REPORT OF THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

MARCH 29, 2022

Review of the Practices and Procedures of the Ministry of Health's 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

Note to the reader

To address security concerns identified by the Ministry of Health, the names of specific electronic systems were substituted with generic names in this version of the report, published May 9, 2022.

CONTENTS

Executive Summary

This report concludes the Information and Privacy Commissioner of Ontario's (IPC or the Commissioner) first review of an inter-ministerial data integration unit under Part III.1 of the *Freedom of Information and Protection of Privacy Act* (Part III.1). The unit reviewed is located in the Capacity Planning and Analytics Division of the Ministry of Health (MOH IMDIU).

A major objective of Part III.1 is to enable the Ontario government to join data sets that had previously been kept in silos, 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. 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 the two classes of data integration units with the broadest authority to collect personal information *before* they can begin collecting it. Now that the review is complete, the MOH IMDIU may begin its work with personal information. However, it must comply with the orders in this report and report back to the IPC within the time periods specified.

During its review, the IPC assessed the MOH IMDIU's practices and procedures. The practices and procedures establish a framework that governs the lifecycle of information collected by the MOH 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 MOH IMDIU was very responsive and amended – or has undertaken to amend – its practices and procedures in accordance with the IPC's comments. However, some of the more significant issues identified require orders to better protect the privacy of individuals and ensure compliance. The IPC orders that the MOH IMDIU:

1. require that a wider range of logs, lists, inventories or documentation are periodically reviewed
2. conduct simulation exercises for breach response and business continuity and disaster recovery;
3. conduct an up-to-date PIA(s) of systems administered by its IT service providers;
4. conduct an up-to-date TRA(s) of systems administered by its IT service providers;
5. log required information throughout the DI Environment and make that information available for monitoring;
6. implement a business continuity and disaster recovery plan addressing certain technical items;
7. update its breach management practices and procedure; and
8. ensure the separation of roles for the coding and linking of personal information

Several recommendations were also offered for how the MOH IMDIU should improve its practices and procedures, some of which include reporting back to the IPC. The recommendations to report back to the IPC are that the MOH IMDIU:

1. describe how its practices and procedures have been changed to address the re-use of personal information and coded information;
2. refine its practices and procedures with respect to service providers who are not members of the DI Unit;
3. document its practices and procedures applicable to the physical security of its premises;
4. refine and clarify the relationship between Ontario government-wide technology standards, and practices and procedures specific to the MOH IMDIU; and
5. refine and clarify its practices and procedures regarding secure disposal and secure destruction, including certificates of secure disposal or destruction.

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

1. Introduction

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

Part III.1 created a new authority allowing designated data integration units to collect and link personal information to create de-identified datasets 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. Where provincial law previously generally required that personal information be siloed and used for the purpose for which is was collected,[1] Part III.1 created a path for breaking down barriers to information sharing for analytics purposes in the public sector. Further, Part III.1 authorizes data integration units in the Ministry of Health and the Ministry of Long-Term Care to collect personal health information directly from health information custodians under the *Personal Health Information Protection Act, 2004 (PHIPA)*.[2]

The new authority created by Part III.1 came with an expanded regulatory regime and role for the IPC. Among other things, Part III.1 allows the IPC to conduct reviews of data integration units' practices and procedures, and *requires* that the IPC conduct reviews of those data integration units with the broadest authority to collect personal information *before* they can begin collecting personal information.

This report concludes the first review of a data integration unit by the Commissioner under Part III.1. In this report, the IPC summarizes its review process, findings, recommendations, and orders relating to the inter-ministerial data integration unit located in the Capacity Planning and Analytics Division of the Ministry of Health (MOH IMDIU).[3]

2. Data Integration Units

Part III.1 defines three types of data integration units and assigns each a different level of authority to collect, use, and disclose personal information. The three types of data integration units along with a general description of their authority to collect personal information, are as follows:

- **Ministry data integration units (MDIUs)** are located within a ministry and are authorized 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;

1 It should be noted that there were already some discrete exceptions to these general rules.

2 See s 49.5(1)3 of *FIPPA*, but also see s. 49.5(1.1) of *FIPPA*. In this report, references to personal information include personal health information, unless the context indicates otherwise.

3 It should be noted that this review initially began as a combined review of the practices and procedures jointly applicable to all three IMDIUs (i.e. The Business Intelligence and Practice Division of the Ministry of Children, Community and Social Services, The Ontario Statistics Office of the Ministry of Finance and MOH IMDIU). However, as the review progressed, the IPC's review focused on the Ministry of Health IMDIU, with the reviews of the other two IMDIUs left to be completed at a later date. As discussed in more detail below, the IPC reviewed layers of practices and procedures, some of which are applicable to all three IMDIUs and some of which are only applicable to the MOH IMDIU.

- **Inter-ministerial data integration units (IMDIUs**) are located within a ministry and are authorized to indirectly collect personal information from Ontario or municipal institutions[4], MDIUs, other IMDIUs, and extra-ministerial data integration units; and
- **Extra-ministerial data integration units (EMDIUs)** are outside of a ministry and are authorized 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 *PHIPA*.[5]

IMDIUs and EMDIUs have been given broader authority than MDIUs and for that reason their practices and procedures must be reviewed by the Commissioner before they can begin to collect personal information under Part III.1 and at least every three years thereafter.[6]

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. – The Capacity Planning and Analytics Division of the Ministry of Health – The Capacity Planning and Analytics Division of the Ministry of Long-Term Care – 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[7] – The Capacity Planning and Analytics Division of the Ministry of Health	– No units have been designated at this time

In order 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[8]. They are referred to as a "member" of the data integration unit.

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

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

6 S. 49.5(1)1.ii.of *FIPPA*

7 Part III.1 specifies that only one IMDIU may be designated whose members are also authorized to collect personal information solely to compile statistical information. The Ontario Statistics Office of the Ministry of Finance, is designated as this unit. See ss. 49.5(1)2 and 49.15(2) of *FIPPA* and s. 1(2) of Regulation 366/19.

8 See the definition of "member" in 49.1(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 Government and Consumer Services (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.[9]

These data standards must be approved by the IPC before any data integration unit can begin collecting personal information under Part III.1.[10] Data integration units must comply with the data standards.[11]

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 involves three stages of information:

- **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).

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

1. **General Requirements:** This standard outlines general requirements for data integration units to ensure that all the Data Standards are effectively implemented and appropriately documented. It also deals with accountability measures and training requirements.
2. **Collection, Use and Disclosure:** This standard outlines the minimum requirements that the data integration units must meet when collecting, using, and disclosing information. Data integration units must take reasonable steps to protect privacy, comply with their legal obligations, and ensure that the persons, entities and organizations they interact with do the same.

9 S. 49.14(1)(a) of *FIPPA*.
10 S. 49.5(1)1.ii. of *FIPPA*.
11 S. 49.14(4) of *FIPPA*.

3. **Secure Retention and Transfer:** This standard outlines requirements for data integration units to put in place safeguards applicable to their technology environment. Specifically, data integration units must adopt administrative, technical and physical safeguards to protect the system components and information assets of its technology environment from breaches.

4. **Secure Disposal and Secure Destruction:** This standard 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, 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 standard outlines requirements for data integration units to retain personal information and coded information until it may or must be deleted.

6. **De-identification and Linking:** This standard 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 Part III.1 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 standard outlines the minimum requirements for data integration units to ensure openness and transparency with respect to their information practices. Under Part III.1 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 must develop, document, and implement practices and procedures that address the requirements set out in Part III.1, its regulations, and the Data Standards.[12] Data integration units must also comply with their practices and procedures.[13]

4. Commissioner's Review of Practices and Procedures

The IPC must conduct a review of the MOH IMDIU's practices and procedures after it is designated and at least once every three years thereafter.[14] As noted above, the MOH IMDIU may not begin collecting personal information under Part III.1 until this first review has been completed.

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]

12 See requirement 1 of the Data Standards.

13 See requirement 1.2.1 of the Data Standards.

14 S. 49.12 (2) of *FIPPA*. This requirement applies to all IMDIUs and EMDIUs. Further, under Part III.1 the Commissioner may further conduct reviews of the practices and procedures of any data integration unit where the Commissioner has reason to believe that the requirements of Part III.1 are not being complied with – see s. 49.12(1) of *FIPPA*.

15 S. 49.12(3) of *FIPPA*

Because this is the first review of the MOH IMDIU, it has not yet begun to collect personal information. The IPC's review has therefore focused on whether the practices and procedures to be implemented by the MOH IMDIU when it becomes operational comply with the requirements of Part III.1.

The IPC has a variety of powers in conducting its review under Part III.1 to require the production of information and records relevant to the subject matter of the review.[16] The data integration unit being reviewed, among others, is required to assist the IPC in the course of its review.[17]

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:

1. Discontinue the practice or procedure;
2. Change the practice or procedure as specified by the IPC;
3. Destroy personal information collected or retained under the practice or procedure; or
4. Implement a new practice or procedure as specified by the IPC.[18]

In the context of this review of the MOH IMDIU, the IPC exchanged multiple iterations of detailed written comments on the practices and procedures reviewed. IPC staff further had numerous video conferences to discuss the review process and to gather additional information. The practices and procedures reviewed, and the rounds of comments, MOH responses, and discussions, are summarized in the below section. The IPC's findings with respect to the practices and procedures reviewed, as well as the IPC's reasons for the orders issued and recommendations to report back, are set out below.

During the review, the MOH IMDIU provided the IPC with a variety of commitments to improve its practices and procedures. As an overarching statement, the IPC recommends and expects that the MOH IMDIU will comply with its commitments. The IPC has not specifically listed each of these commitments as separate recommendations, below. However, where an issue is discussed below that warrants further consultation and a report back to the IPC on the MOH IMDIU's progress, that recommendation is specifically itemized below.

The IPC's orders and recommendations to report back are also summarized in **Appendix A**.

16 S. 49.12(5) of *FIPPA*

17 Ss. 49.12(4) and (6) of *FIPPA*

18 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 MOH IMDIU Practices and Procedures

In the lead-up to the first review of their practices and procedures by the IPC, the three IMDIUs designated under Part III.1[19] worked together to develop an overarching policy and compliance architecture. To that end, the three IMDIUs developed a joint OPS Data Integration Practices and Procedures Manual as well as templates and logs to comply with the Data Standards, and submitted these practices and procedures for IPC review.

In fact, this review began as a review of the practices and procedures of all three IMDIUs. However, after the IPC reviewed the joint practices and procedures, the IPC determined that it would need to review significantly more detailed and granular documentation to determine whether the requirements of Part III.1 and the Data Standards were being complied with. In turn, this meant that the practices and procedures requested by the IPC began to relate increasingly to the activities of individual IMDIUs, and were no longer at the level of joint practices and procedures.[20]

The MOH IMDIU requested that the IPC review its practices and procedures first, and indicated that the other two IMDIUs agreed that the review of their practices and procedures could be resumed later. Therefore, this review proceeded with respect to the MOH IMDIU only.

While this report only concludes the review of one IMDIU (the MOH IMDIU), the IPC encourages data integration units to jointly apply standard practices and procedures wherever possible. While such standardization is not strictly required by Part III.1 and the Data Standards, it improves efficiency of the review process for all.

It may be particularly beneficial to establish common practices and procedures addressing IMDIUs' relationships with the information technology service providers within the government of Ontario. A common way of working with these IT providers, including a method of ensuring that the IT providers comply with the Data Standards where necessary, would help expedite future IPC reviews and help the IMDIUs to have confidence that their IT solutions meet the requirements of the Data Standards.

5.1. Documents Reviewed

Between September 2021 and March 2022, the MOH IMDIU provided the IPC with documentation reflecting its practices and procedures. The MOH IMDIU also provided responses to the IPC's requests for clarification, additional information, and confirmation of certain facts. In some cases, these responses included revisions to documents the MOH IMDIU had previously provided to the IPC. See **Appendix B** for the complete list of practices and procedures reviewed and representations made by the MOH IMDIU, organized by date of IPC receipt.

19 The other two being the Business Intelligence and Practice Division of the Ministry of Children, Community and Social Services and the Ontario Statistics Office of the Ministry of Finance.

20 It has occasionally been suggested that the joint "OPS Data Integration Practices and Procedures Manual" satisfies the "practices and procedures" that may be reviewed by the IPC under s. 49.12 of *FIPPA*, and that more granular documentation is not caught by the review. The IPC does not accept this position. In the IPC's view, the reference to the review of "practices and procedures" in Part III.1 reflects the full suite of activities and documentation necessary to demonstrate compliance with Part III.1 and the Data Standards.

6. Findings of the Review

This section is divided into sub-sections corresponding to each of the seven overarching Data Standards. Each sub-section follows a similar format and contains a summary of:

- each requirement under the Data Standards;
- the relevant practices and procedures provided by the MOH IMDIU;
- the IPC's staff level comments on those practices and procedures made during the review; and
- the MOH IMDIU's responses to the IPC's staff level comments.

The sub-sections include recommendations to report back to the IPC and orders under s. 49.12(7) of *FIPPA* that the Commissioner has decided to make, along with the Commissioner's reasons.

On the whole, the MOH IMDIU was very responsive to the IPC's staff level comments. It should be noted that this summary focusses on the most significant and potentially still outstanding issues identified by the IPC. Drafting comments, comments that were fully resolved, and comments and recommendations that do not relate to significant privacy or security risks are generally not summarized below.

6.1. General Requirements

This Standard sets out the overarching responsibilities of the MOH IMDIU to ensure compliance with Part III.1, the Data Standards, the 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: 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 MOH IMDIU to internally monitor its own compliance by reviewing logs, lists, inventories, or documentation that they are required to maintain. The MOH 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 MOH IMDIU's compliance obligations, and are cohesive.

The MOH IMDIU provided the IPC with written practices and procedures meant to address compliance with the Data Standards. These include the high level OPS Data Integration Practices and Procedures Manual ("DI Manual"), several standard operating procedures, various templates, standard forms, and supporting documents. The DI Manual sets out general roles and responsibilities and reporting lines for members of the MOH 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 member role is responsible for throughout the lifecycle of a data integration project, as well as supporting technology and administrative tasks.

Overall, the IPC found that the entire suite of MOH IMDIU practices and procedures reviewed by the IPC should be revised to make it more consistent, clearer, and simpler. The IPC observed that the same practices and procedures were referred to by different names, cross-references were out-of-date, and, in some cases, practices and procedures put forward inconsistent or incomplete requirements on the same issue. The IPC identified several of these inconsistencies in its comments to the MOH IMDIU and they need not be summarized here. The crucial point is that members of the MOH IMDIU must be able to practically implement the final written practices and procedures without needing to have in mind all the background and thinking that went into drafting them. The MOH IMDIU said it would make necessary clarifications, simplifications, and correct inconsistencies by March 31, 2022.

The IPC also found that the processes to address non-compliance and outstanding recommendations were often not sufficiently fleshed-out.[21] More information on such processes should be added to address how recommendations and non-compliance will be documented and communicated within the MOH IMDIU to ensure timely action. The IPC further found that, in many instances, time frames for addressing recommendations arising from reviews are not clearly defined.[22] The MOH IMDIU indicated the requested changes would be made and were aimed for completion by March 31, 2022. The IPC is satisfied that the risks associated with the above findings can be addressed through the MOH IMDIU's commitment, and that an order is not necessary.

More significantly, however, the IPC found that several of the reviews that must be periodically conducted by the MOH IMDIU of required logs, lists or documentation were not clearly required to occur.[23] The IPC advised that the practices and procedures should clearly require periodic reviews of the logs, lists, or documentation set out in requirements 5.3, 8.3, 12.2, 22.3, 25.3, and 27.3 of the Data Standards. The MOH IMDIU indicated this requested change would be made, with completion targeted for March 31, 2022.

While the IPC appreciates that the MOH IMDIU indicated it will make this requested change, the IPC also recognizes the significant role that internal reviews of logs, lists, inventories or documentation play under the Data Standards.[24] This is an important mechanism for the MOH IMDIU to detect and remediate non-compliance once it begins to collect personal information. It relates to significant matters such as: which members have physical access to the MOH IMDIU; the de-identification of coded information; and the datasets retained by the MOH IMDIU. In these circumstances, it is appropriate for the Commissioner to make an order under paragraph 2 of s. 49.12(7) of *FIPPA* that the MOH IMDIU change its documented practices and procedures to ensure they explicitly require internal reviews in compliance with the Data Standards.

21 See requirements 1.1-1 and 1.1-2 of the Data Standards.

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

23 See requirement 1.3 of the Data Standards.

24 See requirement 1.3 of the Data Standards.

Order #1

On or before April 29, 2022[25], the MOH IMDIU must:

a) change its documented practices and procedures to clearly require that logs, lists, inventories or documentation under requirements 5.3, 8.3, 12.2, 22.3, 25.3, and 27.3 be periodically reviewed in accordance with requirement 1.3;

b) ensure that the changed practices and procedures in a) address the process for conducting these reviews and identify the member responsible for compliance in accordance with requirements 1.1-1 and 1.1-2; and

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

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 MOH IMDIU members must receive in order to access the DI Environment[26] 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 relate to the specific roles that members perform in the MOH IMDIU. Training materials must be kept up-to-date. Also, simulation exercises must be performed annually to test breach response procedures and the business continuity and disaster recovery plan with findings documented and any recommendations arising from the exercise addressed in a timely manner.

The MOH IMDIU provided the IPC with practices and procedures addressing this requirement. The DI Manual sets out the overarching obligation to perform training. The MOH User Management standard operating procedures assigns a responsible member for ensuring that training occurs and states members can only access the DI Environment after training is completed. The MOH IMDIU also provided the IPC with copies of training presentations which largely addressed the required content. The IPC suggested some specific improvements to the presentations, and the MOH IMDIU has generally addressed the IPC's comments and no order is necessary.

More significantly, the IPC found that the provided DI Compliance Management standard operating procedures contained an empty placeholder section intended to address the requirement for annual breach and business disruption simulations.[27] This section appears to have been left incomplete in error. The MOH

25 While the MOH IMDIU indicated these changes, and other changes discussed below, were aimed for completion by March 31, 2022, this timeline for compliance is faster than the IPC would generally order with a requirement to provide written confirmation of compliance (especially given the date of this report). For that reason, the MOH IMDIU will be given longer deadlines (in this case until April 29, 2022) to make the ordered changes to its documented practices and procedures, on or before which it must further send written confirmation to the IPC of compliance with this order.

26 The "DI Environment" is defined in the Data Standards (p. 54) as:
"All associated system components and information assets of a [MOH 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."

27 See requirements 2.4.1 and 2.4.2 of the Data Standards.

IMDIU committed to completing the section as requested by March 31, 2022. While the IPC appreciates that the MOH IMDIU has indicated that it will be making the requested changes, the IPC also found that content detailing how this requirement would be implemented was absent from the practices and procedures it reviewed. Conducting these simulation exercises is important for ensuring that the members who are responsible for addressing actual or suspected privacy and security breaches and for implementing the business continuity and disaster recovery plan understand what they are required to do and have identified any gaps to be remediated. In these circumstances, it is appropriate for the Commissioner to make an order under paragraph 4 of s. 49.12(7) *FIPPA* requiring that the MOH IMDIU implement a documented practice and procedure to ensure compliance with the Data Standards.

Order #2

On or before April 29, 2022, the MOH IMDIU must:

a) implement a documented practice and procedure to ensure that members responsible for addressing actual or suspected privacy and security breaches, or for implementing the business continuity and disaster recovery plan, periodically conduct simulation exercises;

b) ensure that the implemented practice and procedure in a) addresses the process for conducting these simulation exercises and identifies the member responsible for compliance in accordance with requirements 1.1-1 and 1.1-2; and

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

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 MOH 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. The purpose of this process is to outline the way in which members can express concerns about actual or suspected wrongdoing within the MOH 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 MOH IMDIU must respond to them in accordance with its breach response procedures as outlined in requirement 14 of the Data Standards.

The MOH DI Compliance Management standard operating procedures provided to the IPC partially address this requirement. These standard operating procedures describe a procedure to enable staff to confidentially report deficiencies. The standard operating procedures further require that reports relating to a privacy or security breach be handled in accordance with the IMDIU breach management processes and procedures.

The IPC found that the practices and procedures reviewed did specifically provide a process to report actual or suspected incidents of non-compliance.[28] However, the practices and procedures state that such reports should be made to the DI Manager who would also lead work to address the reports. The IPC finds that the DI Manager should not play this oversight role because they may not be impartial in that they are likely to be involved in the matter or have direct authority over the concerned individuals and activities. Therefore, the standard operating procedures do not satisfy the requirements for an impartial process to deal with confidential reports.[29] While reports may be made to the DI Manager's director, this reporting line creates similar issues. The IPC further requested that the MOH IMDIU provide a description of how the current process with respect to handling the whistleblowing provisions set out in the *Public Service of Ontario Act (PSOA)* would or would not apply to the MOH IMDIU's activities under Part III.1 of *FIPPA*, and work with the IPC to develop practices and procedures that fully comply with this requirement. The MOH IMDIU committed to providing the requested material to the IPC by March 31, 2022 and continuing to work with the IPC to resolve this matter.

The IPC recognizes that there are already existing whistleblower provisions in *PSOA* that address the disclosure and investigation of alleged wrongdoing in the Ontario public services. The IPC determined that existing practices and procedures under *PSOA* will likely partly address requirement 3 of the Data Standards, and that the MOH IMDIU has further developed practices and procedures under Part III.1 that partially comply with the Data Standards. The IPC recognizes that the MOH IMDIU committed to providing the amended documents to the IPC by March 31, 2022 and continuing to work with the IPC to resolve this matter. The Commissioner does not consider it necessary to issue an order in these circumstances.

28 See requirement 3.1-2 of the Data Standards

29 See requirements 3 and 3.2.1-2 of the Data Standards

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

Requirement 4 of the Data Standards stipulates that privacy impact assessments (PIAs) must be conducted to identify, analyze and mitigate privacy risks. The MOH 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 MOH IMDIU's activities under Part III.1 that could affect the privacy of individuals or the confidentiality of information.[30]

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

The MOH IMDIU provided the IPC with documentation addressing this requirement, including: an overarching requirement in the DI Manual to conduct PIAs; several provisions in standard operating procedure; a template PIA to be used for specific data integration initiatives; and a September 2021 PIA focused on the MOH IMDIU's DI Environment (the Environment PIA).[31]

The IPC found that the Environment PIA's scope did not include the Data Transfer Tool (DTT) used to collect and disclose information from/to external entities, The Environment PIA further referenced a separate PIA conducted on the BIT data environment.[32] The IPC requested the MOH IMDIU provide the status of any identified risks with respect to assessments of those systems. In the case of accepted risks, the IPC requested the reasoning behind not implementing the recommendation. Finally, the IPC asked whether or not the assessments of BIT and DTT had been updated in light of the MOH IMDIU's status under Part III.1, and if not, to provide an explanation. The MOH IMDIU responded that it was not the business owner of the BIT and DTT PIAs, it assumes the related risks have been assessed and addressed, and it is committed to the continual improvement of the IMDIU Practices and Procedures that fall within the Ministry of Health's mandate to ensure the safe handling of personal information and personal health information.

The IPC finds that DTT and BIT are critical components of the information transmission and retention functions of the MOH IMDIU's DI Environment under the Data Standards and its role under Part III.1. When the MOH IMDIU becomes operational, its reliance on DTT and BIT will constitute a new (in relation to its activities under Part III.1) program, process, technology or system relating to its activities under Part III.1 that could affect the privacy of individuals or the confidentiality of information.[33] The MOH IMDIU is required to conduct a PIA in accordance with the Data Standards of this program, process, technology, or system. More broadly, the MOH IMDIU is accountable for having an up-to-date understanding of the risks of using such platforms.

30 See requirements 4.1.2 and 4.1.3 of the Data Standards.

31 The PIA provided to the IPC was assigned version number 0.4, and included a placeholder for a final version 1.0. The provided PIA included placeholders for a summary of privacy findings and actions and a risk mitigation plan.

32 More information about these systems can be found in the discussion of Requirement 9.

33 Within the meaning of requirement 4.1.2-2 of the Data Standards.

The IPC acknowledges that DTT and BIT are administered outside the MOH IMDIU, but this does not affect the fact that the MOH IMDIU, its members (and more broadly the minister of the ministry in which the MOH IMDIU is located)[34] are responsible for compliance with Part III.1 and the Data Standards —they cannot assume that risks have been addressed. The requirement to conduct PIAs and address risks arising therefrom is one of the most important safeguards of this data integration model. In these circumstances, it is appropriate for the Commissioner to make an order under paragraph 4 of s. 49.12(7) *FIPPA* requiring that the MOH IMDIU implement a documented practice and procedure in respect of PIAs to ensure compliance with the Data Standards.

Order #3

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

a) implement the documented practice and procedure of conducting an up-to-date PIA(s), or ensure that an up-to-date PIA(s) has been conducted, of BIT and DTT in compliance with requirement 4;

b) prioritize and address any recommendations resulting from the PIA(s) in a) 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.

6.2. 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 MOH 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.[35]

Requirement 5: Collect, use and disclose personal information, coded information and/or de-identified information only in accordance with applicable requirements in Part III.1, 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 MOH 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).

34 See s. 49.11 of *FIPPA*.

35 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 MOH IMDIU, and a requirement to review this inventory on an annual basis.[36]

The MOH IMDIU provided the IPC with the MOH DI Request Management standard operating procedures, which set out detailed procedures throughout the lifecycle of a data integration request (i.e. a project).[37] This includes specific procedures under the headings *Request Intake and Data Acquisition*, in which the standard operating procedures identify and define the requirements and/or conditions that must be satisfied to permit the collection of personal information and coded information. Specifically, the procedures require that the Intaker role[38] performs an assessment of the request against applicable eligibility requirements. The standard operating procedures also include procedures for maintaining a 'data holdings inventory' intended to track the personal information and coded information collected by the MOH IMDIU. The provided MOH DI Compliance Management standard operating procedures further describes the procedure by which the required annual reviews of the inventory are to be conducted.

The IPC found that the data holdings inventory did not fully address the minimum content of the inventory per requirement 5.4.2 of the Data Standards. Specifically, the IPC noted that the data holdings inventory must include fields for documenting the purpose of the collection as well as the need for that collection in relation to the identified purpose. The IPC further noted that the standard operating procedures do not explicitly identify the member responsible for maintaining the inventory. The IPC requested that changes be made to address these issues. The MOH IMDIU committed to making the requested changes by March 31, 2022. In light of the MOH IMDIU's commitment, no order is required.

Use

Similar to collection, 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 MOH 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 conditions, requirements, and conditions have been satisfied.[39]

The MOH DI Request Management standard operating procedures reviewed by the IPC focus on uses of personal information and coded information identified at the time of its collection. The standard operating procedures generally set out a linear, project-specific lifecycle for personal information and coded information. Information associated with a particular project is kept logically segregated in project-specific repositories.

Setting out a linear project-specific information lifecycle appears to correspond to the MOH IMDIU's anticipated usual workflow. This workflow involves a request being made for a data integration project, and the identification of the anticipated uses and disclosures of the information at or around the time of collection. However, the IPC notes that other uses and disclosures (as discussed below) can be reasonably anticipated to occur and that are unknown at the time a data integration project is requested and approved. Where practices and procedures exclusively cover usual workflow, and not reasonably anticipated

36 See requirement 5.1 to 5.4 of the Data Standards.

37 The DI Manual contains a very high level description of the collection, use and disclosure practices and procedures and need not be summarized here.

38 The Intaker role is the first and key point of contact for data integration requests for both internal and external MOH IMDIU stakeholders. The Intaker role performs the initial review of the data integration request.

39 See requirements 5.5 to 5.7 of the Data Standards.

contingencies, they create opportunity for activities that may not be in compliance with Part III.1 and the Data Standards. In that regard, the IPC commented that the provided standard operating procedures do not address the re-use of previously collected personal information or coded information.

The IPC requested that the MOH IMDIU clarify whether it intends to use personal information or coded information for such purposes (and to make necessary changes to the practices and procedures).[40] Additionally, the standard operating procedures did not address the use (as opposed to disclosure) of personal information or coded information to facilitate the right of access and correction under s. 47 of *FIPPA* as required by the Data Standards. The MOH IMDIU responded that it will update its standard operating procedures to address both the re-use of personal information and coded information and the use of personal information and coded information to respond to access and correction requests by March 31, 2022. The IPC determined that an order would not be necessary in light of the MOH IMDIU's commitment to updating its standard operating procedures, and the fact that the use cases to which the IPC's comments are directed appear to be uncommon at this point. However, the IPC recommends continued engagement on this subject, and in particular that the MOH IMDIU report back to the IPC within a year of this report.

Recommendation to Report Back #1

On or before one year after the date of this report, the MOH 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 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 conditions, requirements and conditions have been satisfied.[41] 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 MOH IMDIU.

Similar to the above discussion on use, the provided MOH DI Request Management standard operating procedures focuses on disclosing personal information, coded information, and/or de-identified information primarily in the context of the specific project for which it was originally collected. In this model, the party to which information is disclosed is the same party that initiated the data integration project (the Requestor). The MOH DI Compliance Management standard operating procedures further included provisions for responding to access and correction requests. The MOH IMDIU also provided the IPC with a De-identification and Linkage Specification, which includes a 'data release checklist' to ensure that the methodology for de-identification has been followed for the de-identified information intended for disclosure. The MOH DI Request Management standard operating procedures further assigns responsibility for approving the release of information to the role of Team Lead.

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

41 See requirements 5.8 and 5.9 of the Data Standards.

The IPC provided several comments with respect to these disclosure specific requirements. We noted that the MOH DI Request Management standard operating procedures imply that personal information, coded information, and/or de-identified information are disclosed in most cases only to the original Requestor, but there was no explicit concise statement itemizing the various parties to whom the information may be disclosed and the circumstances in which and purposes for which those disclosures may occur.[42] As with the discussion on use, the standard operating procedures do not clearly address potential disclosures outside of the context of fulfilling a specific request identified at the time of collection. The IPC requested that the MOH IMDIU update its standard operating procedures with a concise statement itemizing the various parties to whom personal information, coded and/or de-identified information may be disclosed and the circumstances in which and purposes for which those disclosures may occur. The MOH IMDIU committed to making the requested changes by March 31, 2022.

In light of the MOH IMDIU's commitments to address the IPC's comments on the disclosure requirements of the Data Standards, no order is necessary.

Requirement 6: Execute a data sharing agreement 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 MOH 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.[43]

Data Sharing Agreements

Under the Data Standards, 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 MOH IMDIU collecting personal information or coded information from a source outside the Ministry of Health, and before disclosing personal information or coded information to another data integration unit outside the Ministry of Health. In certain circumstances, a DSA may further be required where the MOH IMDIU is collecting or disclosing de-identified information. Each DSA must include certain minimum content. The MOH IMDIU is also required to develop and maintain a log of DSAs executed by the MOH IMDIU. The log must contain certain minimum content.

The intake process in the MOH DI Request Management standard operating procedures includes provisions that assign responsibility to the Intaker-DIU role to determine if a DSA should be executed. The standard operating procedures require that DSAs be executed in the circumstances listed in Requirement 6.1.2-1 and 6.1.2-2 of the Data Standards, and executed DSAs must be documented in a log. The MOH IMDIU provided the IPC with a data sharing agreement template intended to address the minimum required content of DSAs under section 6.2.2 of the Data Standards, and the IPC provided comments on this template. The MOH DI Request Management standard operating procedures further requires that DSAs follow the provided template.

The IPC found that the standard operating procedures only referred to the requirement to execute a DSA at the Intake (i.e. collection) stage. The practices and procedures do not address disclosures to other parties besides the requester, and the need to execute DSAs in those circumstances under requirement 6.1 of the Data Standards and to maintain logs of DSAs under requirement 6.3 of the Data Standards. This omission

42 See requirements 5.8-1, 5.8-2, 5.8.-3, and 5.9 of the Data Standards.

43 See requirements 6 to 6.9 of the Data Standards.

is another example of gaps created by the linear, project-specific information lifecycle which is assumed in the MOH IMDIU's practices and procedures. The IPC requested that the MOH DI Request Management standard operating procedures be amended to reflect when a DSA is required for disclosures, with associated processes, approvals and identification of the member responsible. The MOH IMDIU committed to addressing this request by March 31, 2022.

Written Acknowledgements

Where a DSA is not executed, the Data Standards require that the MOH IMDIU obtain a written acknowledgment (WA) 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 WA must generally be obtained where the MOH IMDIU is collecting personal information or coded information from the broader Ministry of Health, or where it is disclosing de-identified information to the broader Ministry of Health.

The MOH DI Request Management standard operating procedures' Intake process assigns responsibility to the Intaker-DIU role to determine if a WA should be established. The standard operating procedures require that the Intaker-DIU confirms the existence of a WA, or initiates a process to create one, in the event of a data integration request from an internal MOH program area, and document completed WAs in a log. The MOH IMDIU further provided two WA templates, one for WAs in the context of the MOH IMDIU as the collecting entity, and one in the context of the MOH IMDIU as the disclosing entity. The IPC provided comments on these templates. The IPC found that the standard operating procedures did not include a general requirement that WAs be conducted in circumstances where it is reasonably necessary to protect the privacy of individuals and the confidentiality of information, nor did it define the minimum specific circumstances in which a WA is reasonably necessary as itemized in the Data Standards under requirement 6.4.2. The standard operating procedures also did not clearly state that where required, WAs must be obtained from the relevant counterparty prior to the collection or disclosure of information under requirement 6.4.4. The MOH IMDIU committed to addressing the IPC's findings by March 31, 2022.

In light of the MOH IMDIU's commitment to address the IPC's findings on the DSA and WA requirements of the Data Standards by March 31, 2022, and the relatively low risk until such time as they are addressed, no order is necessary.

6.3. Secure Retention and Transfer

Requirement 7: Ensure that the DI Environment is only accessible to members who require access to it in the performance of their duties under Part III.1

Requirement 7 of the Data Standards stipulates that the MOH IMDIU must identity and define various access management controls and ensure, among other things, that the DI Environment is only accessed by members where authorized for defined purposes and circumstances and 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;[44] ensuring that access is only available in specific approved circumstances and is clearly logged; and that all MOH IMDIU members and service providers sign agreements that include specific minimum content.

The MOH IMDIU provided the IPC with several documents addressing this requirement. The DI Operational and Data Governance Document and the DI Manual[45] provides an overview of the various business roles in the MOH IMDIU and their primary responsibilities. The MOH DI User Management standard operating procedures generally outline criteria used to grant user access to the DI Environment. This includes a requirement to sign a confidentiality agreement before access to the DI environment is granted, and assigning overall responsibility to the Team Lead for approving and logging most changes to member access privileges, including revoking access when the DI member's employment or contract relationship with the DI Unit ends. The IPC was also provided with a spreadsheet documenting the permissions required by each role for various major systems within the DI Environment, a template User Confidentiality Agreement, as well as a template for logging user registration and access events.

The IPC found several instances where security measures required under the Data Standards were absent from the practices and procedures provided. With respect to Requirement 7, the IPC noted the absence of:

- requirements specifically relating to password strength, protection, use, confidentiality and change requirements;[46]
- a process for handing failed log-in/access attempts, including the number of failed attempts that will result in a denial of access;[47]
- a specific process for handling idle sessions, including the length of time idle that will require re-authentication (although there are some general references as "DI Users machines must be password protected with short time-out sessions in the event DI Users must leave their machines unattended);[48] and
- The use of multifactor authentication to minimize risks.[49]

44 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;

45 Note that the DI Manual references to secure retention and transfer requirements are fairly general, and are generally not summarized in this section of the report for the sake of brevity.

46 See requirement 7.2-4b of the Data Standards

47 See requirement 7.2-4c of the Data Standards

48 See requirement 7.2-4d of the Data Standards

49 See requirement 7.2-4e of the Data Standards

Based on the DI Manual's references to numerous Government of Ontario Information Technology Standards (GO-ITS standards),[50] the IPC understood that the MOH IMDIU was subject to those additional standards and requested that the MOH IMDIU identify these GO-ITS standards for review. The MOH IMDIU provided the IPC with a document mapping the relevant Data Standards to GO-ITS standards applicable more broadly to the OPS addressing password strength, handling failed logins, session timeouts, and multifactor authentication that address the requirements under this Standard. After review of the MOH IMDIU's mapping document and referenced GO-ITS standards, the IPC is satisfied and no order is necessary.

With respect to confidentiality agreements, the IPC found that the provided template agreement should specify the approved purposes for which access to the DI Environment is permitted. This will help ensure that DI Members acknowledge their obligation to only collect, use, and disclose personal information and/or coded information for those purposes permitted by the confidentiality agreement[51] and where other or less information will not serve the required purpose.[52] The MOH IMDIU informed the IPC they will respond to this issue in the User Confidentiality Agreement by March 31, 2022.

The IPC further found that the information it had received did not address the requirements for service providers of the MOH IMDIU (where they are not members) to enter into written agreements if they are supplying services related to the collection, linkage, use, disclosure, de-identification, retention, transfer, disposal or destruction of personal information, coded information or de-identified information.[53] The MOH IMDIU informed the IPC that many IT operations services are provided to the MOH IMDIU by the Health Services I&IT Cluster (HSC) of the Ministry of Health and more generally the OPS Information Technology Services (ITS) organization.

The IPC was provided a Service Level Agreement (SLA) between the Capacity Planning and Analytics Division of MOH (under which the MOH IMDIU operates), and HSC. This SLA predates the establishment of the Data Standards and does not address requirement 7.8 of the Data Standards. While the MOH IMDIU informed the IPC that HSC/ITS administrators would be required to sign user confidentiality agreements, the IPC further commented it was unclear if HSC/ITS administrators were considered members of the DI Unit as defined in the Data Standards. The MOH IMDIU clarified that HSC/ITS administrators performing data integration work would be considered members.

The IPC requested that the MOH IMDIU update the standard operating procedures to require that all 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, be required to execute a version of the template user confidentiality agreement with amendments requested by the IPC to address requirement 7.8.2. In response to the IPC's recommendation, the MOH IMDIU provided the IPC with an updated User Confidentiality Agreement that included provisions intended to address requirement 7.8. However, the updated text is integrated into the overall agreement in an unclear manner, and appears to combine requirements applicable to members, with requirements that are not applicable to members. Therefore, it is not clear that the amended confidentiality agreement meets the requirements in 7.8 of the Data Standards.

50 "The Government of Ontario Information and Technology Standards (GO-ITS) are the official publications concerning the standards, guidelines, technical reports and preferred practices adopted by the Government of Ontario" – see **Information technology standards | ontario.ca**

51 Or, in the case of disclosure, as required by law. See requirement 7.5-6 of the Data Standards

52 See requirement 7.5-7 of the Data Standards

53 See requirement 7.8 of the Data Standards

The IPC is satisfied that the risks associated with the above comments can be addressed through the MOH IMDIU's changes to its practices and procedures, and that an order is not necessary. However, the IPC recommends further changes to address the IPC's above comments and that the MOH IMDIU report back to the IPC to consult further.

Recommendation to Report Back #2

On or before one year after the date of this report, the MOH IMDIU should:

a) refine its practices and procedures with respect to 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; and

b) consult with the IPC on these practices and procedures.

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 MOH 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 MOH IMDIU's physical premises. The MOH 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 DI Unit 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.[54]

The MOH DI Environment Management standard operating procedures provided to the IPC include provisions with respect to visitor access to the DI Unit's physical premises. The standard operating procedures further state that physical controls with respect to OPS facilities were out of scope for the SOP. The IPC understood that physical security of the MOH IMDIU's premises were provided by other areas of the Ontario Public Service who may follow existing OPS standards The IPC requested the MOH IMDIU to confirm in writing how certain physical security requirements are being met, including:

- the locks, alarms, and monitoring of the physical premises in accordance with requirements 8.1-1 and 8.2-1;
- how visitors are identified in accordance with requirements 8.1-2; and
- whether identified physical security vulnerabilities are resolved in a timely manner based on their level of severity in accordance with requirement 8.2-2.

54 See requirements 8 to 8.3 of the Data Standards.

The MOH IMDIU responded that it had created a ticket with the administrators of the data centre used by the MOH IMDIU to obtain information on the physical security measures in data centres (e.g. the locations where electronic records of personal information and coded information are actually retained on servers). The IMDIU committed to providing their response to the IPC once it is received. The MOH IMDIU further provided the IPC with GO-ITS 25.18: Data Centre Physical Security Standards – which addresses physical security measures for such data centres in a manner compliant with the Data Standards.

The overall design of the MOH IMDIU prohibits retention of PI and or coded information outside of a virtualized environment (discussed further in the next section). The DI environment's data is retained in a data centre subject to GO-ITS 25.18. In these circumstances, an order is not necessary with respect to physical security at the data centres (as the location where PI, coded information, and/or deidentified information is retained).[55]

However, the IPC has not received information describing the physical security measures of the premises of the MOH IMDIU[56] (i.e. its office as opposed to the data centres). Given the data retention model of the MOH IMDIU involves no information being retained in the office context, the risk that this omission poses to the security of personal information and coded information is not significant. Nevertheless, given the requirements of the Data Standards in relation to physical security, the IPC recommends that this omission be promptly addressed and that the MOH IMDIU report back to the IPC in that regard.

Recommendation to Report Back #3

On or before June 30, 2022, the MOH IMDIU should:

a) work with its Ontario Public Service partners to document its practices and procedures applicable to the physical security of its premises; and

b) provide these practices and procedures to the IPC.

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 MOH IMDIU must ensure that personal information and coded information is only retained and transferred in electronic format where authorized for defined purposes and circumstances, and all conditions, requirements and restrictions have been satisfied, and ensure that identified vulnerabilities are addressed in a timely manner.

55 See requirement 8.2-1 of the Data Standards.

56 See requirement 8.2-1 of the Data Standards.

The MOH IMDIU provided a variety of technical documents that describe the conceptual architecture of the DI Environment IT solution. Several major IT systems are involved:

1. Data Transfer Tool (DTT): Used by parties outside the MOH IMDIU to securely transfer information to the DI Unit, and by the MOH IMDIU to disclose information to outside parties;
2. Business Analysis Platform (BAP) is an MOH HSC data analysis solution involving several major components:
    a. The Remote Workspace (RW): A Windows environment that DI members remotely access from their primary Ontario Public Service workstations. The RW servers are the environment in which MOH IMDIU work must be conducted. Each member password protects their working folder in the RW; and
    b. Business Intelligence Tool (BIT): An array of IT systems architected to support business intelligence applications. BIT uses the Data Warehousing Tool (DWT) as an underlying database system. BIT is hosted in a virtual network environment segregated from other applications. Within BIT, each member uses an DWT 'personal schema' that only they have permission to access. Within the personal database schema, members retain and use personal information, coded information, and de-identified information. Shared access 'transfer schemas' are in place to support different user roles exchanging work product with one another; and
3. Data Analytics Tool (DAT)[57]: MOH IMDIU members use the DAT application running on their local workstations to connect to a DAT server inside of BAP which acts as an interface to BIT and the DWT database schemas used to retain personal information, coded information and de-identified information. DAT is the front-end data analysis application in which personal information is transformed into coded information and de-identification techniques are applied to coded data sets, with the results saved back into BIT/DWT schemas or exported into the RW.

The MOH DI Environment Management standard operating procedures further describes the quarterly vulnerability scanning and annual penetration testing practices of the MOH IMDIU. Vulnerability scans and penetration tests must also be conducted after significant changes to the DI Environment.

The IPC acknowledged that password-protected folders in the RW and the DWT personal schemas serve as mechanisms to logically segregate the activities of members from one another. The virtual network environment housing BAP further segregates the DI Environment from other OPS systems. In March 2022, the MOH IMDIU clarified that the RW is a dedicated environment for the MOH IMDIU, and that controls are in place limiting access to DWT schemas to specific network addresses. This additional information satisfies the IPC with respect to Requirement 9.1-1 and no order is required.

The MOH IMDIU further provided the IPC with a Threat Risk Assessment (TRA) conducted for the DI Environment in 2021. Among other subjects, this TRA provided a brief description of the firewalls in place to secure the DI Environment as well as the anti-malware measures in place for various system components. This TRA, however, did not cover DTT. The IPC noted that it did not observe any documentation discussing anti-malware measures on the DTT system, and that the use of firewalls was not clearly documented in the MOH IMDIU standard operating procedures.[58] The IPC requested that the MOH IMDIU clarify its use of these

57 This footnote has been redacted as it provided an explanation of the original name of the DAT system.

58 See requirements 9.1-2 and 9.1-5 of the Data Standards.

security controls. In March 2022, the MOH IMDIU clarified the anti-malware measures in place on DTT and the use of firewalls to the IPC's satisfaction and no order is necessary.[59]

The IPC noted another finding from the TRA was that the MOH IMDIU did not conduct any real-time monitoring of the DI environment. The TRA recommended that the MOH IMDIU take advantage of the enhanced monitoring services offered by the Ontario Public Service (OPS) Cyber Security Operations Center (CSOC). The IPC commented that it shares the concern expressed in the TRA that the monitoring measures defined for the MOH IMDIU are reactive in nature.[60]

The IPC requested that the MOH IMDU clarify if it intends to implement any real-time monitoring capabilities. The MOH IMDIU stated that it intends to engage in "pro-active monitoring but it will not be in real time but performed on a regular basis to provide for sufficient coverage." The MOH IMDIU further raised the issue of cost and resource limitations, and that it understands "the level of risk is low." Additionally, the monitoring being conducted by the MOH IMDIU Compliance Officer is intended to primarily address threats from within the OPS network directly interacting with the applications being used by DI members on a regular basis.

In terms of the security of the perimeter of the DI Environment, the MOH IMDIU informed the IPC that proactive monitoring of the perimeter, firewall and email is carried out by the OPS ITS and Corporate Cyber Security, and that such monitoring follows **GO-ITS 25.0 General Security Requirements** and **GO-ITS 25.6 Security Requirements for Firewalls**. These standards provide significant detail about the perimeter security monitoring required to be in place for OPS networks. The MOH IMDIU further stated they would work with ITS to obtain real-time network monitoring capabilities to detect unauthorized access to the broader OPS network in which the IMDIU DI Environment resides.

Based on this information, in addition to the MOH IMDIU's statement that they "intend to start slowly" (i.e. with few DI members), the perimeter monitoring being conducted provides a reasonable degree of assurance that the highest-risk threats are being regularly monitored (e.g. external threats). Given the small number of DI members having access to personal information and coded information, the after-the-fact monitoring by the Compliance Officer in conjunction with the fact that DI members are informed that such monitoring is occurring serves as a reasonable deterrent for malicious insiders that may help to prevent breaches involving snooping or insider data theft.

For the above reasons, the IPC is generally satisfied with the monitoring being conducted on the DI Environment and no order is required. This finding is based on the proactive perimeter monitoring being conducted, the small number of MOH IMDIU members having access, and the deterrent effect of those members being informed of the regular monitoring being conducted by the compliance officer. The effectiveness of these controls may change should the MOH IMDIU grow in members or the breadth of its activities change significantly, among other considerations. We would also note that the effectiveness of monitoring in respect of detecting breaches is dependent on the scope of the activities subject to logging and the frequency and reliability by which information about these activities is made available to the Compliance Officer for review. For this reason, the IPC's order under Requirement 11 with respect to audit logging references the need to readily make all logged information available to the Compliance Officer.

59 Note that an order is issued under requirement 11 of the Data Standards requiring a TRA be conducted for DTT.

60 See requirements 9 to 9.2 of the Data Standards.

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.[61] The MOH IMDIU is required to identify and define various items, including requirements, restrictions, methods, and specifications on both remote access and mobile retention. In addition, the MOH 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 all conditions, requirements and restrictions have been satisfied. The MOH IMDIU must also ensure that other requirements are addressed such as those relating to data minimization, purpose limitation, encryption and access management.

With respect to remote access, as introduced in the preceding section, the MOH IMDIU's practices and procedures provide that its work is to be conducted in the Remote Workspace (RW) via a remote access connection. In essence, approval to access the MOH IMDIU's DI Environment in general is a form of remote access approval.

The IPC understands the rationale to require all members to perform MOH IMDIU work in the managed RW environment via a remote connection. However, the practices and procedures with respect to this model do not address the types of threats intended to be addressed by the remote access portion to this requirement. Those threats pertain to access to the personal information and/or coded information originating from a network and physical location outside of the management of the MOH IMDIU or its service providers (i.e. teleworking). The IPC commented that it did not receive any information describing practices and procedures with respect to approving telework (as a subset of remote access)[62]. In light of this, the IPC stated that the MOH IMDIU should provide it with further documentation describing its practices and procedures with respect to remote access, including a description on any reliance on OPS GO-ITS standards as applicable.

In response to the IPC's comments the MOH IMDIU provided GO-ITS Standard 25.7: Security Requirements for Remote Access Services. This Standard includes requirements for subjects including training, restrictions on granting access, authentication measures, and device authorization. The MOH IMDIU further provided the IPC with a document entitled: Remote Access Instructions to Reach DII Environment. This document describes the process for logging into the DII Remote Workspace from outside of the OPS workplace. In consideration of the provided information, the IPC is largely satisfied on the subject of remote access and no order is necessary.

With respect to mobile retention, the MOH DI User Management standard operating procedures prohibits the retention of 'DII data' on mobile devices in all circumstances. The IPC acknowledged that, by design, personal information and coded information is intended to be retained exclusively within the RW, but the omission of laptops and tablets from the definition of mobile devices introduces ambiguity. The IPC requested the MOH IMDIU expand its definition of mobile device to include laptops and tablets. The MOH IMDIU committed to doing so by March 31, 2022. In consideration of the provided information, the IPC is largely satisfied on the subject of mobile retention and no order is necessary.

61 See requirements 10 to 10.3 of the Data Standards.

62 See requirements 1.1-2 and 10.2-1 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 (TRA) as well as the capture and review of audit logs.[63] This includes identifying and defining: the circumstances in which a TRA is required (which must be done before the MOH 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 detect and monitor 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 TRA provided by the MOH IMDIU included in its scope the BIT database environment, the DAT application, and the Remote Workspace. The TRA also assessed the various business roles in the DI Environment as well as the MOH IMDIU's business processes. The MOH IMDIU defined mitigation strategies for all identified risks. Based on those mitigation strategies the TRA raised seven total risks for the MOH IMDIU at project go-live, with none rated high or critical, three medium, three low, and one very low. However, the TRA provided did not address DTT. As noted above, DTT is used by parties outside the MOH IMDIU to securely transfer information to the DI Unit, and by the MOH IMDIU to disclose information to outside parties.

The IPC requested that the MOH IMDIU provide security assessments conducted for DTT, from January 2021 until February 2022, and a copy of the most recent TRA conducted for DTT. The MOH IMDIU responded that it had requested this information from HSC, and it is committed to the continual improvement of the IMDIU practices and procedures that fall within Ministry of Health's mandate to ensure the safe handling of personal information and personal health information.

As the IPC found above in its discussion of PIAs, DTT is a critical component of the information transmission and retention functions of the MOH IMDIU's DI Environment. The MOH IMDIU is accountable for having an up-to-date understanding of the risks of using such platforms and for conducting TRAs in relation to the DI Environment before it becomes operational.[64] The IPC acknowledges the fact that STFS is administered outside the MOH IMDIU, but this does not change the fact that the MOH IMDIU, its members (and more broadly the minister of the ministry in which the MOH IMDIU is located) are responsible for compliance with Part III.1 and the Data Standards. While the MOH IMDIU's use of a broader ministry program, process, technology or system may introduce administrative challenges for the MOH IMDIU as a single part of the broader ministry, this does not affect the fundamental character of the obligations imposed on the MOH IMDIU under Part III.1 and the Data Standards. The MOH IMDIU has not provided the IPC with a TRA demonstrating compliance with this requirement with respect to DTT. The IPC notes that the requirement to conduct TRAs is another of the most important safeguards built into the data integration model. In these circumstances, it is appropriate for the Commissioner to make an order under paragraph 4 of s. 49.12(7) of *FIPPA* that the MOH IMDIU implement a documented practice and procedure in respect of threat and risk assessments to ensure compliance with the Data Standards.

63 See requirements 11 to 11.5 of the Data Standards.

64 See requirements 11 and 11.1-1 of the Data Standards.

Order #4

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

a) implement the documented practice and procedure of conducting an up-to-date TRA(s), or ensure that an up-to-date TRA(s) has been conducted, of DTT in compliance with requirement 11;

b) prioritize and address the 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.

Audit Logs

The MOH Compliance Management standard operating procedures generally require that information be logged to capture, detect, and monitor privacy and security breaches. In signing the User Confidentiality Agreement, each MOH IMDIU member agrees to enable a 'Local Log' in their DAT application to activate additional user activity logging.

The standard operating procedures further mention the use of DAT Macros, a Data Presence Report, a Data Movement Report, and Data Use Report, which are meant to provide information in support of detecting and investigating potential privacy or security breaches. The MOH IMDIU also provided the IPC with DI Audit Breach Procedures, which include numerous examples of information which can be compiled from Macros. This includes file and user history for the DTT transfer application, RW failed login attempts, personal schema failed login attempts, and file movement events between personal and transfer schemas.

The IPC found that the information presented in the DI Audit Breach Procedures were characterized as 'examples' and it was unclear if the capability to log and review this information was implemented. Additionally, the DI Environment TRA provided to the IPC issued a recommendation stating that "all activity from the various user categories must be logged and actively monitored to appropriately identify any undesired user and system activity", but the mitigation strategy associated with the recommendation stated that while critical operations are audited "not all activities" are logged. The IPC found that it was not clear if all systems in the DI Environment logged the required information.[65]

In response, the MOH IMDIU provided the IPC with a detailed mapping (DII-Standards-Logs Mapping) that cross-referenced the information required to be logged under this requirement with the major systems within the DI Environment. While the IPC appreciates the detailed submission from the MOH IMDIU on this subject, the provided mapping highlights gaps in the MOH IMDIU's logging practices and procedures. For example, according to the mapping, the Remote Workspace does not fully log the information necessary under Requirement 11. This omission would mean that the MOH IMDIU Compliance Officer has limited visibility into the activities in the RW file system. As discussed above, the RW is used as a staging area for the Coder to save new files containing personal information transferred into the IMDIU's custody via DTT. Without logging in place in the RW, a risk arises that the Coder could use or disclose personal information via the RW in an unauthorized manner with little to no direct evidence retained about those activities.

65 See requirement 11.4 of the Data Standards.

The IPC appreciates that a variety of compensating controls reduce the likelihood of such an incident occurring, such as limiting access to data sets to specifically named individuals, and logging at various other points of the information lifecycle. However, the IPC finds that the MOH IMDIU is not complying with requirement 11.5 of the Data Standards, and that this non-compliance creates risks to the privacy and confidentiality of individuals. The MOH IMDIU subsequently informed the IPC that its IT service provider is in the process of testing changes to update event logging functionality in the RW and that the updated functionality is expected to be in place by March 31, 2022. The IPC has reviewed the proposed changed to logging functionality, and notes that the intended changes will log file access, file deletion, login attempts, along with the date and time and user ID of the person performing the action. The IPC appreciates the MOH IMDIU's commitment to closing the gap in its RW logging practices and procedures, and recognizes this is an area in which the MOH IMDIU has told IPC it will be making ongoing improvements. However, given the critical of importance of effective logging for detecting and monitoring of privacy and security breaches and the significant risks in its absence, it is appropriate for the Commissioner to make an order under paragraph 2 of s. 49.12(7) of *FIPPA* that the MOH IMDIU change its documented practices and procedures in respect of audit logs to ensure compliance with the Data Standards.

Order #5

On or before June 30, 2022, the MOH IMDIU must:

a) change its documented practices and procedures to:

   i. log the information specified under requirement 11.5 for events occurring in the DI Environment;

   ii. make the information logged under a) available to the Compliance Officer for regular monitoring of privacy and security breaches; and

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

For greater clarity, order provision a)i. includes logging all reasonably foreseeable member activities that may involve transmitting personal information and/or coded information from any system in the DI Environment to the member's workstation.[66]

66 This is an instance "where PI and/or coded information is viewed, handled or otherwise dealt with" within the meaning of requirement 11.5.2-4.

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

Requirement 12 of the Data Standards requires the MOH 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 to monitor and review 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 MOH IMDIU standard operating procedures describe many situations that would trigger the change management process. These include responding to recommendations arising from log reviews, breach reports, PIAs, TRAs, vulnerability scans, and penetration tests. Change management is also initiated if required as part of business continuity management and standard maintenance activities.

The MOH DI Compliance Management standard operating procedures distinguish between:

- a process for correction and prevention change management when an MOH IMDIU Member or possibly an external entity such as a data source or other data integration Unit, or HSC/ITS etc., suggests a change to a policy, process, procedure or artifact for example. This then becomes a Reported Issue by the staff member. This could also be triggered by a complaint from the public, a partner or client.
- a "broader change management" procedure designed to ensure that the Compliance Officer is aware of the impacts of a DI Change Request on potentially a broad assortment of data integration operational processes, artifacts, technical designs and specifications.

The correction and prevention change management process includes the creating formal change requests; review of those requests by the DI Unit Manager and other stakeholders as required; and the appointment of a member to act as the change request lead who completes a 'CR and Impact Matrix' that captures the results of change testing as needed. The broader change management procedure largely involves stakeholders outside the MOH IMDIU, specifically the HSC/ ITS cluster (who administer much of the MOH IMDIU DI environment). The MOH IMDIU further provided the IPC with a 'DI Maintenance Plan' document that describes patching notifications for various systems, including the frequency at which these notices are sent.

The IPC found that it was unable to locate MOH IMDIU standard operating procedures that address vendor supplied changes (e.g. patches and updates).[67] The IPC further found that the provided DI Maintenance Plan implies that vendor updates to environments are handled by HSC/ITS, but the process by which this occurs is unclear.[68] This process is important for ensuring systems are kept up-to-date and patched against security vulnerabilities. In respect of the relationship between the MOH IMDIU and HSC/ITS, the IPC flagged a broader issue that the IPC was not provided information which describes the procedures HSC/ITS follows with respect to change management. The IPC requested that the MOH IMDIU provide the IPC with practices and procedures that fully address requirement 12 of the Data Standards.

In response, the MOH IMDIU provided the IPC with an updated DII Maintenance Plan document which addresses roles and responsibilities concerning vendor-supplied updates. Also with respect to vendor security patches, the MOH IMDIU provided the IPC with **GO-ITS 42: Security Requirements for Enterprise Vulnerability Management**. GO-ITS 42 establishes a framework for vulnerability management at the OPS,

67 See requirement 12.1 of the Data Standards.

68 See requirement 12.1 of the Data Standards.

including the DI Environment components administered by the MOH IMDIU's IT providers. The framework assigns responsibility to monitoring for security vulnerabilities and associated patches and establishes risk-based timelines for IT administrators to apply patches through change management procedures. The MOH IMDIU further provided the IPC with **GO-ITS 35: Ontario Public Service Enterprise Change Management Standard**, which establishes the change management framework for the OPS. Overall the IPC is satisfied that the information provided to it in respect of this requirement addresses requirement 12 of the Data Standards and no order is required. However, the IPC recommends that the MOH IMDIU continue to refine and clarify the relationship between GO-ITS standards, standard operating procedures, and the DI Manual in its documented practice and procedures and report back to the IPC on these changes. This is a broader recommendation that applies beyond change management more generally to the MOH IMDIU's reliance on GO-ITS standards to demonstrate compliance. This recommendation arises out of the complicated interplay between GO-ITS standards, the MOH IMDIU's standard operating procedures and DI Manual -which the IPC found was not always clear.

Recommendation to Report Back #4

On or before June 30, 2022, the MOH IMDIU should:

a) refine and clarify the relationship between GO-ITS standards, standard operating procedures and the DI Manual in its documented practices and procedures; and

b) consult with the IPC on these practices and procedures.

For greater clarity, this recommendation applies to all instances in which the MOH IMDIU relies on GO-ITS standards to demonstrate compliance with Part III.1 and the Data Standards.

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 MOH IMDIU has an effective business continuity and disaster recovery plan

Requirement 13 of the Data Standards stipulates that the MOH IMDIU must ensure that personal information and coded information is backed up in a manner that allows it to be fully recovered, and that the MOH 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.

With respect to business continuity and disaster recovery, a plan must be identified and defined in order to describe how the MOH 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 subjects.

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 MOH IMDIU provided the IPC with several documents that address this requirement. The MOH DI Compliance Management standard operating procedures includes a section entitled 'Continuity Management' that requires the Compliance Officer role, in the event of an outage or business disruption (among other things), to follow steps outlined in the DI Business Continuity Plan and complete the Continuity Recovery Resolution Template (both of which were also provided to the IPC for review). The standard operating procedures further includes procedures to ensure the continuity management plan is kept up-to-date in the event of changes to the DI Environment.

The draft Business Continuity Plan provided to the IPC by the MOH IMDIU includes: a description of types of outages and disruptions; a high level process map for following in the event of an outage or disruption; a business impact matrix template intended to document the business criticality of the systems; resources; and processes relied upon by the MOH IMDIU in order to support appropriate recovery prioritization efforts. This Plan identifies key MOH IMDIU personnel and their roles and responsibilities with respect to implementing the plan. The Plan includes several phases: awareness of the incident; deciding whether or not to activate the BCP; and resumption and recovery efforts prioritized according to the business impact matrix. The plan describes the impacts of certain components of the DI Environment being disrupted, as well as some steps DI members should take to notify others and check for data loss. The plan further describes backup procedures and frequencies for various IT systems. The plan includes a section entitled 'process for testing' – but this section is comprised of only one sentence.

Overall, regarding Requirement 13,the IPC found that the Continuity Management Plan was still in draft form and should be completed. With respect to back-up and recovery, the IPC found that the Continuity Management Plan offered limited details about the circumstances in which backed up information is made available.[69] While this practice and procedure alluded to yearly testing of backup and recovery methods, detailed procedures were not provided. The IPC requested that the MOH IMDIU provide the IPC with more detailed practices and procedures with respect to back up and recovery, including any relevant GO-ITS standards, if applicable. The MOH IMDIU responded by stating that additional detail to address the IPC's comments would be added to the business continuity plan, as well as relevant sections of the standard operating procedures, by end of March 2022.

The IPC further stated that if the MOH IMDIU is relying on its IT service provider to maintain separate business continuity and disaster recovery plans with respect to technology infrastructure such as firewalls, domain names, and other systems listed in requirement 13.2.2-7, the MOH IMDIU should clarify what systems are subject to a separate business continuity and disaster recovery plan and provide the IPC with a copy of those plans. The MOH IMDIU responded to the IPC stating that they understand that their IT Service providers have a business continuity and disaster recovery plan in place, but the MOH IMDIU is not relying on their IT providers to maintain a separate plan. As a result, the IPC finds that it has not received information that would satisfy this requirement. While the MOH IMDIU's use of broader ministry program, process, technology or system may introduce administrative challenges for the MOH IMDIU as a single part of the broader ministry, this does not affect the fundamental character of the obligations imposed on the MOH IMDIU under Part III.1 and the Data Standards. The IPC notes the critical importance of effective business continuity and disaster recovery plans for protecting the privacy of individuals. In these circumstances, it is appropriate for the Commissioner to make an order under paragraph 4 of s. 49.12(7)

69 See requirement 13.1-3 of the Data Standards.

of *FIPPA* that the MOH IMDIU implement a documented practice and procedure in respect of a business continuity and disaster recovery plan to ensure compliance with the Data Standards.

Order #6

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

a) implement the documented practice and procedure, or ensure the implementation of the documented practice and procedure, of a business continuity and disaster recovery plan that applies to the items listed in requirement 13.2.2-7; 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: Breach Response

Requirement 14 of the Data Standards requires the MOH 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 MOH IMDIU members report actual or suspected breaches at the first reasonable opportunity, that privacy and security breach investigations ensure that all reasonable steps are taken to prevent future breaches, and to assess whether notifications to the IPC or affected individuals was effective. Privacy breaches and security breaches are defined in the glossary to the Data Standards.[70]

The MOH IMDIU provided the IPC with several documents describing practices and procedures that address this requirement. Most relevant is the MOH DI Compliance Management standard operating procedures which includes a section entitled 'Breach Management' that refers readers to a document entitled 'DI Detailed Auditing Steps' for specific details on privacy and security auditing. The DI Detailed Auditing Steps document (which was also provided to the IPC for review) sets out detailed instructions for the Compliance Officer to follow in the event of a confirmed or reported breach as directed by the DI Manager. With respect to detecting breaches, the document references staff reporting and log monitoring. Assessment questions are provided as examples to determine the facts of the breach such as the information at issue, the systems involved, and the scope of the breach. Containment procedures are described, such as "eliminating access to a data store if the source of the breach is known." The Detailed Auditing Steps document also includes fine-grained descriptions of the information that can be made available to the Compliance Officer by running a variety of different log reports in order to perform a breach investigation. The document also includes a requirement to include change requests as required to mitigate and prevent a reoccurrence of the same type of breach.

The IPC found that DI Detailed Auditing Steps do not include the full definition of privacy breaches and security breaches under the Data Standards and requested the MOH IMDIU update its practices and procedures to include that definition.[71] The MOH IMDIU indicated it would update its practices and procedures to address this request by March 9, 2022. In addition, the IPC noted that the DI Detailed Auditing Steps document provided a narrower definition of the DI Environment than the definition under the

70 Data Standards, p. 55.
71 Data Standards, p. 55

Data Standards.[72] For instance, the DI Detailed Auditing Steps does not include in its scope the workstations used by DI Members to access the RW and perform their roles. Many breaches originate from attacks targeting end users, and not including this category of system in the scope of the breach management practices and procedures limits the ability of the practices and procedures to identify privacy and security breaches at an early stage in the attack lifecycle. The IPC requested the MOH IMDIU confirm that its breach management practices and procedures apply to all systems in the DI Environment as defined in the Data Standards. The MOH IMDIU indicated it will make every effort to complete the request by March 31, 2022.

The IPC further found that the provided practices and procedures do not specifically describe how it is determined whether a privacy breach or security breach occurred – and specifically whether a particular action is or is not authorized. The IPC requested that the artifacts be updated to describe such a process. The MOH IMDIU indicated it will make every attempt to complete the request by March 31, 2022

With respect to required notifications in the event of a breach, the IPC found that the DI Detailed Auditing Steps document and other artifacts do not clearly refer to the obligation to notify the IPC and affected individuals in accordance with s. 49.11(3) of *FIPPA*. Furthermore, the practices and procedures do not mandate the minimum notification content as required by the Data Standards and s. 49.11(3) of *FIPPA*. Further, the role responsible for evaluating the effectiveness of the notice to individuals and the IPC was not identified[73]. The IPC requested that the practices and procedures be updated to address these omissions. The MOH IMDIU indicated it will make every attempt to complete the request by March 31, 2022.

The IPC further found that the DI Detailed Auditing Steps do not specifically require that that all reasonable steps are taken in a timely manner to eliminate and reduce the risk of future privacy and security breaches.[74] This includes reviewing and updating safeguards, practices and procedures, training material, and testing and evaluating such remedial actions to ensure they have been implemented correctly. The IPC requested that MOH IMDIU update its breach management procedures to address this issue in consideration of the items set out in paragraphs a-d of requirement 14.3-2. MOH IMDIU indicated it will make every attempt to complete the request by March 31, 2022.

While the IPC appreciates the MOH IMDIU's cooperation in addressing the issues identified for this requirement, due to the significance of breach management procedures as a safeguard for identifying, reporting, containing, providing notification of, investigating, and remediating actual or suspected privacy and security risks and compliance issues, it is appropriate for the Commissioner to make an order under paragraph 2 of s. 49.12(7) of *FIPPA* that the MOH IMDIU change its documented practices and procedures in respect of its privacy and security breach management practices and procedures to ensure compliance with the Data Standards.

72 Data Standards, p. 54

73 See requirements 1.1-1 and 14.3-3 of the Data Standards.

74 See requirements 14, 14.2-6 and 14.3-2 of the Data Standards.

Order #7

On or before June 30, 2022 the MOH IMDIU must:

a) change its documented privacy and security breach management practices and procedures to:

   i. include the full definition of "privacy breach" and "security breach" from the Data Standards;

   ii. ensure that it applies to the entire "DI environment" as defined in the Data Standards;

   iii. specifically describe how it is determined whether a privacy breach or security breach occurred – including whether a particular action is or is not authorized;

   iv. clearly refer to the obligation to notify the IPC and affected individuals in accordance with s. 49.11(3) of *FIPPA* and mandate that the minimum required information is included in notifications to affected individuals and the IPC;

   v. assign a responsible member role for assessing the effectiveness of notifications; and

   vi. specifically require that that all reasonable steps are taken in a timely manner to eliminate and reduce the risk of future privacy and security breaches; and

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

6.4. Secure Disposal and Secure Destruction

The Data Standards require that the MOH IMDIU ensure the secure disposal or destruction of personal information or coded information and related storage media.[75]

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.[76] 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.[77] To reach the higher standard of secure disposal or destruction, the deletion process would have to be structured to include specific safeguards, or additional actions that would have to be taken, such as to the underlying storage media (e.g. physical destruction).

75 Sections 49.11(1)(a) and (d) of *FIPPA* are also relevant to this requirement.

76 Data Standards, p. 55

77 See the definition of "Delete", Data Standards, p. 54

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 MOH 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 require that the MOH IMDIU identify and define conditions under which personal information and coded information and related media must be securely disposed of or destroyed. 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.[78]

With respect to the practices and procedures provided by the MOH IMDIU, the DI Manual contains high level references to the deletion and secure disposal or destruction of information. The MOH IMDIU's practices and procedures indicate that it intends to combine these steps together and, specifically, that it intends to rely on deletion as meeting the standard for secure disposal or destruction. The Data Management standard operating procedure provided by the MOH IMDIU describes when files containing personal information or coded information will be deleted, from which repositories and by which members/roles. However, the most significant issue identified by the IPC under this group of requirements was that these practices and procedures did not specifically address how deletion meets the standard for secure disposal or destruction. The IPC and the MOH IMDIU exchanged numerous iterative comments on this point. In particular, the IPC questioned how the MOH IMDIU determined that any residual information remaining on storage media after a deletion was not reasonably foreseen to be retrievable.

The MOH IMDIU initially indicated that it did not believe there was any storage media for the deleted electronic files containing personal information and coded information. However, through further discussion it became clear that the MOH IMDIU was actually referring to the absence of local storage media, and that the personal information and coded information at issue was retained on centrally managed Ontario government computer servers. The IPC notes that the MOH IMDIU's obligations regarding secure disposal or destruction (among others) continue to apply even where personal information and coded information it has collected are retained on centrally managed Ontario government computer systems (i.e. DTT, RW, BIT, backups). The IPC and the MOH IMDIU had several further exchanges relating to the safeguards in place, such as: the encryption of the deleted files/databases; the roles, obligations, and access rights of IT administrators to the centrally managed computer servers; agreements with IT administrators; and the storage of encryption keys. The IPC further sought clarification on the safeguards in place relating to the secure disposal or destruction of centrally managed computer servers and how the MOH IMDIU ensured that personal information and coded information was only retained on such servers.

With respect to this issue, the MOH IMDIU has provided sufficient information for the IPC to determine that the actual risk of insecure disposal and destruction of personal information or coded information is low. Information is retained in the RW and BIT in encrypted form, and without access to the corresponding encryption key, it is not reasonably foreseeable that deleted information on the storage media could be reconstituted. Further the storage and use of encryption keys by BIT and RW administrators are subject to administrative and technical safeguards stipulated in the **GO-ITS Standard 25.12: Security Requirements for the Use of Cryptography**. Finally, the BIT and RW storage media are subject to the **GO-ITS Standard 25.20: Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media**. That standard requires that storage media at the end of its lifecycle be subject to methods that the IPC considers secure destruction (such as multiple passes of data overwriting, cryptographic erasure, and

78 See requirements 15 to 15.2 in the Data Standards.

physical destruction of storage media by qualified vendors). Regardless, the IPC is of the opinion that the MOH IMDIU should better clarify its practices and procedures with respect to how it meets the requirements of the Data Standards, and the MOH IMDIU has agreed to work with the IPC towards addressing issues relating to secure disposal and secure destruction to the satisfaction of the IPC under requirements 15, 16 and 17, within six months of the completion of the IPC's review. As a result of the MOH IMDIU's expressed willingness to continue to collaborate on this issue, no order is necessary, but the IPC makes a related recommendation to report back, below.

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 state that the MOH IMDIU must 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 MOH 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.[79]

The MOH IMDIU indicated that no storage media (including paper records) are retained locally. As above, it indicated that all personal information and coded information is retained on centrally managed Ontario government computer servers. For that reason, most of requirement 16 had little direct application to the activities of the MOH IMDIU (because there were no local storage media to be retained and transferred, which is the precondition for most of the requirements in 16.1 and 16.2 of the Data Standards). With respect to the destruction of storage media in centrally managed computer services (i.e. BIT, DTT, the RW and backups), we note that the provided **GO-ITS Standard 25.20: Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media**, which the MOH IMDIU has stated applies to those environments, is applicable to this requirement. GO-ITS 25.20 requires that all functioning electronic storage media are 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.

In addition, some requirements in this Data Standard continue to apply even with the MOH IMDIU's caveat that no storage media are retained locally. Requirement 16.2-1 of the Data Standard still has direct application to the practices and procedures of the MOH IMDIU, and requires that it ensure that personal information, coded information, and related storage media are securely disposed of or destroyed only in authorized circumstances, and where all conditions, requirements or restrictions have been satisfied, including the requirements in the Data Standards, among others. The IPC noted that the Data Management standard operating procedure provided by the MOH IMDIU stated that coded information would be retained for "1 year from the date of creation of the last file in the group", after which they would be deleted. Inasmuch as the MOH IMDIU's practices and procedures equate deletion with secure disposal or destruction, the IPC was concerned that application of this retention period would result in the secure disposal or destruction of coded information when that information was still required to be retained by the Data Standards. Specifically, 18.1.3-1 of the Data Standards requires that coded information 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."[80] The MOH IMDIU committed to addressing this issue by the end of March 2022.

79 See requirements 16 to 16.2 in the Data Standards.

80 This issue was also addressed in the IPC's comments to the MOH in relation to requirement 18.1.3-1 and the MOH IMDIU made the same commitment there. No order is required.

In light of the MOH IMDIU's commitment to addressing these issues (in addition to their commitment to continue to engage with the IPC with respect to the closely related requirement 15) and the security protections that the IPC understands has already been put in place regarding deletion and secure disposal and secure destruction, no orders are necessary, but the IPC makes a related recommendation to report back, below.

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 MOH IMDIU's practices and procedures identify and define the required content of certificates of secure disposal or destruction, and specify certain minimum required content.[81] The MOH 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 MOH 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 are maintained, and that the destruction and disposal methods are periodically reviewed for effectiveness.

The application of this requirement to the circumstances of the MOH IMDIU was complicated by its decision to rely on deletion of a file as meeting the threshold for secure disposal or destruction. As different versions of a file will be retained, deleted, and backed-up at different times, it was unclear how the obligation to verify secure disposal or destruction of storage media, particularly through the preparation and receipt of one-time certificates of secure disposal or destruction, would be operationalized.

The MOH IMDIU initially indicating that obligations to obtain a certificate of secure disposal or destruction for storage media were "not applicable." As noted above, simply because storage media are not locally managed by the MOH IMDIU does not mean that the requirements in the Data Standards do not apply. However, the IPC also recognizes that the computer environment developed by the MOH IMDIU makes the preparation and completion of certificates of secure disposal or destruction in the traditional sense (e.g. the physical destruction of a hard drive containing specific records of personal information) impractical without significant changes to its computing environment.

In addition, while the MOH IMDIU has expressed that in their view, the deletion of personal information and coded information from their environment can be considered secure destruction, the provided **GO-ITS Standard 25.20: Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media** also pertains to this requirement. The servers administered by the MOH IMDIU's IT providers relied upon by the MOH IMDIU to retain personal information and coded information are subject to this standard. 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, with the exception of expressly stating the data integration unit from which the storage media came.

While the IPC understands that the MOH IMDIU is relying on deletion as the basis of issuing certificates of destruction/disposal, to demonstrate greater assurance, the MOH 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. As above, the MOH IMDIU committed to working with the IPC following the release of this report

81 See requirement 17.1.2.

to address any outstanding issues regarding secure disposal and destruction. In light of this commitment, no orders are necessary but it is appropriate for the IPC to make a recommendation for the IMDIU to report back.

Recommendation to Report Back #5

On or before six months after the date of this report, the MOH IMDIU should:

a) refine and clarify its practices and procedures regarding secure disposal and secure destruction, including certificates of secure disposal or destruction; and

b) consult with the IPC on these practices and procedures.

For greater clarity, this recommendation applies to the MOH IMDIU's practices and procedures under requirements 15, 16 and 17.

6.5. Retention Period

Requirement 18 of the Data Standards outlines requirements for practices and procedures relating to how long the MOH IMDIU can or must retain personal information and coded information.[82] 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) by the MOH IMDIU. 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.[83]

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

The Data Standards require that the MOH 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 MOH 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);[84] and

82 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.

83 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 MOH IMDIU, but are subject to variations or further specification in the Data Standards.

84 See the issue in relation to this requirement identified and discussed under requirement 16, above.

- 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. There are possible exceptions to this 180 day retention requirement in specific circumstances.

Under requirement 18.3, the MOH IMDIU must ensure that personal information and coded information is deleted at the earlier of the expiry of a maximum retention period or where the information is no longer necessary to fulfil its purpose (and provided the minimum retention period has expired). The MOH IMDIU is further required to document its deletions of personal information and coded information under requirement 18.5.[85]

The MOH IMDIU provided the IPC with several practices and procedures to review in relation to this requirement. The DI Manual set out a general process and related member responsibilities for setting and complying with retention periods. The MOH IMDIU also provided its Data Management Standard Operating Procedures which went into greater detail on how and when the retention periods will apply to personal information and coded information, and related requirements to delete the information. Further, the MOH IMDIU provided the IPC with its "DII Operational & Data Governance" policy. The MOH IMDIU's practices and procedures indicated that a spreadsheet "Data Holdings Inventory" will be used to track arrival, creation, location, and destruction[86] of data sets, and provided a copy of this spreadsheet for IPC review as it was relevant to the tracking of retention periods.

The MOH IMDIU's practices and procedures indicated that the maximum and minimum retention periods for coded information would be the same: one year. The IPC notes that the Data Standards do not require that the maximum and minimum retention periods for coded information be identical, nor does it require any *specific* maximum retention periods for coded information. The Data Standards set a minimum retention period of one year to allow individuals the opportunity to seek access and correction. With that said, the MOH IMDIU is generally free to set a more restrictive maximum retention period for coded information than is required by the Data Standards.[87]

The practices and procedures reviewed by the IPC were not clear on what retention period would apply to the minimal amount of personal information necessary for the purpose of linking under Requirement 20.3 (i.e. the ID mapping table). The IPC requested that the MOH IMDIU specifically provide a retention period for the ID Mapping table and further that this retention period must be the same as the above noted one year retention periods for coded information to facilitate individuals' requests for access and correction to their own information.[88] Otherwise, it would be difficult or impossible to identify the records applicable to the individual requesting access or correction. The MOH IMDIU confirmed that its practices and procedures would be amended by March 31, 2022 in accordance with the IPC's staff level comments.

With respect to the MOH IMDIU's obligation to ensure the deletion of personal information and coded information in specific circumstances, the IPC was unable to locate any clear practices and procedures

85 Requirement 18.4 is not discussed here because it was included in the Data Standards for clarification purposes to explain the relationship of the retention requirements in the Data Standards with the references to retention periods under sections 49.6(1)4 and 49.11(1)(c) of *FIPPA*.

86 As noted above, the MOH IMDIU is relying on deletion of information as a form of secure destruction and secure disposal.

87 Elsewhere, the IPC commented that the MOH IMDIU should set out the retention period for de-identified information. The MOH IMDIU's response indicated that de-identified information would only be retained for one year. Again, this would appear to be another place where the MOH IMDIU has set a more restrictive standard than is required by the Data Standards.

88 As above, the Data Standards do not require a specific maximum retention period for the minimal amount of personal information necessary for the purpose of linking under requirement 20.3 (i.e. the ID mapping table). Indeed, one of the major purposes of such a table is to allow consistent and accurate linking over time across multiple data integration projects. The IPC's comment is only directed at this table being retained long enough to facilitate access to coded information, and not that the Data Standards require that it can only be kept for one year.

requiring that personal information and coded information be deleted where its retention is no longer necessary to fulfill the purpose for which it was collected or created, following the expiry of the minimum retention periods (as required by 18.3-3). Further, the IPC did not locate any clear practices and procedures specifically requiring the deletion of personal information in the ID Mapping Table in accordance with Requirement 18.3 of the Data Standards. The MOH IMDIU confirmed in writing that its relevant practices and procedures would be amended to address the IPC's comment by March 31, 2022.

Given the responsiveness of the MOH IMDIU to the IPC's comments, there is no need for an order to address the issues identified under this requirement.

6.6. De-Identification and Linking

Under Requirement 19, the MOH 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.[89] 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 MOH IMDIU separate the roles for data coding (i.e. removing direct identifiers and replacing them with a secure unique code) and data linking (i.e. using the secure unique code to link records in separate datasets) within the MOH IMDIU.[90] 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.

Both the DI Manual and the De-identification and Linkage Standard Operating Procedures provided by the MOH IMDIU clearly indicate that it has created two distinct roles for the Coder and Linker in the de-identification process. These practices and procedures both state that:

> The Data Coder and Data Linker are separate roles and are to be performed by distinct DI staff members. The Data Coder and Data Linker will operate in a manner to facilitate protection of privacy, avoid concentration of [personal information] by one role […]

The De-identification and Linkage Standard Operating Procedures further describe the different safeguards that will be in place (including technical safeguards) to separate the work of the Coder and Linker. The MOH IMDIU also provided a spreadsheet mapping which roles have access to the different components and tools of the DI Environment.

However, the IPC found that the MOH DII Operational & Data Governance document did not clearly indicate how the role of the Coder and Linker are distinct or specifically indicate what information the Linker does not have access to that the Coder does (so that members are clearly and consistently informed of which MOH IMDIU datasets are off limits for which role).

89 Data Standards, p. 43

90 See requirements 19 to 19.2 of the Data Standards.

The IPC was also unable to locate a clear prohibition on Coders and Linkers using other applications to deal with personal information and coded information and requested this be added. Lastly, the practices and procedures did not address which roles do and do not have access to the ID Mapping table (i.e. the database of identifiers used for mapping between each assigned internal code and the minimum common identifiers). Given the fact that this ID mapping table could be used to easily 'decode' the linked information created by the Linker (and thereby identify numerous facts about identifiable individuals), the practices and procedures should clearly address the ID Mapping Table and ensure the Linker does not have access to it.

The MOH IMDIU confirmed that amendments to reflect all but one of the IPC's comments would be made to the DII Operational & Data Governance document and standard operating procedures by the end of March 2022. However, the distinction between the Linker and Coder is one of the core protections in the Data Standards, and goes directly to the ability of the data integration lifecycle to collect and link information from multiple sources in a privacy protective manner that does not give a single member end-to-end control over a potentially immense volume of personal information. Given the significant risks involved, it is appropriate for the Commissioner to make an order under paragraph 2 of s. 49.12(7) of *FIPPA* that the MOH IMDIU change its documented practices and procedures in respect of the linking and coding roles to ensure compliance with the Data Standards.

Order #8

On or before April 30, 2022, the MOH IMDIU must:

a) change its documented practices and procedures to specifically and clearly ensure the separation of member roles for coding and linking processes using administrative, technical and physical safeguards that are reasonable in the circumstances in accordance with requirement 19.2 and having regard to the IPC's above comments;

b) ensure that the changed practice and procedure in a) addresses the process for separating member roles and identifies the member responsible for compliance in accordance with requirements 1.1-1 and 1.1-2; and

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

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

The Data Standards require that the MOH 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 MOH IMDIU is not left in its most identifiable format for longer than is 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 MOH 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.[91]

In respect of practices and procedures reviewed, the MOH IMDIU provided the IPC with the DI Manual, which describes the de-identification and linking process at a very high level. The MOH IMDIU also provided the IPC with its: De-identification and Linking Standard Operating Procedures (contained within their Request Management standard operating procedure); De-identification and Linkage Specification (a template for documenting and prompting the coding and linking process and analysis); and data field classification framework (that serves as a reference guide for identifying various direct and indirect identifiers).

The IPC noted one issue with the coding and linking process in the De-identification and Linking Standard Operating Procedures:[92] the standard operating procedures suggests that the Linker will conduct linking utilizing either a health card number or first and last name. This should not be possible if all direct identifiers have been removed from the database (as is required by the Data Standards). The IPC notes that this was only one statement in a suite of practices and procedures that otherwise indicate that direct identifiers would be removed. The IPC further requested that if the linking process is intending to refer to the use of coded fields corresponding to health card number or first and last name, that should be clarified. In response to the IPC's comment, the MOH IMDIU confirmed that its Request Management Standard Operating Procedures would be amended by the end of March 2022 to clarify that the Linker will rely on the secure internal code unique to the individual to conduct linkages and not direct identifiers, such as health card number or first and last name.

Given the MOH IMDIU's written confirmation that it will amend its practices and procedures this month to address the IPC's comment, there is no need for an order.

91 See requirements 20 to 20.3 of the Data Standards.

92 Which itself is part of the broader Data Integration Request Management Standard Operating Procedures.

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

The Data Standards require that the MOH IMDIU identify and define 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 MOH 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 MOH IMDIU periodically review linkages made to ensure they are accurate.[93]

The DI Manual provided by the MOH IMDIU was relevant to this requirement, and described the linking process at a very high level. The MOH IMDIU also provided the IPC with its De-identification and Linking Standard Operating Procedure, its De-identification and Linkage Specification (a template for documenting and prompting the coding and linking process and analysis), and a data field classification framework for direct and indirect identifiers.

The De-identification and Linking Standard Operating Procedure, in particular, describes linking methodologies as well as a method for identifying linkage accuracy and addressing mitigation methods. However, one item that the IPC did not locate was clear practices and procedures to be followed for specific records if they are unable to be linked accurately. This is important as Linkers should have clear guidance for what to do where the linkage process and accuracy risk assessment does not resolve to an acceptable solution. The MOH IMDIU confirmed in writing that its practices and procedures will be amended by the end of March 2022 to provide a process that would be followed for specific records if they are unable to be linked accurately.

With respect to the obligation for the MOH IMDIU to ensure that coded information is only linked in authorized circumstances and where all conditions, requirements and restrictions have been satisfied (requirement 21.2-1), the IPC noted that the detailed linking procedure provided did not specifically address this requirement. For example, the practices and procedures did not reference how the Linker would ensure that their actions were in keeping with the original project approval. Again, the MOH IMDIU confirmed in writing that its Request Management Standard Operating Procedure would be amended by the end of March 2022 to address the IPC's comment.

Given the MOH IMDIU's written confirmation that it will amend its practices and procedures this month to address the IPC's comment, there is no need for an order.

93 See requirements 21 to 21.2 of the Data Standards.

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 created by 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 MOH 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 MOH IMDIU identify and define the criteria to be used in calculating the risk of re-identification. The Data Standards further require that the MOH IMDIU identify and define 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 Standard further contain ancillary requirements relating to documentation.[94]

The IPC found that the practices and procedures provided did not clearly require the successful application of the de-identification methodology prior to the disclosure of coded information, nor did the practices and procedures explicitly reference the threshold for de-identification referenced in the Data Standards (requirement 22.2). While the above two points were certainly implicitly present in the practices and procedures reviewed, the IPC was of the view they should be explicitly stated given their importance. The MOH IMDIU indicated that its practices and procedures will be amended by March 31, 2022 to refer to the re-identification threshold in s. 22.2 of the Data Standards, clearly relate the de-identification methodology selected to this threshold, and clearly prohibit members from disclosing coded information for analysis prior to:

- the application of the de-identification methodology to the coded information;
- the completion of a re-identification risk assessment finding that the risk of re-identification of the coded information is within the acceptable threshold; and
- approval of the disclosure by the MOH IMDIU Manager or higher (with associated approval processes).

In light of the MOH IMDIU's responsiveness to the IPC's comments and commitments to address them, and the fact that the comments made by the IPC generally related to providing clarifications to its practices and procedures, no order is necessary.

94 See requirements 22 to 22.3 of the Data Standards.

6.7. Public Notice and Annual Reporting

This standard outlines the minimum requirements for the MOH IMDIU to ensure openness and transparency with respect to its information practices.[95] This standard is comprised of five overarching requirements.

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 MOH 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 obligation to publish a notice of collection is also reflected in paragraph 3 of s. 49.4(1), paragraph 3 of s. 49.4(2) and s. 49.10 of *FIPPA*. 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 MOH IMDIU provided the IPC with numerous practices and procedures addressing compliance with the obligations set out in requirement 23 of the Data Standards. The DI Manual contains high level requirements reflecting the obligation to publish a notice of collection at the data acquisition stage – covering the steps to be followed by the MOH IMDIU when it is preparing to collect records of personal information. The DI Manual further contains a more detailed procedure reflecting roles and responsibilities for the publishing of notices of collection and referencing a template notice of collection that had already been prepared. The IPC further reviewed multiple drafts of this template notice of collection.

The IPC also reviewed the applicable standard operating procedures of the MOH IMDIU, which contained more granularity on the procedures and responsibility for publishing notices of collection that contain the information mandated by requirement 23 of the Data Standards.

The IPC provided the MOH IMDIU with discrete comments regarding its practices and procedures regarding the publication of notices of collection, which were generally in the nature of requesting that specific clarifications and details be added. The MOH IMDIU was quite responsive to these comments. No outstanding compliance issues were identified in the MOH IMDIU's practices and procedures regarding notices of collection and no orders are necessary.

Requirement 24: Publish a complete list of notices of collection published by the MOH IMDIU

Requirement 24 of the Data Standards requires that the MOH 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 is able to access an organized list of notices of collection, containing high level details about the projects undertaken by the MOH IMDIU with the personal information collected, and allowing the public and individuals to quickly and effectively locate relevant notices of collection and access more detailed information where desired.

The MOH IMDIU provided the IPC with practices and procedures addressing this requirement. The DI Manual contains a high level reference to the obligation to update and publish the list of notices of collection, as well as a template list of notices of collection. The IPC was also provided with the template

95 Data Standards, p. 47

list of notices of collection in the format it would appear on the internet. The MOH IMDIU further provided the IPC with its standard operating procedures providing more detail on how and when the list of notices of collection will be updated.

The IPC had a discrete comment on the MOH IMDIU's standard operating procedures. These standard operating procedures suggest that only non-active notices of collection will be included in the list of notices of collection. However, the Data Standards do not limit the requirement to publish a list of notices of collection to only non-active notices. The MOH IMDIU confirmed that it will amended its standard operating procedures to refer to all notices of collection by the end of March, 2022.

Given the MOH IMDIU's responsiveness to the IPC's comments and its commitment to address them this month, no orders are necessary.

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 MOH IMDIU publish a report on the use of personal information to link and de-identify, which includes, at a minimum:

- the list of the MOH IMDIU's personal information and coded information developed and maintained under requirement 25.3; and
- descriptions of audits undertaken under s. 49.7(1)(b) of *FIPPA*.

The requirement to report on the use of personal information also relates to s. 49.7(2) of *FIPPA*. Requirement 25.1 further states that the IMDIU "may combine this report on use with the annual report."

As noted above, the report must include a list of the MOH IMDIU's datasets maintained under requirement 25.3. That requirement stipulates that the MOH IMDIU develop and maintain a list of datasets retained by the MOH IMDIU of:

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

The Data Standards require that the MOH IMDIU's list of datasets include, at a minimum, the six elements identified in requirement 25.3.2.

The MOH IMDIU provided the IPC with practices and procedures addressing this requirement. The DI Manual references the report on use under this requirement and indicates that it may be combined with the annual report of the MOH IMDIU under requirement 26, and references an annual report template. The MOH IMDIU provided the IPC with the Annual Report Template which indicates how this template will be used to comply with the reporting on use obligations in requirement 25. The MOH IMDIU further provided the IPC with its more detailed standard operating procedures which explain responsibility for generating and publishing the annual report (including the fields set out in Requirement 25) and again references the Annual Report template.

The IPC had specific comments on the practices and procedures of the MOH IMDIU (including the Annual Report template). Of particular note, the MOH IMDIU indicated in its submissions that it was complying with the requirement to develop and maintain a list of datasets (see 25.3.1) through the use of its Data Holdings Inventory (which was also provided to the IPC for review). However, neither the standard operating procedures, nor the DI Manual, clearly indicate that the Data Holdings Inventory was intended to include the identifiers retained for use in assigning internal identifiers and linking under requirement 20.3 (see requirement 25.3.1-1). If the MOH IMDIU is relying on the Data Holdings Inventory to comply with this requirement, its practices and procedures should clearly and consistently state the action that must be taken and information to be maintained to achieve compliance. The MOH IMDIU responded to this comment by confirming in writing that both the DI Manual and the Request Management Standard Operating Procedure will be amended to include a reference to the Data Holdings Inventory including the identifiers, by March 31, 2022.

Given the MOH IMDIU's responsiveness to the IPC's comments and commitment to address them this month, no orders are necessary.

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 MOH IMDIU must ensure that an annual report is published on or before April 1 in the year following the report coverage period, and it must cover the period from January 1 to December 31. The Data Standards require that the MOH IMDIU include, in its annual report, the information identified in 26.2 to 26.6. The obligation to publish an annual report is also reflected in s. 49.13 of *FIPPA*.

The MOH IMDIU provided the IPC with practices and procedures addressing this requirement. The DI Manual references the obligation to prepare an annual report, and references an annual report template. The MOH IMDIU provided the IPC with the Annual Report Template and the IPC provided comments on this document. The MOH IMDIU further provided the IPC with its more detailed standard operating procedures which explain responsibility for generating and publishing the annual report (and again references the Annual Report template). The IPC's comments during the review were generally of the nature of requesting that clarifications and additional details be added to more specifically reflect requirement 26. The MOH IMDIU responded satisfactorily to these comments and no orders are necessary.

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

Requirement 27 states that the MOH 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 MOH 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 MOH 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 MOH IMDIU's procedure to respond to privacy complaints and inquiries include, at a minimum, the five factors identified in requirement 27.2.2. The MOH IMDIU is further required to develop and maintain a log of privacy complaints received, and this log must contain minimum content (see requirement 27.3).

The MOH IMDIU provided the IPC with practices and procedures addressing this requirement. The DI Manual contains a very high level summary of procedures to be followed for addressing privacy complaints and inquiries. The MOH IMDIU further provided the IPC with more granular standard operating procedures addressing public reports 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 member of the MOH IMDU responsible for assessing how such a complaint or inquiry should be addressed, among other things. The MOH IMDIU further provided the IPC with draft website text addressing the information that is required to be made public about its process for addressing privacy complaints and inquiries. Lastly, the MOH IMDIU provided the IPC with a template to be used for logging privacy complaints it receives. This log is referenced in the MOH IMDIU's practices and procedures.

The IPC had individual and specific comments on the MOH IMDIU's practices and procedures in relation to privacy complaints and inquiries and these were addressed by the MOH IMDIU. No outstanding compliance issues were identified in the MOH IMDIU's practices and procedures regarding privacy complaints and inquiries and no orders are necessary.

Appendix A: Summary of Orders and Recommendations to Report Back

Order #1

On or before April 29, 2022, the MOH IMDIU must:

a) change its documented practices and procedures to clearly require that logs, lists, inventories or documentation under requirements 5.3, 8.3, 12.2, 22.3, 25.3, and 27.3 be periodically reviewed in accordance with requirement 1.3;
b) ensure that the changed practices and procedures in a) address the process for conducting these reviews and identify the member responsible for compliance in accordance with requirements 1.1-1 and 1.1-2; and
c) send written confirmation to the IPC of compliance with this order.

Order #2

On or before April 29, 2022, the MOH IMDIU must:

a) implement a documented practice and procedure to ensure that members responsible for addressing actual or suspected privacy and security breaches, or for implementing the business continuity and disaster recovery plan, periodically conduct simulation exercises;
b) ensure that the implemented practice and procedure in a) addresses the process for conducting these simulation exercises and identifies the member responsible for compliance in accordance with requirements 1.1-1 and 1.1-2; and
c) send written confirmation to the IPC of compliance with this order.

Order #3

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

a) implement the documented practice and procedure of conducting an up-to-date PIA(s), or ensure that an up-to-date PIA(s) has been conducted, of BIT and DTT in compliance with requirement 4;
b) prioritize and address any recommendations resulting from the PIA(s) in a) 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 #4

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

a) implement the documented practice and procedure of conducting an up-to-date TRA(s), or ensure that an up-to-date TRA(s) has been conducted, of DTT in compliance with requirement 11;
b) prioritize and address the 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 #5

On or before June 30, 2022, the MOH IMDIU must:

a) change its documented practices and procedures to:
   i. log the information specified under requirement 11.5 for events occurring in the DI Environment;
   ii. make the information logged under a) available to the Compliance Officer for regular monitoring of privacy and security breaches; and
b) send written confirmation to the IPC of compliance with this order.

For greater clarity, order provision a)i. includes logging all reasonably foreseeable member activities that may involve transmitting personal information and/or coded information from any system in the DI Environment to the member's workstation.[96]

Order #6

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

a) implement the documented practice and procedure, or ensure the implementation of the documented practice and procedure, of a business continuity and disaster recovery plan that applies to the items listed in requirement 13.2.2-7; and
b) send written confirmation to the IPC of compliance with this order.

Order #7

On or before June 30, 2022 the MOH IMDIU must:

a) change its documented privacy and security breach management practices and procedures to:
   i. include the full definition of "privacy breach" and "security breach" from the Data Standards;
   ii. ensure that it applies to the entire "DI environment" as defined in the Data Standards;
   iii. specifically describe how it is determined whether a privacy breach or security breach occurred – including whether a particular action is or is not authorized;
   iv. clearly refer to the obligation to notify the IPC and affected individuals in accordance with s. 49.11(3) of *FIPPA* and mandate that the minimum required information is included in notifications to affected individuals and the IPC;
   v. assign a responsible member role for assessing the effectiveness of notifications; and
   vi. specifically require that that all reasonable steps are taken in a timely manner to eliminate and reduce the risk of future privacy and security breaches; and
b) send written confirmation to the IPC of compliance with this order.

Order #8

On or before April 30, 2022, the MOH IMDIU must:

a) change its documented practices and procedures to specifically and clearly ensure the separation of member roles for coding and linking processes using administrative, technical and physical safeguards that are reasonable in the circumstances in accordance with requirement 19.2 and having regard to the IPC's above comments;

96 This is an instance "where PI and/or coded information is viewed, handled or otherwise dealt with" within the meaning of requirement 11.5.2-4.

b) ensure that the changed practice and procedure in a) addresses the process for separating member roles and identifies the member responsible for compliance in accordance with requirements 1.1-1 and 1.1-2; and
c) 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 MOH 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 coded information.

Recommendation to Report Back #2

On or before one year after the date of this report, the MOH IMDIU should:

a) refine its practices and procedures with respect to 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; and
b) consult with the IPC on these practices and procedures.

Recommendation to Report Back #3

On or before June 30, 2022, the MOH IMDIU should:

a) work with its Ontario Public Service partners to document its practices and procedures applicable to the physical security of its premises; and
b) provide these practices and procedures to the IPC.

Recommendation to Report Back #4

On or before June 30, 2022, the MOH IMDIU should:

a) refine and clarify the relationship between GO-ITS standards, standard operating procedures and the DI Manual in its documented practices and procedures; and
b) consult with the IPC on these practices and procedures.

For greater clarity, this recommendation applies to all instances in which the MOH IMDIU relies on GO-ITS standards to demonstrate compliance with Part III.1 and the Data Standards.

Recommendation to Report Back #5

On or before six months after the date of this report, the MOH IMDIU should:

a) refine and clarify its practices and procedures regarding secure disposal and secure destruction, including certificates of secure disposal or destruction; and
b) consult with the IPC on these practices and procedures.

For greater clarity, this recommendation applies to the MOH IMDIU's practices and procedures under requirements 15, 16 and 17.

Appendix B: List of Submitted Practices and Procedures and Representations

MOH IMDIU Practices and Procedures

September 23, 2021

- OPS Data Integration Practices and Procedures Manual (2021-09-21) v2.0

October 19, 2021

- CERTIFICATE OF DESTRUCTION v1.0
- DATA SHARING AGREEMENT (DSA) LOG v1.0
- De-IDandLinkageSpecificationTemplate_v1.0
- DI – Written Acknowledgment (Collection) v1.0.doc
- DI – Written Acknowledgment (Disclosure) v1.0
- DI REQUEST PROJECT LOG v1.0
- DI User Confidentiality Agreement v1.0.doc
- ENVIRONMENT SPECIFIC LOG REPORT v1.0
- LOG OF CONFIDENTIAL REPORTS BY MEMBERS v1.0
- LOG OF INTERNAL REVIEWS OF PRACTICES AND PROCEDURES v1.0
- LOG OF PRIVACY AND SECURITY BREACHES v1.0
- LOG REVIEW v1.0
- P&S Training Module 1 – Introduction to Data Integration and *FIPPA* Part III.1 v1.0
- P&S Training Module 2 – Protecting Data Privacy and Security v1.0
- P&S Training Module 3 – Collection, Use and Disclosure v1.0
- PIA COMPLETED LOG v1.0
- PIA NOT COMPLETED LOG v1.0
- PUBLIC INQUIRIES OR COMPLAINTS LOG v1.0
- Release Message to Requestor v1.0
- TRA, PEN TEST and VS TRACKING LOG v1.0
- TRAINING TRACKING LOG v1.0
- USER REGISTRATION AND ACCESS LOG v1.0
- WRITTEN ACKNOWLEDGEMENTS (WA) LOG v1.0

October 22, 2021

- VISITOR SIGNIN SHEET v1.0

November 1, 2021

- DI User Confidentiality Agreement v1.0

November 2, 2021

- DII Data Sharing Agreement template 10.22.21 DRAFT FOR REVIEW
- DSA schedule Mapping to standards v1.0

November 4, 2021

- Data Integration Request Form v1.0

November 9, 2021

- Privacy Assessment Template v1.0

November 19, 2021

- DRAFT_Annual Report_IMDIU Template_1.5_for IPC review
- DRAFT_Notice of Collection_IMDIU_Template_2.3 for IPC review

December 22, 2021

- Data Holdings Inventory 2021Dec22
- DII Operational + Data Governance 2021Dec22
- MOH DI Data Management SOP 2021Dec22

January 10, 2022

- Data Integration Initiative PIA v0.4 2021-09-01
- Data Sharing Agreement Template v2.0
- MOH DI Compliance Management SOP v1.0
- MOH DI Data Management SOP v2.0
- MOH DI Environment Managment SOP v1.0
- MOH DI Request Management SOP v1.0
- MOH DI User Management SOP v1.0

January 19, 2022

- DI – Written Acknowledgment (Collection) v2.0.doc
- DI – Written Acknowledgment (Disclosure) v2.0
- P&S Training Module 1 – Introduction to Data Integration and *FIPPA* Part III v2.0
- P&S Training Module 2 – Protecting Data Privacy and Security v2.0
- P&S Training Module 3 – Collection, Use and Disclosure v2.0
- Privacy Assessment Template v2.0

January 21, 2022

- Data Field Classification Framework 2021-09-28

January 24, 2022

- IPC Response Secure Disposal and Destruction Jan 24 2022

January 25, 2022

- DI User Confidentiality Agreement v2.0
- MOH MLTC DI Business Rules v.1.0

February 1, 2022

- BAP Functional Requirements Document.pdf
- Change Request Form and Applicable Impact Matrix v1.0
- De-identification and Linkage Specification Template V2.0
- DIU-Continuity Management Plan-Vs 0.7 (1 Mar 2021)
- DRAFT_Annual Report_IMDIU Template_2.0
- DRAFT_Notice of Collection LIST_IMDIU_Template_2.0 NEW
- DRAFT_Notice of Collection_IMDIU_Template_3.0
- ENVIRONMENT SPECIFIC LOG REPORT v2.0
- Mapping between User Role and Environment Components and Tools v1.0
- MOH HSC-Capacity Planning and Analytics SLA F2020-21 FINAL.pdf
- MOH MLTC Hardware and software Inventory v1.0
- USER REGISTRATION AND ACCESS LOG v2.0

February 10, 2022

- Business Impact Matrix-Draft (18 Feb 2021)
- Continuity Recovery Template v01-Feb08-22
- DI Breach Audit Completion Form v1.0
- DI Breach Audit Procedures v02-Feb4-2022
- DI Maintenance Plan Feb 04 2022 v1.0
- DII Diagrams (work in progress) V21 enabled
- DII Diagrams (work in progress) V21
- DII IT Solution Aug 17 2020
- LOA# 21-010 HSC Data Integration Initiative TRA Report v1.0 – 06.03.21 – FINAL Report.pdf
- OPS Data Integration Practices and Procedures Manual (2022-02-09) v3.0

March 2, 2022

- DI User Confidentiality Agreement v2.0 [2022-03-02 MOH Staff Responses]
- Privacy Assessment Template v2. [2022-03-02 MOH Staff Responses]
- PS Training Module 1 – Introduction to Data Integration and *FIPPA* Part III v2.0 [2022-03-02 MOH Staff Responses]
- PS Training Module 2 – Protecting Data Privacy and Security v2.0 [2022-03-02 MOH Staff Responses]
- PS Training Module 3 – Collection Use and Disclosure v2.0 [2022-03-02 MOH Staff Responses]

March 9, 2022

- DII Maintenance Plan-Mar8-22
- Remote Access Instructions-Mar8-22
- GO-ITS X-Ref

MOH IMDIU Responses to IPC staff comments

December 22, 2021

4. Secure Disposal and Secure Destruction 2021Dec22

January 10, 2022

1. General Requirements.2022-01-07
2. Collection Use and Disclosure.2022-01-07
5. Retention Period.2022-01-07
6. De-Identification and Linking.2022-01-07
7. Public Notice and Annual Reporting.2022-01-07

January 28, 2022

- IPC – MOH IMDIU Secure D-D Response – Jan28-22

February 1, 2022

3. Secure Retention and Transfer.2022-01-31

March 2, 2022

- General Requirements [2022-03-2 MOH Staff Responses]
- Collection Use and Disclosure [2022-03-02 MOH Staff Responses]
- Secure Retention and Transfer [2022-03-02 MOH Staff Responses]
- Secure Disposal and Secure Destruction [2022-03-03 MOH Staff Responses]
- Retention Period [2022-03-03 MOH Staff Responses]
- De-Identification and Linking [2022-03-02 MOH Staff Responses]
- Public Notice and Annual Reporting [2022-03-02 MOH Staff Responses]

March 9, 2022

- DIU Responses to IPCs March 9-22
- DII-Standards-Logs Mapping

March 13, 2022

- MOH response to IPC March 11 2022

Review of the Practices and Procedures of the Ministry of Health's 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

March 2022