de-identifying personal information,
- reporting publicly on the use of personal information,
- securely retaining personal information, including providing for a minimum retention period for personal information, and
- securely disposing of personal information.[7]

These data standards must be approved by the IPC under Part III.1[8] and all data integration units must comply with these approved data standards.[9]

On April 27, 2021, the IPC approved the data standards provided by the Responsible Minister. The IPC's approval letter can be read here. The approved Ontario Public Service Data Integration Data Standards can be read here (the Data Standards).

The Data Standards apply to personal information throughout its lifecycle under Part III.1. This lifecycle includes the de-identification of the personal information at various levels. The process of de-identification involves the transformation of personal information along a spectrum of identifiability from the original personal information collected by the data integration unit, and information that has been de-identified to an acceptable threshold before it can be made available by the data integration unit for analysis in relation to:

- the management or allocation of resources;
- the planning for the delivery of programs and services provided or funded by the Government of Ontario; and
- the evaluation of those programs and services.

The Data Standards refer to information included within this spectrum as "coded information."[10] As such, there are three categories of information referred in the Data Standards and this report:

- **personal information** (i.e., the original identifiable information collected by the data integration unit and the dataset containing the direct identifiers removed from such original identifiable information as part of the process of creating coded information);
- **coded information** (i.e., personal information from which direct identifiers have been removed and replaced with an internal code used for linking different records of coded information together); and
- **de-identified information** (i.e., information for which it is not reasonably foreseeable, in the circumstances, that an individual could be identified).[11]

7 S. 49.14(1)(a) of FIPPA.
8 S. 49.5(1)1.ii. of FIPPA.
9 S. 49.14(4) of FIPPA.
10 Data Standards, p. 2.
11 For more detail on these categories of information, see the relevant definitions in *FIPPA* and the Data Standards.

The Data Standards are divided into seven distinct categories. These are:

1. **General Requirements:** This category outlines general requirements for data integration units to ensure that all the Data Standards are effectively implemented and appropriately documented. Accountability measures and training requirements outlined in this Part are intended to enhance compliance and consistency of practice, as well as to uphold operational integrity across all data integration units.

2. **Collection, Use and Disclosure:** This category outlines the minimum requirements that the data integration units must meet when collecting, using, and disclosing personal information, coded information, and de-identified information, as applicable. Under the requirements, data integration units must take reasonable steps to ensure the protection of privacy, comply with their legal obligations, and ensure that the persons, entities, and organizations they interact with do the same.

3. **Secure Retention and Transfer:** This category outlines requirements for data integration units to put in place safeguards applicable to their technology environment that ensure the secure retention and transfer of personal information and coded information. Specifically, data integration units must adopt administrative, technical, and physical safeguards to protect the system components and information assets of its technology environment from attempts to attack, breach, or access them in an unauthorized manner.

4. **Secure Disposal and Secure Destruction:** This category outlines requirements for data integration units to ensure the secure disposal or destruction of personal information, coded information, and related storage media. Once securely disposed of or destroyed, data integration units must ensure personal information and coded information is permanently removed from the relevant storage medium such that it cannot be reconstructed or retrieved in reasonably foreseeable circumstances.

5. **Retention Period:** This category outlines requirements for data integration units to retain personal information and coded information for specified periods. A retention period is the overall length of time that information must be kept before it can and, in some cases, must be deleted.

6. **De-identification and Linking:** This category outlines requirements for data integration units to implement an accurate, privacy-protective de-identification and linking process to ensure that the personal information collected under the Part can be transformed and used for analysis. It also requires that the de-identification process, in particular the transformation of personal information into coded information, be undertaken as soon as reasonably possible in the circumstances.

7. **Public Notice and Annual Reporting:** This category outlines the minimum requirements for data integration units to ensure openness and transparency with respect to their information practices. Under the Part, data integration units must make information about how they collect, use, and disclose personal information publicly available. In particular, data integration units must create and publish notices of collection, reports on use, annual reports, and processes for privacy complaints and inquiries.

Data integration units are required to develop, document, and implement practices and procedures that address each of the requirements set out in Part III.1, its regulations, and the Data Standards.[12] Data integration units are further required to comply with their practices and procedures.[13]

12 See requirement 1 of the Data Standards.

13 See requirement 1.2.1 of the Data Standards.

4. Commissioner's Review of Practices and Procedures

Part III.1 requires that the IPC conduct reviews of the two classes of data integration units with the broadest authority to collect personal information before they can begin collecting it, namely IMDIUs and EMDIUs. In the case of IMDIUs and EMDIUs, the IPC must conduct an initial review of their practices and procedures after they are designated and at least once every three years after initial review has concluded.[14] The IPC may also conduct reviews of the practices and procedures of data integration units any time the IPC has reason to believe that the requirements of Part III.1 are not being complied with.

The purpose of the IPC's review under Part III.1 is to determine whether:

a. there has been unauthorized collection, retention, use, disclosure, access to, or modification of personal information collected under Part III.1; and

b. the requirements under Part III.1, including requirements with respect to notice, de-identification, retention, security, and secure disposal, have been met.[15]

In conducting its review under Part III.1, the IPC has a variety of powers to require the production of information and records relevant to the subject matter of the review. The data integration unit being reviewed is required to assist the IPC in its review.[16]

At the conclusion of a review the IPC may, after giving the data integration unit the opportunity to be heard, order the data integration unit to:

- Discontinue the practice or procedure.
- Change the practice or procedure as specified by the IPC.
- Destroy personal information collected or retained under the practice or procedure.
- Implement a new practice or procedure as specified by the IPC.[17]

14 S. 49.12 (1) of FIPPA.

15 S. 49.12(3) of FIPPA.

16 S 49.12(5) and (6) of FIPPA.

17 S. 49.12(7) of *FIPPA*. The IPC may order no more than what is reasonably necessary to achieve compliance with Part III.1 – see s. 49.12(8) of FIPPA.

5. Review of the MCCSS IMDIU Practices and Procedures

In the context of this review, the MCCSS IMDIU and the IPC exchanged several rounds of detailed correspondence and had several discussions on the practices and procedures reviewed, as well as the review process. Between June 2022 and June 2023, the MCCSS IMDIU provided the IPC with documentation reflecting its practices and procedures. The MCCSS IMDIU also provided responses to the IPC's requests for clarification, additional information, and confirmation of certain facts during this time. See Appendix B for the complete list of practices and procedures reviewed and representations made by the MCCSS IMDIU. The IPC's review of the MCCSS IMDIU's practices and procedures was based on the current approved Data Standards, dated April 2021.

6. Findings of the Review

This Findings section is broken down into sub-sections corresponding to each of the seven categories of the Data Standards. Each sub-section contains a summary of:

- the requirements forming that category of the Data Standards;
- the practices and procedures provided by the MCCSS IMDIU that relate to those Data Standards; and,
- the IPC's observations and findings with respect to those practices and procedures made during the review.

Where applicable, the sub-sections also include recommendations to report back to the IPC on certain items to be addressed and formal orders under s. 49.12(7) of FIPPA that the Commissioner has decided to make, along with the Commissioner's reasons. These recommendations and orders focus on the most significant issues identified by the IPC that were still outstanding at the time the review was completed.

Category 1: General Requirements

This standard sets out the overarching responsibilities of the MCCSS IMDIU to ensure its compliance with Part III.1, the Data Standards, the unit's Practices and Procedures, other applicable provisions of *FIPPA* and its regulations, and agreements and acknowledgements made pursuant to them.

Requirement 1: Develop, document, and implement Practices and Procedures that address each of the requirements set out in the Part, its regulations, and the Data Standards

Requirement 1 of the Data Standards applies to all other requirements in the Data Standards. It requires the development and implementation of written practices and procedures for every requirement in Part III.1, its regulations, and the Data Standards. Further, these developed, documented, and implemented practices and procedures must describe, for each requirement: data integration unit member (DIU member) roles and responsibilities, accountability structures, documentation practices regarding decisions relating to personal information and/or coded information, and applicable time frames, among other things. Requirement 1 further sets out an overarching structure for the MCCSS IMDIU to internally monitor its own compliance by reviewing logs, lists, inventories, or documentation that they are required to maintain. The MCCSS IMDIU is also required to conduct broader internal reviews of its practices and procedures and their implementation at least once every three years to ensure they are kept up-to-date, continue to address the MCCSS IMDIU's compliance obligations, and are cohesive.

Many of the requirements related to logging, auditing, and monitoring in the Data Standards were addressed by the MCCSS IMDIU using templates and tracking spreadsheets that require DIU members to manually review and input information. While the method of meeting the requirements set out under the Data Standards is at the discretion of the MCCSS IMDIU, where possible the IPC encourages the adoption of technology and tools to automate the logging and monitoring activities required to implement data integration.

The MCCSS IMDIU provided the IPC with several written practices and procedures to address compliance with the Data Standards. These included the OPS Data Integration Practices and Procedures Manual (DI Manual) that was drafted in collaboration with other IMDIUs, various standard operating procedures, templates, and supporting documents. The DI Manual sets out general roles and responsibilities and reporting lines for members of the MCCSS IMDIU, as well as a high-level overview of the data integration activities subject to the practices and procedures. The standard operating procedures describe in more detail the various tasks that each DIU member role is responsible for throughout the lifecycle of a data integration project, as well as supporting technology and administrative tasks.

Overall, the IPC initially found that the MCCSS IMDIU's practices and procedures contained the relevant information needed to address this requirement. However, in several areas there was a lack of necessary detail: certain elements defined in the standards were not included. The relationship between the DI Manual and the standard operating procedures was unclear and there were some inconsistencies across documentation. In discussions with the MCCSS IMDIU, it was clarified that the DI Manual was intended to be complementary to the practices and procedures, and the standard operating procedure documentation was drafted to independently address the Data Standards.

The IPC also initially found that necessary documentation and detailed procedures regarding implementation of the requirements surrounding the internal review of logs, inventories, and the IMDIU's periodic review of its practices and procedures were missing. The MCCSS IMDIU was very responsive in expanding on these areas and incorporating the level of detail required to ensure the practices and procedures could be practically acted upon.

The Data Standards state that where a requirement under the Data Standards gives discretion to IMDIUs to determine how it will be implemented, IMDIUs must exercise discretion in a manner that is reasonable in the circumstances.[18] As a general comment, while the IPC is satisfied the MCCSS IMDIU has addressed gaps identified in its practices and procedures regarding the timelines for actioning issues such as DI member non-compliance, it was found that the term "timely manner" was used frequently in instances where it would be advisable to articulate a defined timeframe to provide staff with greater clarity as to what constitutes a timely manner in a given situation.[19] While defining a timeframe would be at the discretion of the MCCSS IMDIU, where appropriate, the IPC encourages the MCCSS IMDIU to define and document clear timeline requirements and expectations.[20]

The IPC is satisfied that the necessary revisions were made to bring the MCCSS IMDIU into compliance with Requirement 1.

18 See requirement 1.2.2 of the Data Standards.

19 See requirement 1.3.2 of the Data Standards.

20 See requirements 1.1-6, 1.3.2, 1.4.2, 4.2.3 of the Data Standards.

Requirement 2: Provide initial and annual privacy and security awareness training to all members

Requirement 2 of the Data Standards focuses on the privacy and security awareness training that MCCSS IMDIU members must receive to access the data integration environment ("DI Environment"[21]) upon starting their role and annually thereafter. The training must cover minimum content including: relevant legal authorities; purposes and limitations with respect to collecting, using, and disclosing personal information and/or coded information; responsibilities in the event of a breach; the safeguards in place and duties with respect to them; various prohibited activities; procedures on handling requests for access to information; and limits on the use of de-identified information. The content of the training must correlate to the specific role that a member performs in the MCCSS IMDIU. Training materials must be kept up-to-date. Simulation exercises must also be performed annually to test breach response procedures and the business continuity and disaster recovery plan, with findings documented. Any recommendations arising from the exercise must be addressed in a timely manner.

The MCCSS IMDIU provided the IPC with relevant practices and procedures addressing this requirement. The DI Manual set out the overarching obligation to perform training. The User and Information Management standard operating procedures addressed the responsibility and accountability structures required for ensuring mandatory training is completed, as well as staff sign-on to all necessary documentation, such as the confidentiality agreements required under the Data Standards, prior to being granted access to relevant areas of the DI Environment. Staff are required to attest in writing that they have completed the initial training modules and re-confirm this annually.

The MCCSS IMDIU provided copies of self-directed training modules to the IPC, which focused on the basics of FIPPA and data integration, privacy and security, purposes, and legal authorities. Initially, the standard operating procedures and the training modules were found to be insufficient to meet the full scope of the requirement, as they did not provide details regarding how DIU members were to apply the practices and procedures in their day-to-day employment or specific roles within the IMDIU.[22] The IPC provided comments on areas where the modules could be improved and highlighted aspects where there were inconsistencies between terminology used in the modules and what was found within the standard operating procedures. The MCCSS IMDIU revised the standard operating procedures and provided an additional training module focused on role-based training for DIU members. The IPC also noted that the training materials did not include descriptions of post-data release activities, specifically data deletion and secure disposal or destruction, and requested the materials be revised to include these activities.

The IPC is satisfied that the revisions made by the MCCSS IMDIU and its commitment to address the remaining items above are sufficient to bring it into compliance with Requirement 2.

---

21 The "DI Environment" is defined in the Data Standards (p. 54) as:
"All associated system components and information assets of a [MCCSS IMDIU's] technology environment, including:
• hardware, software, applications, security systems, network appliances, and servers; and
• [personal information], coded information, de-identified information, logs, and authentication data."

22 See requirement 2.1.3 of the Data Standards.

Requirement 3: Identify and define an impartial process for members to report operational gaps or deficiencies, as well as actual or suspected incidents of non–compliance by other members

Pursuant to requirement 3 of the Data Standards, the MCCSS IMDIU must identify and define an impartial process for members to report operational gaps or deficiencies, as well as actual or suspected incidents of non-compliance by other members.[23] The purpose of this process is to outline the way in which members can express concerns about actual or suspected wrongdoing within the MCCSS IMDIU without fear or risk of retribution. The process must be confidential and must ensure that reports are not made to or addressed by an individual who may be involved in, or have direct authority over, the matter being reported. If such reports are determined to be actual or suspected breaches, the MCCSS IMDIU must respond to them in accordance with its breach response procedures as outlined in requirement 14 of the Data Standards.

The MCCSS IMDIU Compliance Management standard operating procedure was provided to address this requirement, as well as several templates and supporting business documents. However, the practices and procedures stated that such reports should be made to the IMDIU Director. The IPC communicated that IMDIU Director should not be involved in this oversight role because they are likely to be involved in the matter or have direct authority over the concerned individuals and activities.[24] Based on the IPC's feedback, the MCCSS IMDIU made the necessary revisions to their Compliance Management standard operating procedure and associated templates, assigning management of the DIU Member Confidentiality Deficiency Reporting process to the MCCSS Access and Privacy Office, which sits outside of the Business Intelligence and Practice Division of the ministry.

Based on its review, the IPC is satisfied that the MCCSS IMDIU's policies and procedures are in compliance with the standards set out under Requirement 3.

23 See requirement 3.1-2 of the Data Standards.

24 See requirements 3 and 3.2.1-2 of the Data Standards.

Requirement 4: Conduct a privacy impact assessment (PIA) to identify, analyze, and mitigate potential privacy risks where required

Requirement 4 of the Data Standards stipulates that privacy impact assessments must be conducted to identify, analyze, and mitigate privacy risks. The MCCSS IMDIU is required to identify and define the circumstances that would require a PIA or an update to a PIA including certain minimum prescribed circumstances. These minimum circumstances are:

- a new collection of personal information or change to an ongoing collection of personal information; and
- implementation of a new, or change to a, program, process, technology, or system relating to the MCCSS IMDIU's activities under Part III.1 that could affect the privacy of individuals or the confidentiality of information.[25]

The MCCSS IMDIU must also describe the required content of a PIA, and this description must include minimum content specified in the Data Standards. Further, the MCCSS IMDIU must prioritize and address PIA recommendations in a timely manner and have related documentation.

The MCCSS IMDIU provided the IPC with documentation addressing this requirement, including several provisions in its Request Management and Environment Management standard operating procedures and a template PIA to be used for specific data integration initiatives. A May 25, 2022 PIA focused on the MCCSS IMDIU's Data Integration Processing Environment (DIPE).[26] Project or initiative specific PIAs are treated as addendums to the base DIPE PIA. The IPC provided some general comments and feedback on how to improve the content and implementation of the project-specific PIA template, including to provide examples of acceptable purpose statements to ensure meaningful, detailed information is captured and to avoid an overuse of canned/templated responses over time.

The IPC noted that the base DIPE PIA did not include an assessment of the Business Intelligence and Practice Division Data Environment high sensitivity file server (BIPDDE Server) or any of the secure file transfer (SFTP) tools or systems utilized by the MCCSS IMDIU. The DIPE PIA indicated that the BIPDDE Server and any external processes related to data transfer were out of scope. However, the Data Standards identify the DI Environment as all associated system components and information assets of an IMDIU's technology environment that are involved in the collection, linking, use, disclosure, de-identification, retention, transfer, and disposal of PI.[27] The IPC finds that the BIPDDE Server, acting as a staging area for PI to be brought into the DIPE, and SFTP tools are critical components of the information transmission and retention functions of the MCCSS IMDIU's DI Environment. When the MCCSS IMDIU becomes operational, its reliance on the BIPDDE server and SFTP tools could affect the privacy of individuals or the confidentiality of information, and therefore, it is required to conduct a PIA on these components of its program, process, technology, or system.[28] Ultimately, the MCCSS IMDIU is accountable for having an up-to-date understanding of the risks of using such platforms or tools with respect to its role as an IMDIU.

25 See requirements 4.1.2 and 4.1.3 of the Data Standards.

26 The PIA provided to the IPC was assigned version number 2.1 and included placeholders for a summary of mitigation actions and a risk mitigation plan.

27 See Glossary of Terms in the Data Standards.

28 See requirement 4.1.2-2 of the Data Standards.

The IPC acknowledges that some of the systems and tools ministries rely on are administered outside the IMDIU, but this does not affect the fact that the IMDIU and its members are responsible for compliance with Part III.1 and the Data Standards, and it cannot be assumed that risks have been addressed.[29] The requirement to conduct PIAs on all the IMDIU's associated systems and tools and to address the risks raised by the PIAs is one of the most important safeguards of this data integration model.

Given the higher level of residual privacy risks that remain at the time of issuing this report, it is appropriate for the Commissioner to make an order under paragraph 4 of s. 49.12(7) of FIPPA requiring that the MCCSS IMDIU bring itself into compliance with the standards by conducting a PIA(s) on the entire DI Environment, including its components parts, the BIPDDE Server and the SFTP tools or systems, taking into account their new uses related to the IMDIU's role under Part III.1.

Order #1

On or before September 30, 2024, the MCCSS IMDIU must:

a) ensure that an up-to-date PIA(s) has been conducted of the BIPDDE high sensitivity file server and all SFTP/file transfer systems, in compliance with Requirement 4;

b) prioritize and address any recommendations resulting from the PIA(s) to address and eliminate privacy and/or confidentiality risks in a timely manner; and

c) send written confirmation to the IPC of compliance with this order.

Category 2: Collection, Use, and Disclosure

This standard outlines the minimum requirements that the data integration units must meet when collecting, using, and disclosing personal information, coded information, and de-identified information, as applicable. The MCCSS IMDIU must take reasonable steps to ensure the protection of privacy, comply with its legal obligations and ensure that the persons, entities, and organizations it interacts with do the same.[30]

Requirement 5: Collect, use, and disclose personal information, coded information, and/or de–identified information only in accordance with applicable requirements in the Part, the Data Standards, the Practices and Procedures, other applicable provisions of FIPPA and its Regulations, and agreements and acknowledgements made pursuant to them.

Requirement 5 of the Data Standards addresses the practices and procedures that must be in place to ensure that the MCCSS IMDIU only collects, uses, and discloses personal information, coded information and/or de-identified information in accordance with applicable requirements. This includes identifying and defining the restrictions in place on collection, use, and disclosure (including specifying certain minimum restrictions).

29 See s. 49.11 of FIPPA.

30 Sections 49.2 to 49.10 of FIPPA are also relevant to these requirements.

Collection

Requirement 5 has several sub-requirements specifically focused on the collection of personal information and coded information. This includes maintaining an inventory of the personal information and coded information with the MCCSS IMDIU, and a requirement to review this inventory on an annual basis.[31]

The MCCSS IMDIU provided the IPC with its Request Management standard operating procedures, which set out detailed actions to be followed by DIU members throughout the lifecycle of a data integration request or project. This includes practices and procedures related to project intake, assessment, and the conditions that must be met to permit the initial collection of PI or coded information. Specifically, the role of Intaker is identified to assess a project to determine if it meets the minimum requirements and conditions to permit the collection of PI and coded information in compliance with the Data Standards and Part III.1. While it was determined that the practices and procedures meet the requirements and generally set out the need to determine public interest prior to collecting PI or coded information,[32] the IPC requested that the MCCSS IMDIU elaborate on the specific factors DIU members must take into consideration when identifying the anticipated public interest.

The standard operating procedures also outline the actions for creating a data holdings inventory maintained by the Intaker to track the collection of PI and coded information by the IMDIU. The MCCSS DI Compliance Management standard operating procedures further describes the procedure by which the required annual reviews of the inventory are to be conducted.

Based on its review, the IPC is satisfied that the sub-requirements related to collection have been met and are in compliance with the standards set under Requirement 5.

Use

Several specific sub-requirements pertain to the use of personal information and coded information. These address such matters as: identifying and defining requirements and purposes governing the MCCSS IMDIU's use of personal information and coded information and ensuring that this information is only used where it is authorized for defined purposes and where all requirements and conditions have been satisfied.[33]

The MCCSS IMDIU Request Management standard operating procedures focus on uses of personal information and coded information identified at the initial submission of a project request and include provisions limiting the use of PI or coded information in accordance with the DI Standards. They set out a linear project-specific information lifecycle primarily designed around facilitation of a specific data integration request or project. However, it is reasonable to assume that, within the permitted retention periods identified in the Data Standards and the standard operating procedures, future unanticipated projects may arise that require access to the same or similar PI or coded information already collected by the MCCSS IMDIU. If a DI unit's practices and procedures do not reasonably anticipate contingencies, they increase the likelihood that future activities may not be in compliance with Part III.1 and the Data Standards. In that regard, the IPC found that the provided standard operating procedures did not address the re-use of previously collected personal information or coded information.

31 See requirement 5.1 to 5.4 of the Data Standards.

32 See requirement 5.2.5 of the Data Standards.

33 See requirements 5.5 to 5.7 of the Data Standards.

The IPC requested that the MCCSS IMDIU clarify whether it intends to potentially re-use personal information or coded information for such purposes and the MCCSS IMDIU responded that it will update its standard operating procedures to incorporate considerations related to the re-use of already collected PI and coded information.[34]

Given the potential downstream uses of the data that may occur in the future for as yet unknown purposes, the IPC recommends continued engagement with the MCCSS IMDIU to address this subject, and that the MCCSS IMDIU report back to the IPC on the status of this recommendation within a year of this report.

Recommendation to Report Back #1

On or before one year after the date of this report, the MCCSS IMDIU should provide the IPC with an update describing how its practices and procedures have been changed to address the potential re use of personal information and coded information.

Disclosure

Requirement 5 pertains to the disclosure of personal information, coded information, and de-identified information. This includes ensuring that this information is only disclosed to parties and for purposes that are identified and defined, and ensuring that it is only disclosed where it is authorized for defined purposes and where all requirements and conditions have been satisfied.[35] These requirements apply to de-identified information in addition to personal information and coded information, due to the additional risks of re-identification where such information leaves the MCCSS IMDIU.

The IMDIU Request Management standard operating procedures are primarily structured around disclosing information in the context of a specific project or request for which the personal information and/or coded information was originally collected, and generally includes the conditions required to permit the disclosure of PI, coded information, and/or de-identified information. The MCCSS IMDIU also provided the IPC with the Public Notice and Annual Reporting standard operating procedure which further sets out the process to be followed for disclosures related to rights of access or correction.[36]

The IPC identified sections of the Environment Management standard operating procedure that discuss the MCCSS Secure Research Lab, a service that would permit data requestors to access de-identified project files and run their analyses on-site in the MCCSS IMDIU's secure environment. To ensure the final de-identified data output met a project's needs, a report describing the data would be provided to the requestor prior to full de-identification. The IPC applauds the inclusion of a secure data environment into the operational design of the IMDIU which adds another layer of privacy and security controls post-data de-identification. In light of this, the IPC requested that the MCCSS IMDIU expand on its practices and procedures related to the disclosure of data using the Secure Research Lab, as well as incorporate clear criteria and guidelines for DIU members generating any pre-release reports to be shared with requestors in order to ensure no PI or coded information is unintentionally included. The Methodologies and Risk Evaluation Framework developed by the MCCSS IMDIU provides guidance on de-identification techniques and re-identification risk. While the methodology takes into consideration the different data release models (e.g., within the ministry vs. external release), at time of review it was unclear how enabling disclosures of de-identified data through the Secure Research Lab factored into the risk assessment. The IPC requested

34 For greater clarity, the IPC is not suggesting that the MCCSS IMDIU's practices and procedures must only be structured in a particular way, but that they should cover all reasonable anticipated uses (and disclosures).

35 See requirements 5.8 and 5.9 of the Data Standards.

36 See FIPPA s.47.

the Methodologies and Risk Evaluation Framework be updated to provide clarity on how it will be applied to data made available within the Secure Research Lab.

In these circumstances, and given the relative lack of clarity still outstanding at the time of this report, the IPC recommends the necessary revisions be made to the Methodologies and Risk Evaluation Framework and the MCCSS IMDIU report back to the IPC on its implementation within one year of this report.

Recommendation to Report Back #2

On or before one year after the date of this report, the MCCSS IMDIU should provide the IPC with an update describing how it has revised its Methodologies and Risk Evaluation Framework to expand upon its practices and procedures, including its how its de-identification and risk methodology have been revised to account for all considerations related to disclosures using the Secure Research Lab.

Requirement 6: Execute a data sharing agreement (DSA) or obtain a written acknowledgement when collecting or disclosing PI, coded information, and/or de-identified information, where required

Requirement 6 of the Data Standards obligates the MCCSS IMDIU to execute a data sharing agreement (DSA) or obtain a written acknowledgement when collecting or disclosing personal information, coded information, and/or de-identified information, as required.[37]

Data Sharing Agreements

Under this Requirement, Data Sharing Agreements (DSAs) must be executed where reasonably necessary to protect the privacy of individuals and the confidentiality of information, including in specific minimum circumstances. DSAs must be executed prior to the MCCSS IMDIU collecting personal information or coded information from a source outside MCCSS, and before disclosing personal information or coded information to another data integration unit outside the ministry. In certain circumstances, a DSA may also be required where the MCCSS IMDIU is collecting or disclosing de-identified information. Each DSA must include certain minimum content. The MCCSS IMDIU is also required to develop and maintain a log of DSAs executed by the MCCSS IMDIU. The log must contain certain minimum content.

The MCCSS IMDIU Request Management standard operating procedures designate the Intaker as responsible for determining the need for a DSA. The standard operating procedures require that DSAs be executed when reasonably necessary to protect the privacy of individuals, including at a minimum the circumstances listed in Requirement 6.1.2-1 and 6.1.2-2 of the Data Standards, and that the details and status of DSAs are documented in the Data Sharing Agreement Log. A data sharing agreement template addressing the minimum required content of DSAs under section 6.2.2 of the Data Standards was provided, which all DSAs are required to follow.

37 See requirements 6 to 6.9 of the Data Standards.

Written Acknowledgements

Where a DSA is not executed, the Data Standards require that the MCCSS IMDIU obtain a written acknowledgment in relation to a collection or disclosure of personal information, coded information, and/or de-identified information where it is reasonably necessary to protect the privacy of individuals and the confidentiality of information, and in specific minimum circumstances. A written acknowledgement must generally be obtained where the MCCSS IMDIU is collecting personal information or coded information from the broader MCCSS, or where it is disclosing de-identified information to the broader ministry.

The MCCSS IMDIU Request Management standard operating procedures designate the Intaker as being responsible for determining if a written acknowledgement is required. If it is determined that a DSA is not required or will not be executed, a written acknowledgement will be signed in relation to a collection or disclosure of personal information, coded information, and/or de-identified information where it is reasonably necessary to protect the privacy of individuals and the confidentiality of information, including at a minimum, the circumstances listed in Requirement 6.4.2 of the Data Standards. The details and status of written acknowledgements are tracked in the Written Acknowledgement Log. The MCCSS IMDIU provided two written acknowledgement templates, one for written acknowledgements in the context of the MCCSS IMDIU as the collecting entity, and one in the context of the MCCSS IMDIU as the disclosing entity.

The IPC noted that while the written acknowledgement templates generally meet the requirements set out in the Data Standards, in instances of *collection* of personal information, coded information, and/or de-identified information by the IMDIU, the document was structured in a manner that required MCCSS business units outside of the IMDIU that may contribute data to acknowledge and confirm specific requirements that should be the responsibility of the MCCSS IMDIU to ensure under the Data Standards.[38] While the MCCSS IMDIU has discretion how it operationally confirms compliance with the requirements, such as data minimization, it cannot delegate away its accountabilities under the Data Standards and Part III.1. Ultimately, the MCCSS IMDIU remains accountable under the Data Standards and Part III.1 which should be reflected in the written acknowledgements.

The IPC is satisfied that the MCCSS IMDIU's commitment to revise its practices and procedures to address the above comments is sufficient to bring it into compliance with Requirement 6.

Category 3: Secure Retention and Transfer

This standard requires DI Units to put in place safeguards to ensure a safe, protective technology environment for the secure retention and transfer of PI and coded information.

38 See Requirement 6.5.2.9a-c of the Data Standards.

Requirement 7: Ensure that the DI Environment is only accessible to members who require access to it in the performance of their duties under the Part

Requirement 7 of the Data Standards stipulates that the MCCSS IMDIU must identity and define various access management controls and ensure, among other things, that the DI Environment is only accessed by members authorized for defined purposes and circumstances and that all conditions, requirements and restrictions have been satisfied. This includes defining business roles and their access needs, keeping operational roles segregated from security and audit functions[39], ensuring that access is only available in specific approved circumstances and is clearly logged, and that all MCCSS IMDIU members and service providers sign agreements include specific minimum content.

The MCCSS IMDIU provided the IPC with several documents addressing this requirement, including the User Information Management standard operating procedure which covers the management of user access to various business and Information Technology (IT) resources. It requires DIU members to complete mandatory training, sign confidentiality agreements, and meet certain security screening requirements based on their role prior to being granted access to the DI Environment. The IMDIU Manager is responsible for ensuring staff complete onboarding requirements including the execution of confidentiality agreements. The MCCSS IMDIU's User Management Log tracks DIU member mandatory privacy and security training and must be reviewed by the IMDIU manager on an annual basis. The IPC was also provided with a Roles and DI Environment Permissions Mapping table documenting the different DIU member positions and key responsibilities, as well as their access permissions and role in each data environment defined on a project-specific basis.

The Environment Management standard operating procedure addresses the MCCSS IMDIU's use of IT systems and resources, primarily through agreements and relationships with centralized ministry Information and Information Technology (I&IT) clusters that maintain and operate the IT solutions of the ministry.

The Data Standards define the DI Environment as all associated system components and information assets of an IMDIU's technology environment.[40] The IPC found that while the practices and procedures generally set out the necessary steps to ensure the DI environment was accessible only to staff members that required it, the secure file transfer systems and/or services utilized by the MCCSS IMDIU and the BIPDDE high sensitivity file server were not consistently monitored or accounted for in the same manner as the DIPE. As a result, it is unclear if the practices and procedures fully identify the access controls for the DI Environment in its entirety.

The Data Standards also require that the IMDIU execute written agreements with any non-members of the unit who perform a role related to the collection, linkage, use, disclosure, de-identification, transfer, disposal or destruction of PI, coded information, or de-identified information.[41] The MCCSS IMDIU's Environment Management standard operating procedures indicated that MCCSS IT staff involved in providing services to the IMDIU would not be granted access to any personal information and/or coded information and were subject to Ontario Public Service (OPS) privacy and security obligations, therefore were not required to enter into any written agreement with the IMDIU. The IPC finds that it is reasonable to assume that individuals who supply such services (whether on their own behalf or on behalf of another person, entity or organization) are reasonably likely to have incidental access to the MCCSS IMDIU's data during the course of providing their services. Service Level Agreements (SLAs) in place that predate the establishment of the Data Standards

39 Except where duties cannot be segregated across multiple distinct members due to lack of available human resources (e.g., in smaller DI Units). In such case, other appropriate controls such as monitoring of activities and management supervision must be enhanced to achieve the same effect.

40 See definition of DI Environment in the Glossary of the Data Standards.

41 See requirement 7.8 of the Data Standards.

or the designation of MCCSS as an IMDIU cannot be expected to address Requirement 7.8. These service providers would be expected to at a minimum either sign IMDIU specific confidentiality agreements, or the legacy SLAs in place may require revision to ensure alignment with Requirement 7.[42]

Given the significance of the access management-related issues that remain outstanding at the time of issuing this report, the IPC makes the following recommendation to the MCCSS IMDIU and asks for a report back on the status of its implementation within one year.

Recommendation to Report Back #3

On or before one year after the date of this report, the MCCSS IMDIU should provide the IPC with an update describing how it has refined its practices and procedures:

- to address business roles and access controls for the BIPDDE high sensitivity file - server and SFTP/file transfer tools, in compliance with all elements set out in - requirement 7; and -
- to address its relationship with individuals who supply services (whether on their own behalf or on behalf of another person, entity or organization) related to the collection, linkage, use, disclosure, deidentification, retention, transfer, disposal, or destruction of PI, coded information, or de-identified information, and who are not members in accordance with requirement 7.8.

Requirement 8: Implement physical security measures that are reasonable in the circumstances to protect personal information and coded information from theft, loss, and unauthorized use and disclosure

Requirement 8 of the Data Standards addresses the physical security measures that must be in place to protect personal information and coded information from theft, loss, and unauthorized use and disclosure. This includes requiring MCCSS IMDIU practices and procedures with respect to locks, alarms, visitor protocols, workspace security, measures to enable the secure retention of personal information and coded information in non-electronic form, and logging of individuals with access to the MCCSS IMDIU's physical premises. The MCCSS IMDIU's practices and procedures must also ensure that only authorized members and visitors may access its physical premises, ensure that physical security vulnerabilities are resolved in a timely manner, ensure that physical access to the IMDIU premises is immediately revoked when access is no longer needed, and ensure that the retention and transfer of non-electronic storage media is authorized for defined purposes and circumstances, and all conditions, requirements, and restrictions have been satisfied.[43]

The MCCSS IMDIU Environment Management standard operating procedures provided to the IPC address the security measures and visitor access to the IMDIU's physical premises, as well as the physical security measures of the DIPE servers that are housed in the OPS Guelph Data Centre. Given that the MCCSS IMDIU will be providing on-site access to de-identified data outputs in the Secure Research Lab environment, a DI

42 For greater clarity, the IPC is not suggesting that the MCCSS IMDIU's relationship with service providers can only be formalized in this manner.
43 See requirements 8 to 8.3 of the Data Standards.

Requestor Code of Conduct was also provided that covers additional considerations including computer access passwords, security badges, and proper use of MCCSS systems on-site. The IPC found that additional detail should be incorporated regarding alarms, how a visitor will be identified, and the return of passkeys, in addition to including an explicit requirement to conduct reviews and ongoing monitoring of the physical environment and associated security measures.

The MCCSS IMDIU further provided the IPC with the Government of Ontario Information Technology Standards (GO-ITS) 25.18 Data Centre Physical Security Standards Services which addressed physical security measures for such data centres in a manner compliant with the Data Standards and GO-ITS 25.7 Security Requirements for Remote Access. When relying on corporate policies or GO-ITS, the MCCSS IMDIU is encouraged to include additional details within the practices and procedures that identify how the IMDIU complies with these standards, and how the requirements they set out are operationalized within the context of the IMDIU's role under Part III.1.

Based on its review, the IPC is satisfied that the MCCSS IMDIU's policies and procedures are in compliance with the standards set out under Requirement 8.

Requirement 9: Implement security measures that are reasonable in the circumstances to protect personal information and coded information retained and/or transferred in electronic format from theft, loss, and unauthorized use and disclosure

Requirement 9 of the Data Standards addresses the security measures that are reasonably necessary to protect personal information and coded information in electronic format from theft, loss, and unauthorized use and disclosure. These measures include placing all system components that are part of the DI Environment in an internal network zone segregated from the remainder of the network; network security controls; vulnerability management; threat detection and monitoring; and the use of encryption. Among other things, the MCCSS IMDIU must ensure that personal information and coded information are only retained and transferred in electronic format where authorized for defined purposes and circumstances, and that all conditions, requirements and restrictions have been satisfied, and identified vulnerabilities addressed in a timely manner.

Several of the MCCSS IMDIU's standard operating procedures address the security requirements set out under Requirement 9, including User Information Management, Environment Management, and Compliance Management. Various technical documentation was provided to describe the IT/data integration processing environment architecture design in addition to a DI Environment Threat Risk Assessment (TRA).

The IPC found that information was missing related to firewall design and system blueprints that describe the network boundaries between the DI Environment and the remainder of the network, including a description of the firewalls to be put in place, and how they must be configured (e.g., ingress/egress rules), etc.[44] The practices and procedures were found to generally meet the requirements with respect to penetration testing; however, the pen test report that was provided to the IPC did not include full testing of the application and associated databases. Additionally, the IPC found that more detail is required regarding implementation of the anti-malware controls and processes to effectively monitor and detect any attempts to gain unauthorized access to the DI Environment, such as account lockup after a few unsuccessful attempts, enforce delay next available login, etc.[45]

44 See requirement 9.1-2 of the Data Standards.

45 See requirement 9.1-5 of the Data Standards.

The required risk management processes are defined in the Compliance Management standard operating procedures. However, some gaps were identified with respect to clear lines of accountability and responsibility as well as timelines for the MCCSS IMDIU's response to address any identified vulnerabilities or weaknesses, which are required for the practices and procedures to be fully implementable.

The IPC is satisfied that the MCCSS IMDIU's commitment to revise its practices and procedures to address the above comments is sufficient to bring it into compliance with Requirement 9.

Requirement 10: Ensure personal information and coded information are only accessed remotely and/or retained on mobile devices in approved circumstances

Requirement 10 of the Data Standards addresses remote access and mobile retention of personal information and coded information.[46] The MCCSS IMDIU is required to identify and define various items, including requirements, restrictions, methods, and specifications for both remote access and mobile retention. In addition, the MCCSS IMDIU must ensure members only remotely access, or retain on a mobile device, personal information, and coded information where it is authorized for defined purposes and circumstances, and that all conditions, requirements, and restrictions have been satisfied. The MCCSS IMDIU must also ensure that other requirements are addressed such as those relating to data minimization, purpose limitation, encryption, and access management practices are in place.

With respect to remote access, the MCCSS IMDIU's practices and procedures provide that its work is to be all conducted via a remote access connection as all data is stored off-site within centralized data centres. In essence, approval to access the MCCSS IMDIU's DI Environment in general is a form of remote access approval as all user access to DIPE is remote.

The MCCSS IMDIU's Environment Management standard operating procedures define remote access as connections from locations that are not considered part of the managed Government of Ontario network (e.g., home, small remote offices, vendor offices, client sites, or a temporary office). The practices and procedures set out the conditions and purposes that permit remote access, restrictions on use, devices permitted to be utilized, and retention that are aligned with GO-ITS 25.7 Security Requirements for Remote Access Services.[47] The IPC was provided with a User Management Log. However, some required elements were not found including a description of the program applications and the information that the user is authorized to access remotely and/or retain on a mobile device.[48] In general, the IPC recommends the practices and procedures and User Management Log be revised to clearly differentiate between general staff member access to the DIPE remote work environment and remote access on approved mobile devices.

The IPC is satisfied that the MCCSS IMDIU's commitment to revise its practices and procedures to address the above comments is sufficient to bring it into compliance with Requirement 10.

46 See requirement 10 to 10.3 of the Data Standards.

47 See requirement 10.1, 1-5 of the Data Standards.

48 See requirements 10.3.1 and 10.3.2 of the Data Standards.

Requirement 11: Conduct threat and risk assessments and keep and review audit logs as reasonable in the circumstances

Requirement 11 of the Data Standards relates to conducting threat and risk assessments (TRAs) and capturing and reviewing of audit logs.[49] This includes identifying and defining: the circumstances in which a TRA is required (which must be done before the MCCSS IMDIU becomes operational and upon a significant change to the DI Environment); the circumstances in which TRAs must be reviewed and updated (which must be done annually for the most recent TRAs); the required content of TRAs; addressing TRA findings in a timely manner based on severity of risk; and maintaining a log of TRAs. With respect to audit logs, IMDIUs must identify and define the information that must be logged to enable detection and monitoring of privacy and security breaches, including certain mandatory information about computer activities involving personal information or coded information in the DI environment.

Threat and risk assessments

The MCCSS IMDIU's Environment Management and Compliance Management standard operating procedures were reviewed for compliance with this requirement. A TRA was provided by the MCCSS IMDIU that included the two servers that comprise the DIPE, but specifically noted that the BIPDDE High Sensitivity File Server and external business processes, such as transfer of personal information, are out of scope.

The IPC found that the MCCSS IMDIU's practices and procedures related to conducting threat and risk assessments met the requirements set out in the Data Standards. Requirements for conducting TRAs were clearly defined, recommendations resulting for assessments are prioritized accordingly, and logs must be maintained to capture and enable detection and monitoring of privacy and security breaches. However, the IPC was unable to locate one of the required logs to monitor DIU member user IDs/accounts, dates and times of access, identity of devices, etc.[50]

Similar to the IPC's findings for Requirement 4, it was found that the base DIPE TRA did not include an assessment of the BIPDDE High Sensitivity File Server or any of the secure file transfer (SFTP) tools or systems utilized by the MCCSS IMDIU. The Data Standards identify the DI Environment as all associated system components and information assets of an IMDIU's technology environment that are involved in the collection, linking, use, disclosure, de-identification, retention, transfer and disposal of personal information and/or coded information.[51]

The IPC finds that the BIPDDE Server, acting as a staging area or transition zone for personal information and/or coded information and SFTP tools are critical components of the information transmission and retention functions of the MCCSS IMDIU. When the MCCSS IMDIU becomes operational, its reliance on the BIPDDE server and SFTP tools could affect the privacy of individuals or the confidentiality of information and therefore, the MCCSS IMDIU is required to conduct a TRA in accordance with the Data Standards of this program, process, technology, or system.[52] Ultimately, the MCCSS IMDIU is accountable for having an up-to-date understanding of the risks of using such platforms or tools with respect to its role as an IMDIU.

49 See requirements 11 to 11.5 of the Data Standards.

50 See requirements 11.5.2, 1-10 of the Data Standards.

51 See Glossary of Terms in the Data Standards.

52 See requirement 4.1.2-2 of the Data Standards.

The IPC acknowledges that some of the systems and tools ministries rely on are administered outside the IMDIU, but this does not affect the fact that the IMDIU and its members are responsible for compliance with Part III.1 and the Data Standards, and it cannot be assumed that risks have been addressed.[53] The requirement to conduct TRAs on all the IMDIUs associated systems and tools and address risks arising therefrom is one of the most important safeguards of this data integration model.

Given the higher level of residual privacy risks that remain at the time of issuing this report, it is appropriate for the Commissioner to make an order under paragraph 4 of s. 49.12(7) FIPPA requiring that the MCCSS IMDIU conduct a TRA(s) on these component systems and tools in compliance with the standards, taking into account their new uses related to the IMDIU's role under Part III.1.

Order #2

On or before September 30, 2022, the MCCSS IMDIU must:

a) ensure that an up-to-date TRA(s) has been conducted of the BIPDDE high sensitivity file server and SFTP/file transfer systems, in compliance with Requirement 11;

b) prioritize and address any recommendations resulting from the TRA(s) to address and eliminate privacy and/or confidentiality risks in a timely manner; and

c) send written confirmation to the IPC of compliance with this order.

Requirement 12: Develop and implement a process to manage changes to the DI Environment

Requirement 12 of the Data Standards requires the MCCSS IMDIU to develop and implement a process to manage changes to the DI Environment. This includes both vendor-supplied changes (i.e., patches or updates) as well as requested changes (e.g., internal requests). Change management must include establishing processes for the monitoring and review of vendor-supplied changes; requesting changes; deciding if a change should be implemented; prioritizing changes; and testing changes. Changes must be documented with certain minimum information captured for each change.

The MCCSS IMDIU Compliance Management standard operating procedure primarily addresses requirements related to changes in the DIPE. Within the IMDIU, a change request can be submitted by any member which must be approved by the DIU Manager. Once approved, the Administrator assesses the request based on certain criteria. The Data Standards require that the IMDIU include specific minimum processes to manage changes to the DI environment. While the Compliance Management standard operating procedure along with the provided Change Request Form and Changes to DIPE log outline the general process of change requests, some of the specific details set out in the requirements were not found, and the IPC requested revisions accordingly.[54]

The IPC is satisfied that the MCCSS IMDIU's commitment to revise its practices and procedures to address the above comments is sufficient to bring it into compliance with Requirement 12.

53 See s. 49.11 of FIPPA.

54 See requirement 12.1.2, 1-5

Requirement 13: Ensure that personal information and coded information is backed up in a manner that allows it to be fully recovered, and that the DI Unit has an effective business continuity and disaster recovery plan

Requirement 13 of the Data Standards stipulates that the MCCSS IMDIU must ensure that personal information and coded information are backed up in a manner that allow the information to be fully recovered, and that the MCCSS IMDIU has an effective business continuity and disaster recovery plan.

With respect to back-ups, this includes identifying and defining the nature and types of backup storage media used, backup frequencies, the circumstances in which backed-up material is required to be made available, and the processes for backup and recovery methods as well as their testing.[55]

With respect to business continuity and disaster recovery, a plan must be identified and documented to describe how the MCCSS IMDIU responds to short and long-term business interruptions and threats to its operating capabilities. The plan must include procedures to address subjects including notification of threat and interruption events, assessing severity of threats and interruptions, the circumstances in which the plan is activated, determining the effort required to recover from the event, identifying and prioritizing the recovery of critical business functions, among other aspects.[56]

Both backup and recovery methods and the business continuity and disaster recovery plan must be tested on at least an annual basis, with findings from the tests documented and resulting recommendations addressed in a timely manner.

The MCCSS IMDIU provided the IPC with several documents that address this requirement. The MCCSS User and Information Management standard operating procedures includes a section entitled 'Data Maintenance' that indicates in the event of an outage or business disruption the Administrator must follow the Continuity of Operations Plan (COOP) developed for the Data Strategy and Solutions Platform (DSSP) in the Business Intelligence and Practice Division (BIPD) of MCCSS. The COOP provides high level information and procedures how to respond and recover from a business disruption. The process for restoration of backup files involves the MCCSS IMDIU submitting a ticket to IT to receive the backup files, used by the Administrator to restore the database(s). Testing of back-ups is carried out by the Administrator by creating a virtual machine. Additionally, the Compliance Management standard operating procedures under 'Continuity Management' describe the COOP for the DIPE and assign responsibility to the Administrator to ensure it is followed. The IPC found that the MCCSS IMDIU's practices and procedures were sufficient to meet some aspects of the Data Standards, however key details regarding the nature and types of back-up storage maintained by the IMDIU were not found.

The IPC finds that the MCCSS IMDIU's COOP along with the associated practices and procedures do not provide sufficient detail to constitute a full business continuity and disaster recovery plan in compliance with the Data Standards.

Given the critical importance of effective business continuity and disaster recovery plans for protecting the privacy of individuals, it is appropriate for the Commissioner to make an order under paragraph 4 of s. 49.12(7) of FIPPA that the MCCSS IMDIU implement a business continuity and disaster recovery plan that complies with Requirement 13.

55 See requirement 13.1 of the Data Standards.

56 See requirement 12.2 of the Data Standards.

Order #3

On or before September 30, 2024, the MCCSS IMDIU must:

a) ensure the implementation of a business continuity and disaster recovery plan that applies to the items listed in requirement 13.2.2; and

b) send written confirmation to the IPC of compliance with this order.

Requirement 14: Respond to privacy and security breaches in a timely and appropriate manner

Requirement 14 of the Data Standards requires the MCCSS IMDIU to establish practices and procedures for responding to privacy and security breaches in a timely and appropriate manner. This includes identifying and defining procedures to identify, report, contain, notify, investigate, and remediate actual or suspected breaches. This further includes ensuring that MCCSS IMDIU members report actual or suspected breaches at the first reasonable opportunity and that privacy and security breach investigations cover a number of aspects, including ensuring that all reasonable steps are taken to prevent future breaches and assessing their effectiveness. Privacy breaches and security breaches are defined in the glossary to the Data Standards.[57]

The MCCSS IMDIU's privacy and security breach response processes are found in the Compliance Management standard operating procedure, as well as several associated business documents and templates. Detailed instructions are set out for all IMDIU staff members to follow in identifying, documenting, and responding to a privacy breach, along with examples. The DIU Manager is identified as being responsible for notifying the MCCSS Access and Privacy Office once a breach is detected and is the key point of contact. To prevent and monitor security breaches, the MCCSS IMDIU will conduct annual reviews of TRAs and systems testing.

The IPC found that the practices and procedures to be followed where an incident is both a privacy and security breach (either potential or confirmed), and the process by which the necessary parties will collaborate to identify and address the breach were unclear and should be further developed.[58] Additionally, the process for determining when notification to the affected individuals, the manner in which notification will be provided, and the content that must be communicated within the notice was unclear.[59] During the review process the MCCSS IMDIU referenced a corporate MCCSS Access and Privacy Office Privacy Breach Protocol document, however the IPC determined at time of review that this document did not address all the considerations required by the Data Standards.

The IPC is satisfied that the MCCSS IMDIU's commitment to revise its practices and procedures to address the above comments is sufficient to bring it into compliance with Requirement 14.

57 Data Standards, p.55.

58 See requirement 14.2.2 of the Data Standards.

59 See requirement 14.2.4-5 of the Data Standards.

Category 4: Secure Disposal and Secure Destruction

This category of Data Standards requires that the MCCSS IMDIU ensure the secure disposal or destruction of personal information or coded information and related storage media.[60]

The Data Standards distinguish between secure disposal or destruction of personal information or coded information and related storage media, and the deletion of information. "Secure disposal or destruction" is a higher standard that requires the permanent removal of information from a storage medium such that its reconstruction or retrieval is not reasonably foreseeable in the circumstances.[61] "Deletion" is a lower standard that refers to the removal of all electronic references to information or, in the case of non-electronic storage media, physical access to information.[62] To reach the higher standard of secure disposal or destruction, additional actions that would have to be taken, such as destroying the underlying storage media (e.g., physical destruction).

Requirement 15: Dispose of or destroy personal information, coded information, and the storage media containing the information promptly and in a secure manner

The Data Standards require that the MCCSS IMDIU identify and define methods for securely disposing of and destroying personal information and coded information and related storage media, taking into account the type of information and storage media. The Data Standards further establish certain minimum conditions under which personal information and coded information and the storage media containing the information must be securely disposed of or destroyed.[63]

The MCCSS IMDIU User and Information Management standard operating procedure states that it will use SDelete, a command line utility within the DIPE, that allows files to be securely destroyed and meets GO-ITS standards for Magnetic Storage Media Overwriting Process, as well as the conditions under which personal information and/or coded information must be securely disposed or destroyed. The DIU manager is responsible for monitoring data retention periods and ensuring the secure disposal/destruction of personal information/and or coded information as authorized by the DIU Director. The policies account for the secure electronic removal of information from the environment, as well as disposal/destruction of computerized devices and digital storage media, if applicable.

Based on its review, the IPC is satisfied that the MCCSS IMDIU's policies and procedures meet the standards set out under Requirement 15.

Requirement 16: Retain and transfer personal information, coded information, and the storage media containing the information in a secure manner pending disposal or destruction

The Data Standards require the MCCSS IMDIU to identify and define a secure physical area and clearly marked and locked containers for retaining personal information and coded data and related storage media pending secure destruction or disposal. The MCCSS IMDIU must further identify and define a procedure for securely transferring personal information and coded data and related storage media outside the unit for disposal or destruction and ensure that several protective goals are met.[64]

60 Sections 49.11(1)(a) and (d) of FIPPA are also relevant to this requirement.
61 Data Standards, p. 55
62 Data Standards, p. 54
63 See requirements 15 to 15.2 in the Data Standards.
64 See requirements 16 to 16.2 in the Data Standards.

The MCCSS IMDIU operates in a fully virtual environment and has indicated that all personal information and coded information is retained on centrally managed Ontario government computer servers. For that reason, most of Requirement 16 has little direct application to the activities of the MCCSS IMDIU since there are no local storage media to be retained and transferred. With respect to the destruction of storage media in centrally managed computer services (i.e., DIPE), the GO-ITS Standard 25.20: Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media requires that all functioning electronic storage media be securely overwritten prior to physical destruction.

Non-functioning storage media that cannot be overwritten must be kept in a secure chain of custody until physically destroyed. The MCCSS IMDIU provided a Records Disposition Report that documents the records eligible for disposition and confirms that they have been reviewed and authorized for disposition by the DIU Director. The IPC found that details regarding where system backups are physically located and in what type of media or format were missing, and requested the practices and procedures be updated accordingly.

The IPC is satisfied that the MCCSS IMDIU's commitment to revise its practices and procedures to address the above comments is sufficient to bring it into compliance with Requirement 16.

Requirement 17: Verify that personal information, coded information, and the storage media containing the information, has been disposed of or destroyed in a secure manner

The Data Standards require that the MCCSS IMDIU's practices and procedures identify and define the required content of certificates of secure disposal or destruction, including certain minimum content.[65] The MCCSS IMDIU's practices and procedures must identify and define timeframes for obtaining certificates of secure disposal or destruction, and the time period and location for retaining these certificates. Further, the MCCSS IMDIU's practices and procedures must ensure that certificates of secure disposal or destruction are obtained for each storage media securely disposed of or destroyed, that a log of transfers for secure disposal or destruction and received certificates of secure disposal or destruction is maintained, and that the destruction and disposal methods are periodically reviewed for effectiveness.

The MCCSS IMDIU's User and Information Management standard operating procedures refer to certificates of secure disposal or destruction as a required artifact upon completion of disposal or destruction of storage media. The MCCSS IMDIU indicated that in some instances this certificate would be issued by a third-party vendor commissioned by the OPS. A template or copy of the certificate of secure disposal or destruction was not provided to the IPC at time of review. While the practices and procedures indicate the certificate meets the set requirements for content, they do not indicate how compliance is to be achieved or set out the procedures the IMDIU will use to ensure the required information is in fact generated.

Under GO-ITS 25-20, a certification of completion must be made available to the program manager accountable for the disposal of storage media after the media is successfully disposed of. This certification is required to contain all of the minimum content required under requirement 17.1.2 of the Data Standards. While the IPC understands that the MCCSS IMDIU is relying on corporate policies and in certain instances third-party vendors to issue certificates of destruction/disposal, the MCCSS IMDIU should clarify any procedures they may have in place with respect to obtaining the certifications required under GO-ITS 25-20 and the Data Standards, and clearly set out the required timeframes within the practices and procedures.

The IPC is satisfied that the MCCSS IMDIU's commitment to revise its practices and procedures to address the above comments is sufficient to bring it into compliance with Requirement 17.

65 See requirement 17.1.2.

Category 5: Retention Period

Requirement 18 of the Data Standards outlines requirements for practices and procedures relating to how long the MCCSS IMDIU can or must retain personal information and coded information.[66] It addresses minimum retention periods (e.g., the length of time that the information must be retained) and maximum retention periods (e.g., a length of time after which the information cannot be retained). Minimum retention periods help to ensure that there is a reasonable amount of time to exercise the individual right of access and correction. Maximum retention periods help to protect against privacy breaches arising from the unnecessary retention of information, among other things.[67]

Requirement 18: Implement retention requirements for personal information and coded information

The Data Standards require that the MCCSS IMDIU identify and define a process for determining the retention period for personal information and coded information, and identifies some of the factors that must, at a minimum, be considered in setting retention periods. In addition to this general process for determining retention periods, the Data Standards set specific minimum and maximum retention periods:

- Requirement 18.1.2 states that personal information in the record created by the MCCSS IMDIU for linking under requirement 20.3 (i.e., the ID Mapping Table) must be retained for long enough to facilitate individual rights of access;
- Requirement 18.1.3 states that coded information must be retained for at least one year after completion of de-identification and delivery of the de-identified information to the requesting person, entity, or organization (again, the purpose of this requirement is to facilitate the individual right of access); and
- Requirement 18.2 states that original non-coded personal information must be retained for a maximum period of 180 calendar days after its transformation into coded information to enable accurate linking. The purpose of this requirement is to ensure that 'raw' data in its original form is only retained for the minimal amount of time necessary to remove direct identifiers and link the information. This limits privacy risks associated with retaining data in a format where it is directly, readily, and immediately identifiable. There are possible exceptions to this 180-day retention requirement in specific circumstances.

The MCCSS IMDIU User and Information Management standard operating procedures address this requirement. Responsibility is assigned to the DIU Manager to work with the MCCSS Records Management Unit (RMU) to define the IMDIU's general record series and develop the unit's records retention schedules. The MCCSS IMDIU's practices and procedures indicate that a spreadsheet titled Data Holdings Inventory will be used to track arrival, creation, and destruction of data sets, as well as the associated retention periods. The practices and procedures define the required retention period for each class of personal information. Where the MCCSS IMDIU has discretion to set its own maximum retention period, coded information would be subject to a maximum retention period of the current calendar year plus one year.

The Record Series Summary Report outlines the retention and disposition policies based on the information series classification. The IPC found that it was unclear how record retention dates will be tracked or implemented with respect to ongoing data collections in a series. While ongoing data collections are contemplated within the practices and procedures, the IPC requested revisions to the standard operating procedures and reporting

66 Requirement 18 only mandates the deletion of personal information and coded information but does not address the secure disposal or destruction of the deleted information, which is addressed above in relation to requirements 15, 16, and 17.

67 Sections 49.6(1)4 and 49.11(1)(c) of FIPPA are also relevant to the minimum and maximum retention periods applicable to the MCCSS IMDIU but are subject to variations or further specifications in the Data Standards.

templates to ensure clarity on the process for tracking and implementing the defined record retention schedules in scenarios where there is ongoing collection of data. Additionally, while not explicitly required under the Data Standards, the IPC recommends the MCCSS IMDIU establish a retention period(s) for de-identified data and document this accordingly.

Based on its review, the IPC is satisfied that the MCCSS IMDIU's policies and procedures meet the standards set out under this requirement.

Category 6: De–Identification and Linking

Under Requirement 19, the MCCSS IMDIU must implement an accurate, privacy-protective de-identification and linking process, transforming personal information that has been collected under Part III.1 into coded information that can be used for analysis.[68] Sections 49.1(2), 49.4(1)5, 49.4(2)5 and 49.6 of FIPPA are also relevant to requirements for linking and de-identifying information.

Requirement 19: Segregate duties in relation to coding and linking

The Data Standards require that the MCCSS IMDIU separate the roles for data coding (i.e., removing direct identifiers and placing them with a secure unique code) and data linking (i.e., using the secure unique code to link records in separate datasets). Separation of these roles in the coding and linking processes must be ensured using administrative, technical, and physical safeguards that are reasonable in the circumstances. The purpose of this requirement is to ensure that no single member has control of the coding and linking process, which could result in that member having the ability to directly identify and link the information of a large volume of Ontarians. Where duties cannot be segregated due to a lack of available human resources, the Data Standards state that an equivalent standard must be met through other safeguards.

The Request Management standard operating procedures outline two distinct roles for a Data Coder and a Data Linker. The Data Coder is responsible for implementing data matching methodologies, generating a unique project linking ID and assigning values to the mapping table. The Data Linker is responsible for conducting linkages between coded datasets using the mapping table that was generated. Within the practices and procedures, the Administrator is also described as having a role with respect to the coding of personal information, being responsible for confirming incoming datasets are accurate and complete, and assigning unique project IDs to the personal information (or confirming if IDs for records already exist).

The practices and procedures further describe the role-based access permissions that are implemented to ensure the separation of duties. For example, the Data Linker is only permitted access to the coded data and the mapping table created by the Data Coder to ensure they do not have access to any source personal information or original identifiers. In scenarios where a DIU member must carry out multiple roles to facilitate an integration project, their access to database tables and workspaces is restricted, and reset between different roles (i.e., access permissions for their current role must be revoked before access permissions for their next role are granted). DIU members are not permitted to act in multiple roles simultaneously. To facilitate this, the MCCSS IMDIU provided the IPC with the DII Roles and DI Environment Permissions Mapping document, which is generated for each unique data integration project and tracks the relevant permissions granted to DIU members.

Based on its review, the IPC is satisfied that the MCCSS IMDIU's policies and procedures meet the standards set out under Requirement 19.

68 Data Standards, p. 43.

Requirement 20: As soon as reasonably possible in the circumstances, transform personal information collected by the MCCSS IMDIU into coded information

The Data Standards require that the MCCSS IMDIU begin transforming the personal information it collects into coded information as soon as "reasonably possible in the circumstances." The purpose of this requirement is to ensure that the original personal information collected by the MCCSS IMDIU is not left in its most identifiable format any longer than necessary to complete the coding and linking process.

The Data Standards further specify minimum requirements for how the coding and linking process must take place, including that the MCCSS IMDIU must identify and define minimum common direct identifiers necessary for linking, and ensure that direct identifiers are removed and replaced with a secure internal code unique to the individual. The direct identifiers that have been removed are placed in a mapping table that explains how to connect the assigned secure internal code with the common identifiers.[69]

The provided Request Management standard operating procedures in addition to the Data Field Classification Framework generally provide the details required to address compliance with this requirement. The Data Field Classification Framework serves as a look-up table for common data fields and their associated data classification rating to assist in the identification of various direct and indirect identifiers and streamline the coding and de-identification process.

Based on its review, the IPC is satisfied that the MCCSS IMDIU's policies and procedures meet the standards set out under Requirement 20.

Requirement 21: Link coded information to other coded information, where necessary for analysis

The Data Standards require that the MCCSS IMDIU identify: the methods that must be used to link coded information; the risks to the accuracy of such linkages; and how such risks to accuracy will be mitigated. The Data Standards further state that the MCCSS IMDIU must ensure that coded information is only linked in approved circumstances (among other requirements) and that the accuracy of linkages must be tested. Further, the Data Standards mandate that the MCCSS IMDIU periodically review linkages made to ensure they are accurate.[70]

The MCCSS IMDIU Request Management standard operating procedures set out the general process for conducting data matching and linking. Record matching and linking occurs on a project-basis and the methodology applied is guided by the Methodologies and Risk Evaluation Framework for Data Linking and De-identification. This process begins with the Data Coder generating the key mapping database containing project-specific linking IDs, as well as information regarding the matching process. The Data Coder is responsible for updating the MCCSS IMDIU's De-identification and Linkage Specification template which identifies and documents the risks to the accuracy of linkages and how these risks will be mitigated. The Data Coder must also produce a Record Matching Report that indicates the methods of matching used in the project, the quality of matching and the testing, and/or validation performed to ensure the quality of the matches.

69 See requirements 20 to 20.3 of the Data Standards.

70 See requirements 21 to 21.2 of the Data Standards.

The IPC was unable to locate clear practices and procedures to be followed for specific records if they are unable to be matched or linked accurately. The practices and procedures indicate that if the matching threshold determined for a specific project/dataset cannot be reached, the requestor will be consulted, however, it is unclear how this process connects with other relevant practices and procedures. This is important as coders and linkers should have clear guidance on what to do with personal information and/or coded information where the linkage process and accuracy risk assessment does not resolve to an acceptable solution. The IPC requested revisions to clarify the steps taken when records cannot be matched or linked accurately.

The IPC is satisfied that the MCCSS IMDIU's commitment to revise its practices and procedures to address the above comments is sufficient to bring it into compliance with Requirement 21.

Requirement 22: De–identify coded information prior to analysis

Information is required to be de-identified prior to it being used for analysis in relation to:

- the management or allocation of resources;
- the planning for the delivery of programs and services provided or funded by the Government of Ontario; and
- evaluation of those programs and services.

In some respects, this requirement prescribes the most critical protections in the data integration scheme of Part III.1. The overarching purpose of this legislative scheme is to allow the government to get the benefit of high-quality datasets for analysis, while minimizing risks that any individual could be identified in these datasets. The core tasks for the MCCSS IMDIU in limiting the identifiability of individuals in the datasets are to effectively calculate the risk of re-identification and implement a methodology for decreasing this risk to the appropriate threshold prior to its use for analysis.

To this end, Data Standards require that the MCCSS IMDIU identify and define the criteria to be used in calculating the risk of re-identification. The Data Standards further require that the MCCSS IMDIU identify a risk-based de-identification methodology (with certain minimum steps) and ensure that methodology is applied to coded information prior to its use for analysis. The Data Standards further contain ancillary requirements relating to documentation.[71]

The IPC found that the MCCSS IMDIU's practices and procedures, along with the Methodologies and Risk Evaluation Framework for Data Linking and De-identification, address this requirement. Specifically, the Methodologies and Risk Evaluation Framework was found to address re-identification risk and establish a risk-based de-identification methodology. The remainder of the requirements were determined to be met through various business artifacts and documentation, such as the De-identification and Linkage Specification Template and the Re-identification Risk Assessment Report.

Based on its review, the IPC is satisfied that the MCCSS IMDIU's policies and procedures meet the standards set out under Requirement 22.

71 See requirements 22 to 22.3 of the Data Standards.

Category 7: Public Notice and Annual Reporting

This final part of the Data Standards outlines the minimum requirements for the MCCSS IMDIU to ensure openness and transparency with respect to its information practices.[72]

Requirement 23: Publish a notice of collection that relates to the personal information to be collected under the Part

Requirement 23 of the Data Standards mandates that the MCCSS IMDIU publish a notice that includes the information specified in requirements 23.2 to 23.8 prior to each new collection of personal information. The purpose of the requirement to publish notices of collection is to provide transparency to the public and individuals on how personal information has been collected for analysis purposes by a data integration unit.

The MCCSS IMDIU provided the IPC with its Request Management and Public Notice and Annual Reporting standard operating procedures, as well as a Notice of Collection template to address compliance with the obligations set out in requirement 23 of the Data Standards. The IPC found that the necessary practices and procedures were in place to ensure that Notices of Collection are published prior to a collection of new personal information.

Based on its review, the IPC is satisfied that the MCCSS IMDIU's policies and procedures meet the standards set out under Requirement 23.

Requirement 24: Publish a complete list of notices of collection published by the DI Unit

Requirement 24 of the Data Standards requires that the MCCSS IMDIU develop and maintain a list of published notices of collection that contains all the information identified in Requirement 24.1.2, while linking each item to the respective individual notices of collection published under requirement 23. The purpose of this requirement is to ensure that the public can access an organized list of notices of collection, containing high level details about the projects undertaken by the MCCSS IMDIU with the personal information collected when desired.

For the requirement, the IPC again reviewed the Public Notice and Annual Reporting standard operating procedures as well as the Notice of Collection template and the Notices of Collection Log. The MCCSS IMDIU practices and procedures contained well defined requirements and processes that aligned with the obligations set out in Requirement 24.

Based on its review, the IPC is satisfied that the MCCSS IMDIU's policies and procedures meet the standards set out under Requirement 24.

Requirement 25: Publish a report on the use of personal information to link and de-identify, and to conduct an audit

Requirement 25 of the Data Standards mandates that the MCCSS IMDIU publish a report on the use of personal information to link and de-identify, which includes, at a minimum, the list of personal information and coded information developed and maintained under requirement 25.3 and descriptions of audits undertaken under s.49.7(1)(b).

72 Data Standards, p.47.

Requirement 25.3 stipulates that the MCCSS IMDIU develop and maintain a list of datasets retained by the MCCSS IMDIU of:

- identifiers retained for use in assigning internal identifiers and linking under Requirement 20.3; and
- coded information.

The datasets list must include, at a minimum, the six elements identified in requirement 25.3.2.

Requirement 25.1 further states that the IMDIU may combine this report with the annual report under Requirement 26.

The MCCSS IMDIU provided the IPC with practices and procedures addressing this requirement, including the Annual Report Template which indicates how this template will be used to comply with the reporting on use obligations in requirement 25. In the Public Notice and Annual Reporting standard operating procedure, it is noted that the MCCSS IMDIU intends to meet requirements 25 and 26 through a single report, via the annual report publishing process set out below.

Based on its review, the IPC is satisfied that the MCCSS IMDIU's policies and procedures meet the standards set out under Requirement 25.

Requirement 26: Publish an annual report that relates to the collection, use, de-identification, linkage, and disclosure of personal information collected under the Part

Requirement 26 of the Data Standards states that the MCCSS IMDIU must ensure that an annual report is published on or before April 1 in the year following the report coverage period, covering the period from January 1 to December 31. The Data Standards require that the MCCSS IMDIU include, in its annual report, the information identified in 26.2 to 26.6.

The MCCSS IMDIU provided the IPC with practices and procedures addressing this requirement as well as the Annual Report template. The IPC found that the standard operating procedures contained detailed instructions setting out the responsibility for creating and publishing the annual report in a manner that satisfies Requirement 26. The IPC noted however that the MCCSS IMDIU intends to publish its annual reports on the Government of Ontario Open Data Catalogue webpage.[73] While this is within the IMDIU's discretion, the IPC recommended that clear connections be made between the Open Data Catalogue that will host the MCCSS IMDIU's annual reports, and the general public-facing website established to meet other public transparency requirements (including the published Notices of Collection) on the MCCSS Personal Information Management webpage to ensure members of the public can easily locate and access the report.[74]

The IPC is satisfied that the MCCSS IMDIU's commitment to revise its practices and procedures to address the above comments is sufficient to bring it into compliance with Requirement 26.

73 See https://data.ontario.ca/ -

74 See Ministry of Children, Community and Social Services personal information management | ontario.ca

Requirement 27: Respond to and address privacy complaints and inquiries from the public in a timely manner

Requirement 27 states that the MCCSS IMDIU must identify and define how a member of the public may make a privacy complaint and inquiry related to its activities. The Data Standards further require that the MCCSS IMDIU's process for the public to make privacy complaints and inquiries must include the three pieces of information defined in requirement 27.1.2. The MCCSS IMDIU is further required to identify and define the procedures and timelines to be followed for: receiving; documenting; tracking; investigating; remediating; and responding to privacy complaints and inquiries from the public.

The Data Standards require that the MCCSS IMDIU's procedure to respond to privacy complaints and inquiries include, at a minimum, the five factors identified in requirement 27.2.2. The MCCSS IMDIU is further required to develop and maintain a log of privacy complaints received, and this log must contain minimum content set out in Requirement 27.3.

The MCCSS IMDIU provided the IPC with practices and procedures aligning with the requirements for public complaints and inquiries. These standard operating procedures address: responding to privacy complaints and inquiries in a timely manner; to whom such complaints or inquiries are shared after they are received; the process for logging complaints and inquiries; and the members of the MCCSS IMDU responsible for assessing and responding to a complaint or inquiry. The Public Notice and Annual Reporting standard operating procedures specify that questions regarding the collection, use and disclosure of personal information for the purposes of Part III.1 will be directed to the DIU Director, while general questions about the collection of personal information by the ministry at-large, and all privacy complaints, will be directed to the MCCSS Access and Privacy Office. The MCCSS IMDIU also provided the IPC with a template to be used for logging inquiries and privacy complaints it receives.

In addition to the above documentation, the IPC also reviewed the MCCSS Personal Information website intended to address the information that is required to be made public about its process for addressing privacy complaints and inquiries.[75] At time of review, the MCCSS Information Management web page did not contain all of the required public complaints and inquiries content defined under requirement 27.2.2. It was also noted that the referenced MCCSS Freedom of Information page also did not provide the minimum information specified under requirement 27.[76] The IPC requested that the MCCSS IMDIU update its webpage to include a clear detailed process for members of the public to submit privacy complaints and inquiries that aligns with requirement 27.

The IPC is satisfied that the MCCSS IMDIU's commitment to revise its practices and procedures and public-facing content to address the above comments is sufficient to bring it into compliance with Requirement 27.

75 See sections 27.2.2-27.2.4 of the Data Standards.

76 See https://www.ontario.ca/page/freedom-information-foi-requests-ministry-children-community-and-social-services

Appendix A: Summary Orders and Recommendations to Report Back

Order #1

On or before September 30, 2024, the MCCSS IMDIU must:

a. ensure that an up-to-date PIA(s) has been conducted of the BIPDDE high sensitivity file server and SFTP/file transfer systems, in compliance with Requirement 4;

b. prioritize and address any recommendations resulting from the PIA(s) to address and eliminate privacy and/or confidentiality risks in a timely manner; and

c. send written confirmation to the IPC of compliance with this order.

Order #2

On or before September 30, 2024, the MCCSS IMDIU must:

a. ensure that an up-to-date TRA(s) has been conducted of the BIPDDE high sensitivity file server and SFTP/file transfer systems, in compliance with Requirement 11;

b. prioritize and address any recommendations resulting from the TRA(s) in a) to eliminate or reduce identified threats and vulnerabilities in a timely manner based on severity of risk; and

c. send written confirmation to the IPC of compliance with this order.

Order #3

On or before September 30, 2024, the MCCSS IMDIU must:

a. ensure the implementation of a business continuity and disaster recovery plan that applies to the items listed in requirement 13.2.2; and

b. send written confirmation to the IPC of compliance with this order.

Recommendation to Report Back #1

On or before one year after the date of this report, the MCCSS IMDIU should provide the IPC with an update describing how its practices and procedures have been changed to address the re use of personal information and/or coded information.

Recommendation to Report Back #2

On or before one year after the date of this report, the MCCSS IMDIU should provide the IPC with an update describing how it has revised its Methodologies and Risk Evaluation Framework to expand upon its practices and procedures, including its how its de-identification and risk methodology have been revised to account for all considerations related to disclosures using the Secure Research Lab.

Recommendation to Report Back #3

On or before one year after the date of the IPC's report, the MCCSS IMDIU should provide the IPC with an update describing how it has refined its practices and procedures:

a. to address business roles and access controls for the BIPDDE high sensitivity file server - and SFTP/file transfer tools, in compliance with all elements set out in requirement 7; and -

b. to address its relationship with individuals who supply services (whether on their own behalf or on behalf of another person, entity or organization) related to the collection, linkage, use, disclosure, deidentification, retention, transfer, disposal, or destruction of PI, coded information, or de-identified information, and who are not members in accordance with requirement 7.8.

Appendix B: List of Submitted Practices and Procedures and Representations

Standard Operating Procedures

- BIPD.SOP_0.General Information_(v5.0 2023-06-09)
- BIPD.SOP_1.RequestManagement_(v5.0 2023-06-09)
- BIPD.SOP_2.UserAndInfoManagment_(v5.0 2023-06-09)
- BIPD.SOP_3.EnvironmentManagement_(v5.0 2023-06-09)
- BIPD.SOP_4.ComplianceManagement_(v5.0 2023-06-09)
- BIPD.SOP_5.PublicNoticeAndAnnualReporting_(v5.0 2023-06-09)

Supporting Documents/Business Artifacts

- 0.0 DIU PIA 2022 Mitigation Plan_v2_2023-06-07
- 0.0 MCCSS FIPPA DOA 2020
- 0.0 Privacy Impact Assessment 2022-09-14
- 0.0 PT2022-092 DII Environment - BIPD Penetration Test Report
- 0.0 Threat Risk Assessment_final draft_2023-06-09
- 0.0 TRA Mitigation Plan_v1_2023-05-31
- 1.1.C.01 Data Field Classification Framework_v1.0
- 1.1.C.02 Data Sharing Agreement (DSA) Log_v2.0
- 1.1.C.04 De-identification and Linkage Specification Template_v2.0
- 1.1.C.05 DI Approved Secure File Transfer Services_v2.0
- 1.1.C.06 DI Request Form_v2.0
- 1.1.C.06a DI Request Form - Data Dictionary_v1.0
- 1.1.C.07 DI Request Project Log_v3.0
- 1.1.C.09 MCCSS Approval Form_v1.0
- 1.1.C.10 MCCSS Decision Note Template_v3.0
- 1.1.C.11 PIA LOG_v2.0
- 1.1.C.12 Privacy Assessment Template_v1.0
- 1.1.C.13 DI - Written Acknowledgment (Collection)_v2.0
- 1.1.C.14 Written Acknowledgements (WA) Log_v1.0
- 1.2.C.01 Data Holdings Inventory_v.2.0
- 1.3.C.04 Deidentification-Guidelines-for-Structured-Data
- 1.3.C.05 Re-identification Risk Assessment Report v1.0
- 1.3.C.07 Record Matching Report Template_v1.0
- 1.3.C.08 Methodologies and Risk Evaluation Framework (MREF)v1
- 1.4.C.04 DI - Written Acknowledgment (Disclosure)_v2.0
- 2.1.C.01 Access Change Request Form
- 2.1.C.02 DII Roles and DI Environment Permissions Mapping_v2.0
- 2.1.C.03a P&S Training Module 1 - Introduction to DI & FIPPA v2.0
- 2.1.C.03b P&S Training Module 2 - Protecting Data Privacy and Security v2.0
- 2.1.C.03c P&S Training Module 3 - Collection, Use and Disclosure v2.0
- 2.1.C.03c P&S Module 4 - Role-based Training_2023-06-12
- 2.1.C.04 User Confidentiality Agreement_v4.0
- 2.1.C.05 User Management Log_v3.0

- 2.1.C.06 Confirmation of Mandatory Privacy Training
- 2.2.C.03 Records Disposition Report_v 3.0
- 2.2.C.04 2022-10-28 Records Series Summary Report - Under Review
- 3.1.C.01 DI Processing Environment Hardware and Software Inventory_v1.0
- 3.1.C.02 DI Processing Environment Design_v2.0
- 3.1.C.04 WIA0012652-Prod SqlServer 2017-Machine Learning DWB V1.4
- 3.1.C.05 - Change Request Documentation_v.2.0
- 3.1.C.05 Change Request Documentation_v1.0
- 3.2.C.02 Visitor Signin Sheet_v1.0
- 3.2.C.04 DI Requestor Code of Conduct v1.0
- 3.2.C.04 DIU Member Access Secure Lab Log_v1.0
- 3.3.C.01 Privacy-Impact-Assessment-Guide-January-2016-REV-2019
- 3.3.C.03 TRA, PEN TEST and VS Tracking Log_v2.0
- 3.4.C.01 DI Operational Governance Document_v1.0
- 4.1.C.02 Audit Scripts & Process Documentation
- 4.1.C.05 Managing Privacy Breaches within MCCSS_v1.0
- 4.1.C.06 Change Request Form
- 4.1.C.07 Log of Confidential Reports by Members_v1.0
- 4.1.C.10 Log of Internal Reviews of Practices and Procedures_v2.0
- 4.1.C.11 Log of Privacy and Security Breaches_v1.0
- 4.1.C.12 Audit-Test-Review_Log_v2.0
- 4.1.C.14 Triennial P&P Review Template
- 4.1.C.15 Changes to DIPE Log v1.0
- 4.2.C.01 COOP Documents Combined 2022_v2.0
- 4.4.C.04 Privacy-Breach-Report-Form_v2.0
- 4.4.C.08 Privacy Protection in MCCSS - InsideOPS_v1.0
- 4.5.C.01 ERM Directive
- 4.5.C.02 OPS Enterprise Risk Management Framework
- 5.1.C.01 Annual Report_Template_v2.0
- 5.1.C.03 Dataset-Risk-Assessment-Considerations_v1.0
- 5.1.C.04 Open Data Risk Assessment Checklist_v1.0
- 5.1.C.05 Dataset Description Submission Form_v1.0
- 5.1.C.08 NOC_Change Request Template_v1.0
- 5.2.C.01 Public Inquiries or Complaints Log v1.0
- 5.2.C.02 OPS Common Service Standards
- 5.3.C.02 Notices of Collection Log_v2.0
- 5.3.C.03 Notice of Collection Template_v1.0
- 5.3.C.04 Web Content Accessibility Guidelines (WCAG) 2.0
- 5.3.C.05 Ontario.ca Style Guide URL
- OPS Data Integration Practices and Procedures Manual

Review of the Practices and Procedures of the Ministry of Children, Community and Social Services Inter-ministerial Data Integration Unit

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada M4W 1A8
Phone: (416) 326-3333 /
1-800-387-0073

www.ipc.on.ca
info@ipc.on.ca

April 2024