Ontario

Ontario Public Service Data Integration Data Standards

Ministry of Government and Consumer Services
April 2021

Table of Contents

DOCUMENT HISTORY

Date	Summary
April 2021	Created: Ontario Public Service Data Integration Data Standards v1.0

ONTARIO PUBLIC SERVICE DATA INTEGRATION DATA STANDARDS

INTRODUCTION

Part III.1 Data Integration (the Part) of the *Freedom of Information and Protection of Privacy Act, 1990* (*FIPPA*) allows the Ontario government and other designated organizations to better leverage information across ministries and other publicly-funded organizations. It enables the development and integration of cross-sectoral and sectoral datasets to derive insights into how government programs and services can be better delivered to Ontarians.

These data integration provisions were introduced in 2019 and provide the government with the tools to create a more data-driven public service. The Part provides for the designation of ministry data integration units, inter-ministerial data integration units and extra-ministerial data integration units (collectively referred to as “DI Units”). Under the Part, DI Units may indirectly collect personal information (PI) for linking to create, and enable access to, de-identified datasets for the purposes of analysis in relation to:

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

Given these authorities, maintaining public trust and ensuring that DI Units act responsibly is paramount to the success of the Part. To ensure transparency, accountability and the protection of privacy, the Part provides a set of rules and safeguards that regulate the manner in which DI Units collect, link, use, disclose, de-identify, retain, transfer and dispose of PI. It also defines an oversight role for the Information and Privacy Commissioner of Ontario (IPC), who is responsible for reviewing the practices and procedures of DI Units, among other things.

To further refine and determine its set of rules and safeguards, the Part requires the development of data standards, which are set out in this document (the “Data Standards”). The Data Standards contain a minimum set of requirements for promoting responsible stewardship of PI throughout its life cycle under the Part. By supplementing the requirements of the Part, the Data Standards ensure a consistent and effective approach to transparency, accountability and protection of privacy across all DI Units. In some cases, DI Units may be required to go beyond the specific protections in the Data Standards in order to meet the broader obligations imposed by the Part.

The Data Standards are divided into the following categories:

1. General Requirements
2. Collection, Use and Disclosure
3. Secure Retention and Transfer
4. Secure Disposal and Secure Destruction
5. Retention Period

6. De-identification and Linkage
7. Public Notice and Annual Reporting

TYPES OF INFORMATION SUBJECT TO THE DATA STANDARDS

The Data Standards apply to PI throughout its life cycle under the Part. However, it is important to clarify the types of PI as well as stages of the life cycle that are included.

The life cycle of PI under the Part includes its de-identification at various levels. The process of de-identification involves the creation of information lying on a spectrum of identifiability between the original PI collected by the DI Unit and information that has been de-identified to an acceptable threshold before it can be made available by the DI Unit for analysis. For the purposes of these Data Standards, “coded information” refers to information included within this spectrum.

Coded information can technically be understood as a type of pseudonymized information. Coded information is PI from which direct identifiers have been removed and replaced with an internal code unique to the individual. The direct identifiers continue to exist but are segregated and kept securely by the DI Unit. To the extent coded information can be reversibly identified by the DI Unit using the available internal code, it is considered to be closer to the original PI on the spectrum of identifiability. Therefore, it is treated generally the same as PI and, among other things, is subject to the individual rights of access and correction to PI under *FIPPA*. Coded information is held by DI Units for the purposes of preparing datasets that will ultimately be fully de-identified and made available for analysis. In order to protect coded information from risks relating to unauthorized re-identification, many of the requirements of the Data Standards need to apply to both PI and coded information.

Coded information in the hands of a person, entity or organization that does not have access to the direct identifiers may or may not be considered de-identified. Information is de-identified when it has been stripped of all information that identifies an individual and that could be used, either alone or with other information, to identify an individual based on what is reasonably foreseeable in the circumstances. A determination of whether PI has been de-identified to an acceptable threshold for release depends on the context and safeguards. Information may be considered de-identified in a certain context with specific safeguards in place (e.g., if released to another part of the same ministry for analysis in a strictly controlled environment), but identifiable in a different context without those safeguards (e.g., if released to the public with no controls in place).

Even de-identified information has some residual risk of re-identification. Therefore, to protect privacy, the Data Standards apply to some de-identified information in certain contexts to protect it from reasonably foreseeable risks of re-identification. For example, restrictions apply to the release of de-identified information outside the DI Units. Similarly, Data Standards relating to the secure retention, secure transfer, secure disposal/destruction, de-identification and linking, privacy and security breach provisions should also be interpreted as protecting de-identified information from reasonably foreseeable risks of re-identification.

However, subject to the requirement that no person or entity shall use or attempt to use information that has been de-identified under the Part to identify an individual, the regulation of de-identified information in the Data Standards should not stifle the release of general statistical information. As such, the Data Standards should not be interpreted as imposing restrictions on information that has been de-identified to the extent necessary for a release to the public. This ensures that the Data Standards do not unduly regulate the public release of general statistical information or open data, where the information is sufficiently de-identified and made available to anyone for download or use without any conditions.

PERSONAL HEALTH INFORMATION

Under *FIPPA*, the definition of PI includes information about an individual's medical, psychiatric or psychological history. The Part also permits the collection of personal health information from persons and entities regulated by the *Personal Health Information Protection Act, 2004*, in limited circumstances. As such, references to PI under the Data Standards include an individual's personal health information, unless the context indicates otherwise.

LEGAL AUTHORITY

The Data Standards are developed by the responsible minister, the Minister of Government and Consumer Services. Section 49.14 (1) (a) of *FIPPA* requires the Minister to prepare draft data standards, including practices and procedures (Practices and Procedures) for use when collecting, using and disclosing PI, de-identifying and linking PI, publicly reporting on the use of PI, securely retaining PI, and securely disposing of PI under the Part. These Data Standards have been provided to, and approved by, the IPC under s. 49.14 (1) (b).[1]

To demonstrate due diligence and provide evidence of compliance, the Data Standards inform the required development and implementation of supporting accountability measures and administrative safeguards in the form of Practices and Procedures. As such, the Data Standards include requirements for Practices and Procedures that must be addressed within each DI Unit.

APPLICATION

As set out in s. 49.14 (4) of *FIPPA*, all members of all DI Units must comply with the Data Standards. All members must also comply with the Part, the Practices and Procedures developed and implemented by their DI Unit, other applicable provisions of *FIPPA* and its regulations, and any agreements and acknowledgements made pursuant to them.

[1] See https://www.ipc.on.ca/decisions/data-integration/

GENERAL REQUIREMENTS

This standard outlines general requirements for DI Units to ensure that all the Data Standards are effectively implemented and appropriately documented. Accountability measures and training requirements are intended to enhance compliance and consistency of practice, as well as to uphold operational integrity across all DI Units.

The goal of implementing the Data Standards is to create a privacy governance and accountability framework. This framework enables DI Units to have a comprehensive, effective and cohesive approach for preventing, identifying, reviewing, logging, tracking, investigating and remediating non-compliance or risks of non-compliance with:

- the Part;
- the Data Standards;
- their Practices and Procedures;
- other applicable provisions of *FIPPA* and its regulations; and
- any agreements and acknowledgements made pursuant to them.

A critical component of this framework, as defined in the Data Standards, is the consistent and systematic tracking or logging of all findings and recommendations resulting from DI Units' reviews, assessments, and investigations to ensure they are addressed in a timely manner.

OVERARCHING REQUIREMENTS

To ensure that DI Units comply with the Part, DI Units must:

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.
2. Provide initial and annual privacy and security awareness training to all members.
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.
4. Conduct a privacy impact assessment (PIA) to identify, analyze and mitigate potential privacy risks where required.

RELEVANT PROVISIONS OF THE PART

These general requirements are outlined in accordance with the following provisions of the Part:

- Practices and Procedures – s. 49.12
- Data Standards – s. 49.14 (1) (a)

SPECIFIC REQUIREMENTS

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.	
1.1	For each requirement set out in the Part, its regulations and the Data Standards, describe in the Practices and Procedures: 1. member reporting lines, duties, roles, any delegations of authority, and the role of the member with responsibility for compliance with the requirement; 2. internal accountability structures, processes, and approval requirements, including the role of the member with authority to grant approval, and how and to whom this approval will be communicated; 3. a requirement to document decisions relating to PI and/or coded information; 4. the minimum content of documentation including notices/notifications, information, agreements, acknowledgements and certificates that must be completed, provided or made, by whom, and how and to whom they must be communicated; 5. the minimum content and the method, nature and format of communications; 6. applicable time frames; and 7. remedial steps to be taken where a requirement to return any item or information, or to obtain or provide a notice, information, agreement, acknowledgment or certificate, is not complied with.
1.2	**1.2.1** Comply with the Part, the Data Standards, the Practices and Procedures**,** other applicable provisions of *FIPPA* and its regulations, and agreements and acknowledgements made pursuant to them. This requirement applies to all DI Unit members and DI Unit activities. **1.2.2** DI Units must exercise discretion in a manner that is reasonable in the circumstances, where a requirement gives discretion to DI Units to determine how it will be implemented.
1.3	**1.3.1** DI Units must internally review any log, list, inventory or documentation that they are required to develop and maintain by the Data Standards to ensure that it is up-to-date, and to detect non-compliance or risks of non-compliance with the relevant requirements. Such reviews must be conducted periodically, or as otherwise indicated in the Data Standards. **Note:** This requirement applies to Requirements 1.5, 2.5, 3.3, 4.3, 4.4, 5.3, 5.4, 6.3, 6.7, 7.3, 7.7, 8.3, 10.3, 11.4, 11.5, 12.2, 14.4, 17.3-2, 18.5, 22.3, 25.3, and 27.3. **1.3.2** Where an internal review of a specific log, list, inventory or documentation identifies non-compliance or a risk of non-compliance, this must be addressed in a timely manner. **1.3.3** DI Units must document these reviews, including:

	1. the specific log, list, inventory or documentation reviewed; 2. the date of the internal review; 3. the name(s) of the member(s) responsible for completing the review; 4. any non-compliance or risks of non-compliance detected; 5. the recommendations arising from the review; 6. the name(s) of the member(s) responsible for addressing each recommendation; 7. the date by which each recommendation was, or is expected to be, addressed; and 8. how each recommendation was, or is expected to be, addressed.
1.4	**1.4.1** In addition to reviews of specific, logs, lists, inventories and documentation under Requirement 1.3, conduct an internal review of the Practices and Procedures and their implementation, at a minimum once every three years, to ensure that: 1. they are up-to-date; 2. they continue to address each of the requirements set out in the Part, its regulations, the Data Standards, and agreements and acknowledgements made pursuant to them; 3. there is cohesion across the implemented Practices and Procedures within the DI Unit; 4. recommendations arising from reviews, assessments and investigations are implemented in a timely manner; and 5. the DI Unit and its members are complying with the Part, its regulations, the Data Standards, Practices and Procedures, and any agreements and acknowledgements made pursuant to them. **1.4.2** Revise the Practices and Procedures to address any recommendations arising from the internal review of the Practices and Procedures and their implementation in a timely manner.
1.5	**1.5.1** Develop and maintain a log of internal reviews conducted of the Practices and Procedures and their implementation. **1.5.2** At a minimum, the log must include: 1. the nature, scope and type of the review conducted, including how sampling was undertaken; 2. the date that the review was completed; 3. the name(s) of the member(s) responsible for completing the review; 4. any non-compliance or risks of non-compliance detected; 5. the recommendations arising from the review; 6. the name(s) of the member(s) responsible for addressing each recommendation; 7. the date by which each recommendation was, or is expected to be, addressed; and 8. how each recommendation was, or is expected to be, addressed.

Requirement 2: Provide initial and annual privacy and security awareness training to all members.	
2.1	**2.1.1** Require all members to complete comprehensive and up-to-date privacy and security awareness training upon commencement of their employment, contractual or other relationship with the DI Unit and, at a minimum, annually thereafter to understand their obligations under *FIPPA*, including: 1. the Part; 2. the Data Standards; 3. the Practices and Procedures; 4. other applicable provisions of *FIPPA* and its regulations; and 5. agreements and acknowledgements made pursuant to them. **2.1.2** At a minimum, the training must include: 1. the definitions of PI, coded information and de-identified information; 2. the authority for the collection, use and disclosure of PI and coded information; 3. the purposes for which PI, coded information and de-identified information is permitted to be collected, used and disclosed, and any applicable limitations, conditions and restrictions; 4. the nature of the information collected by the DI Unit and from whom this information is typically collected; 5. the procedures that must be followed when disclosing PI, coded information and de-identified information outside the DI Unit; 6. the member's duties and responsibilities relating to privacy and security breaches and the consequences of non-compliance; 7. the relevant administrative, technical and physical safeguards implemented to protect PI and coded information against theft, loss and unauthorized use or disclosure, including the secure manner in which such information must be retained, transferred and disposed of or destroyed; 8. the duties and responsibilities related to implementing these administrative, technical and physical safeguards; 9. that members are prohibited from: a. collecting and using PI, coded information and de-identified information except as permitted in the confidentiality agreement that members must execute; and b. disclosing such information except as permitted in the confidentiality agreement or as required by law; and 10. the process to be followed where: a. de-identified information is being disclosed further to a right of access under s. 10 of *FIPPA*; and b. PI and/or coded information is being disclosed further to the rights of access and correction under s. 47 of *FIPPA*; and 11. the limits on use of de-identified information pursuant to s. 49.8 of the Part.

	2.1.3 The content of training must relate to members' particular roles in order to ensure that members understand how to apply the Practices and Procedures in their day-to-day employment, contractual or other relationships with the DI Unit.
2.2	Only permit members to access the DI Environment after the required initial privacy and security awareness training is completed.
2.3	Ensure that training materials are periodically reviewed and kept up-to-date so they: 1. continue to address the requirements defined in the Part, the Data Standards, the Practices and Procedures, other applicable provisions of *FIPPA* and its regulations, and agreements and acknowledgements made pursuant to them; and 2. reflect any applicable findings and recommendations resulting from reviews, assessments and investigations conducted by the DI Unit.
2.4	**2.4.1** 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. These exercises are conducted for training purposes and to identify recommended improvements to the Practices and Procedures of the DI Unit. **2.4.2** Ensure that any recommendations arising from these simulation exercises are implemented in a timely manner.
2.5	**2.5.1** Develop and maintain a log of members' privacy and security awareness training. **2.5.2** At a minimum, the log must include: 1. the name of each member; 2. the date that the member completed the initial privacy and security training; and 3. the dates that the member completed ongoing privacy and security training.

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.	
3.1	At a minimum, the process must facilitate members' reporting of: 1. gaps or deficiencies in the DI Unit's Practices and Procedures, business processes, privacy and security measures and controls, and accountability structures; and 2. actual or suspected incidents of non-compliance by other members with the Part, the Data Standards, the Practices and Procedures, other applicable

	provisions of *FIPPA* and its regulations, and agreements and acknowledgements made pursuant to them. **Note:** The purpose of this process is to outline the way in which members can express concerns about actual or suspected wrongdoing within the DI Unit without fear or risk of retribution.
3.2	**3.2.1** Ensure that: 1. the reporting process is confidential and identifies the applicable roles, responsibilities and required next steps to address raised concerns in a timely manner; and 2. reports are not made to, or addressed by, an individual involved in the matter or with direct authority over any of the individuals or DI Unit activities involved in the matter. **3.2.2** If the concerns give rise to an actual or suspected privacy or security breach, then the DI Unit must respond to the concern in accordance with Requirement 14.
3.3	**3.3.1** Develop and maintain a log of reports by members under Requirement 3. **3.3.2** At a minimum, the log must include: 1. a description of the gaps or deficiencies or actual or suspected incidents of non-compliance reported; 2. the date of the report; 3. the name(s) of the member(s) responsible for responding to the report; and 4. the steps taken in response to the report including dates on which they were completed or expected to be completed.

Requirement 4: Conduct a privacy impact assessment (PIA) to identify, analyze and mitigate potential privacy risks where required.	
4.1	**4.1.1** Identify and define the circumstances or events that would trigger a PIA or update to a PIA within the DI Unit. **4.1.2** At a minimum, a PIA must be conducted prior to: 1. a new collection of PI; and 2. implementation of a new program, process, technology or system relating to the DI Unit's activities under the Part that could affect the privacy of individuals or the confidentiality of information. **4.1.3** At a minimum, an update to a PIA must be done prior to: 1. a change to an ongoing collection of PI; and

	2. a change to a program, process, technology or system relating to the DI Unit's activities under the Part where the change could affect the privacy of individuals or the confidentiality of information. **Note:** A new collection is when PI is collected from a source for the first time. An ongoing collection is when the same data elements of PI are collected from the same source on a defined basis (e.g., the same data elements of PI are collected every month for two years). A new PIA is not required at each new instance of a collection that is part of an ongoing collection. However, if an ongoing collection of PI is to be changed, prior to the change being implemented, DI Units should update their PIA by conducting a delta analysis to identify potential new risks and related recommendations (i.e., mitigations). If no PIA was previously conducted on the program, process, technology or system to be changed, then a new PIA must be conducted. While PIAs will generally be conducted in relation to PI, there may also be circumstances in which a PIA may need to be conducted in relation to coded or de-identified information (e.g., where there is a change to a program, process, technology or system dealing with coded information or de-identified information that may create new privacy risks). To address such circumstances, the minimum content of a PIA includes references to coded and de-identified information (as applicable).
4.2	**4.2.1** Identify and define the required content of a PIA. **4.2.2** At a minimum, a PIA must include: 1. a description of the collection of PI and/or the program, process, technology or system at issue; 2. the nature and type of PI, coded information and/or de-identified information collected, used or disclosed; 3. the sources of the PI, coded information and/or de-identified information; 4. the purpose(s) for which the PI, coded information and/or de-identified information is collected, used or disclosed; 5. the reason the PI and/or coded information is required for the identified purposes (i.e., as opposed to being able to use de-identified information); 6. the flows of the PI, coded information and/or de-identified information (i.e., who will have access to it, when and for what purpose); 7. the statutory authority for each collection, use and disclosure identified in the PIA; 8. any limitations imposed on the collection, use and/or disclosure of the PI, coded information and/or de-identified information; 9. whether or not the PI and/or coded information is, or will be, linked to other information, the nature and source of any information to which it will be linked, how linkages will be conducted, and why the linkages are required for the identified purpose(s);

	10. whether or not the PI and/or coded information will be de-identified and the de-identification process; 11. the retention period for the PI coded information and/or de-identified information; 12. the secure manner in which the PI and/or coded information is, or will be, retained, transferred and disposed of or destroyed; 13. the risks to the privacy of individuals or confidentiality of information arising from the collection of PI and/or the program, process, technology or system, and an assessment of the privacy or confidentiality risks; 14. recommendations to address and eliminate or reduce the privacy and/or confidentiality risks identified; and 15. the administrative, technical and physical safeguards implemented or proposed to be implemented, to protect against privacy and/or confidentiality risks. **4.2.3** Prioritize and address the recommendations resulting from PIAs to address and eliminate privacy and/or confidentiality risks in a timely manner.
4.3	**4.3.1** Develop and maintain a log of PIAs that have been completed or are being completed within the DI Unit. **4.3.2** At a minimum, the log must include: 1. a description of the collection of PI and/or the program, process, technology or system at issue; 2. the date(s) that the PIA was completed or updated or is expected to be completed or updated; 3. the name(s) of the member(s) responsible for completing/updating or ensuring the completion/update of the PIA; 4. the recommendations arising from the PIA; 5. the name(s) of the member(s) responsible for addressing each recommendation; 6. the date that each recommendation was, or is expected to be, addressed; and 7. how each recommendation was, or is expected to be, addressed.
4.4	**4.4.1** Develop and maintain a log of all instances where a determination is made that a PIA will not be conducted or updated in relation to changes to, or implementation of, a program, process, technology or system relating to the DI Unit's activities under the Part. **4.4.2** At a minimum, this log must include: 1. the implemented or changed program, process, technology or system; 2. the date the determination was made; 3. the reason that a PIA was not conducted or updated; and 4. the name(s) of the member(s) responsible for making this determination.

COLLECTION, USE AND DISCLOSURE

This standard outlines the minimum requirements that the DI Units must meet when collecting, using and disclosing PI, coded information and de-identified information, as applicable. DI Units must take reasonable steps to ensure the protection of privacy, comply with their legal obligations and ensure that the persons, entities and organizations they interact with do the same.

OVERARCHING REQUIREMENTS

To ensure that DI Units comply with the Part, DI Units must:

5. Collect, use and disclose PI, coded information and/or de-identified information only in accordance with applicable requirements in the Part, the Data Standards, the Practices and Procedures, other applicable provisions of *FIPPA* and its regulations, and agreements and acknowledgements made pursuant to them.
6. Execute a data sharing agreement (DSA) or obtain a written acknowledgement when collecting or disclosing PI, coded information and/or de-identified information, where required.

RELEVANT PROVISIONS OF THE PART

The requirements for the collection, use and disclosure of PI, coded information and de-identified information are outlined in accordance with the following provisions of the Part:

- Purpose for the collection of personal information – s. 49.2
- General rule re personal information – s. 49.3 (1)
  - Extent of information (2)
- Collection of personal information – s. 49.4 (1)
  - Collection of personal information, ministry data integration unit (2)
  - Additional requirements (3)
  - Disclosure to unit (4)
  - Conflict (5)
  - Same (5.1)
  - Collection of excluded information (6)
- Restrictions on collection – s. 49.5 (1)
  - Collection of personal health information (1.1)
  - Definitions (2)

- Linking and de-identification – s. 49.6 (1)
  - Same (2)
- Limits on use of personal information – s. 49.7 (1)
  - Extra-ministerial data integration unit (1.1)
  - Reporting on use (2)
- Limits on use of de-identified information – s. 49.8
- Disclosure of personal information – s. 49.9 (1)
  - Exception (2)
- Notice of collection – s. 49.10
- Data standards – s. 49.14 (1) (a) (i)
- Regulations – s. 49.15 (1)
  - Inter-ministerial data integration unit (2)

Other relevant provisions of *FIPPA*:

- Part III.1 record s. 10 (1.1)
- Application of the Part - Same – s. 37 (2)
- Request and manner of request (Exception, s. 25) – s. 48 (2.1)

SPECIFIC REQUIREMENTS

Requirement 5: Collect, use and disclose PI, coded information and/or de-identified information only in accordance with applicable requirements in the Part, the Data Standards, the Practices and Procedures, other applicable provisions of *FIPPA* and its regulations, and agreements and acknowledgements made pursuant to them.	
Collection	
5.1	Identify and define: 1. the requirements and/or conditions that must be satisfied to permit the collection of PI and coded information, including all requirements in the Part, the Data Standards, the Practices and Procedures, other applicable provisions of the *FIPPA* and its regulations, and agreements and acknowledgements made pursuant to them; 2. the types of persons and entities from whom PI and/or coded information may be collected; 3. the purpose(s) for which PI and/or coded information is collected; and 4. any restrictions that may apply to the collection of PI and/or coded information.
5.2	Ensure PI and/or coded information is collected only where: 1. it is authorized for defined purposes and circumstances, and all conditions, requirements and restrictions have been satisfied;

	2. the purpose of the collection could not otherwise be served by collecting other information (such as by collecting de-identified information); 3. no more PI and/or coded information will be collected than is reasonably necessary to meet the purposes of the collection; 4. the minister or a person designated by the minister (or the senior officer in the case of an extra-ministerial DI Unit) has considered the privacy interests of affected individuals and how their PI and/or coded information will be protected; and 5. the minister or a person designated by the minister (or the senior officer in the case of an extra-ministerial DI Unit) has determined that there is a public interest in collecting the PI and/or coded information.
5.3	Develop and maintain an up-to-date description of: 1. the purpose for which PI and/or coded information is collected; 2. the nature and type of PI and/or coded information collected; 3. entities from whom PI and/or coded information is collected (i.e., the source); 4. entities from whom PI and/or coded information cannot be collected pursuant to s. 49.5 of the Part; and 5. the means by which PI and/or coded information is collected (e.g., via secure transfer, via email, via courier, etc.).
5.4	**5.4.1** Develop and maintain an inventory of PI and coded information within the DI Unit. **5.4.2** At minimum, the inventory must include: 1. the purpose of the collection of the PI or coded information; 2. the specific data elements or fields contained within the PI or coded information (e.g., gender, date of birth or age, event dates, locations, etc.); 3. the source(s) of the PI or coded information; and 4. the need for the PI or coded information in relation to the identified purpose. **5.4.3** Internal reviews of the inventory must be conducted annually.

Use	
5.5	Identify and define: 1. the requirements and conditions that must be satisfied to permit the use of PI and/or coded information, including all requirements in the Part, the Data Standards, the Practices and Procedures, other applicable provisions of *FIPPA* and its regulations, and agreements and acknowledgements made pursuant to them;

	2. the purposes for which PI and/or coded information may be used, including the use of PI and/or coded information for the purpose of facilitating a right of access and correction under s. 47 of *FIPPA*; and 3. any restrictions that may apply to the use of PI and/or coded information.
5.6	Ensure PI and/or coded information is only used where: 1. it is authorized for defined purposes and circumstances, and all conditions, requirements and restrictions have been satisfied; 2. the purpose(s) of the use could not otherwise be served by using other information (such as by using de-identified information); 3. no more PI and/or coded information will be used than is reasonably necessary to meet the purpose(s) of the use; 4. it is limited to the minimum amount and least identifiable PI and/or coded information that is necessary for carrying out their DI-related responsibilities; 5. it is limited to those members who require the use in order to carry-out their responsibilities in the DI Unit; and 6. the length of time for which use is permitted has been defined and will not exceed a timeframe that is reasonably necessary to meet the identified purpose.
5.7	Restrict members from using coded information, alone or in combination with other information, to identify an individual, except as specifically identified and defined under Requirement 5.5.

Disclosure	
5.8	Identify and define: 1. the requirements and conditions that must be satisfied to permit the disclosure of PI, coded information and/or de-identified information, including all requirements in the Part, the Data Standards, the Practices and Procedures, other applicable provisions of *FIPPA* and its regulations, and agreements and acknowledgements made pursuant to them; 2. the types of entities to whom PI, coded information and/or de-identified information may be disclosed; 3. the purpose for which the PI, coded information and/or de-identified information may be disclosed; and 4. the process to be followed where: a. de-identified information is being disclosed further to a right of access under s. 10 of *FIPPA*; and b. PI and/or coded information is being disclosed further to the rights of access and correction under s. 47 of *FIPPA*.
5.9	Ensure members only disclose PI, coded information and/or de-identified information where:

	1. it is authorized for defined purposes and circumstances, and all conditions, requirements and restrictions have been satisfied; 2. in the case of PI and/or coded information, the identified purpose cannot reasonably be accomplished without disclosing the PI and/or coded information; and 3. no more PI and/or coded information will be disclosed than is reasonably necessary to meet the identified purpose. **Note:** DI Units may disclose PI, coded information and/or de-identified information to members of the same DI Unit who need access to the information in the performance of their duties under this Part. DI Units should address the disclosure of PI and/or coded information to their own members in their Practices and Procedures developed for the specific requirements for use under Requirements 5.5 to 5.7. The specific requirements for use under Requirements 5.5 to 5.7 do not apply to de-identified information. As such, the disclosure of de-identified information to members may, or may not, be addressed in the specific requirements for use, at the discretion of the DI Unit.

Requirement 6: Execute a data sharing agreement (DSA) or obtain a written acknowledgement when collecting or disclosing PI, coded information and/or de-identified information, where required.	
6.1	**6.1.1** Execute a DSA in relation to a collection or disclosure of PI, coded information and/or de-identified information where it is reasonably necessary to protect the privacy of individuals and the confidentiality of information. **6.1.2** At a minimum, a DSA is reasonably necessary and must be executed when: 1. collecting PI and/or coded information from a source outside the person, entity or organization in which the DI Unit is located (e.g., the ministry); 2. disclosing PI and/or coded information to another DI Unit outside of the person, entity or organization in which the DI Unit is located; and 3. disclosing PI and/or coded information to a researcher. **6.1.3** Required DSAs must be completed, approved and executed before the PI, coded information and/or de-identified information is collected or disclosed. **Note:** A DSA will generally be executed where a DI Unit is collecting or disclosing PI and/or coded information. However, there may be circumstances where a DSA is required to be executed in relation to the collection or disclosure of de-identified information by a DI Unit. For example, where it is an administrative safeguard

	required in the de-identification process or otherwise reasonably necessary in the circumstances. In these specific circumstances involving de-identified information, the requirements below apply to the collection or disclosure of de-identified information by a DI Unit.
6.2	**6.2.1** Identify and define the required content of a DSA. The content must be consistent with the Notice of Collection outlined in the Public Notice and Annual Reporting standard. **6.2.2** At a minimum, the DSA must include: 1. the parties to the DSA and their roles, including identification of the party that is collecting PI, coded information and/or de-identified information, and the party that is disclosing PI, coded information and/or de-identified information; 2. a description of the status of the DI Unit under *FIPPA* and the duties and responsibilities arising from this status, including definitions of PI, coded information and de-identification; 3. the statutory authority for the collection, use and disclosure identified in the DSA; 4. details of the PI, coded information and/or de-identified information to be collected or disclosed; 5. the source(s) of the PI, coded information and/or de-identified information; 6. the purpose(s) for which the PI, coded information and/or de-identified information will be collected or disclosed; 7. the purpose(s) for which the PI, coded information and/or de-identified information will be used, including whether it will be linked with other information; 8. if the PI and/or coded information will be linked to other information, the nature and source of any information to which it will be linked, how any linkages will be conducted, and why the linkages are required for the identified purpose(s); 9. the specific time period over which collection or disclosure will take place (e.g., monthly for two years); 10. the retention period for the PI, coded information and/or de-identified information; 11. whether the PI and/or coded information will be de-identified and the de-identification process; 12. the specific manner in which the PI and/or coded information will be securely retained, including whether it will be retained in identifiable form; 13. the specific process that will be used to securely transfer (including return, if applicable) the PI, coded information and/or de-identified information; 14. whether the PI, coded information and/or de-identified information will be returned or disposed of or destroyed in a secure manner following the retention period or termination date set out in the DSA and the timeframe within which this must be completed;

	15. the specific process that will be used to securely dispose of or destroy the PI, coded information and/or de-identified information; 16. a requirement that actual or suspected privacy and security breaches related to the DSA be reported to other parties to the DSA at the first reasonable opportunity, including the method of notification and key contacts; 17. a requirement that reasonable steps be taken to contain privacy and security breaches relating to the DSA; 18. the consequences of privacy and security breaches and whether compliance with the DSA will be audited and, if so, the manner of auditing; and 19. relevant conditions, requirements and restrictions including: a. whether PI, coded information and/or de-identified information may be further disclosed by the collecting party; b. where PI, coded information and/or de-identified information may be further disclosed by the collecting party, limitations on the subsequent use and disclosure of the PI, coded information and/or de-identified information; i. at a minimum, these limitations must include that any person, entity or organization to which de-identified information is further disclosed will agree not to use the information, alone or in combination with other information, to identify an individual; c. that the PI, coded information and/or de-identified information shall be retained only for as long as necessary to fulfill the purposes for which it was collected or as required by law; d. that the PI and/or coded information collected or disclosed pursuant to a DSA must be necessary for the purpose for which it was collected or disclosed; e. that the PI and/or coded information will only be collected, used or disclosed if other information, namely de-identified information, will not serve the purpose; f. that no more PI and/or coded information will be collected, used or disclosed than is reasonably necessary to meet the purpose; g. that reasonable steps will be taken to protect the PI and/or coded information against theft, loss and unauthorized use or disclosure and the specific reasonable steps that are required to be taken; h. that de-identified information will not be used, alone or in combination with other information, to identify an individual; and i. that all persons who will have access to the PI and/or coded information will be aware of, and agree to comply with, the terms and conditions of the DSA prior to being given access to the PI and/or coded information.
6.3	**6.3.1** Develop and maintain a log of DSAs executed by the DI Unit. **6.3.2** At a minimum, the log must include:

	1. the name of the person, entity or organization from whom the PI, coded information and/or de-identified information was collected, or to whom the PI, coded information and/or de-identified information was disclosed; 2. the date that the collection or disclosure of PI, coded information and/or de-identified information was approved; 3. the date the DSA was executed; 4. the date the PI, coded information and/or de-identified information was collected or disclosed; 5. the nature of the PI, coded information and/or de-identified information subject to the DSA; 6. the retention period for the PI, coded information and/or de-identified information set out in the DSA, or the date of termination of the DSA; 7. whether the PI, coded information and/or de-identified information will be securely returned, or will be securely disposed of or destroyed, following the retention period or termination date set out in the DSA; and 8. the actual or expected date the PI, coded information and/or de-identified information is securely returned or securely disposed of or destroyed.
6.4	**6.4.1** Where a DSA is not executed, obtain a written acknowledgment in relation to a collection or disclosure of PI, coded information and/or de-identified information where it is reasonably necessary to protect the privacy of individuals and the confidentiality of information. **6.4.2** At a minimum, a written acknowledgement is reasonably necessary and must be obtained when: 1. collecting PI and/or coded information from an area outside the DI Unit, but within the person, entity or organization in which the DI Unit is located; and 2. disclosing de-identified information to an area outside the DI Unit, but within the person, entity or organization in which the DI Unit is located. **6.4.3** A DI Unit may, or may not, require that a written acknowledgement be formally executed (i.e., signed), as reasonably necessary in the circumstances. **6.4.4** Required written acknowledgments must be obtained from the party disclosing PI, coded information and/or de-identified information to the DI Unit, or collecting PI, coded information and/or de-identified from the DI Unit before the PI, coded information and/or de-identified information is collected and/or disclosed. **Note:** Other than the two specific minimum circumstances referenced above where a written acknowledgment must be obtained, there may be other circumstances where a written acknowledgement is reasonably necessary to protect the privacy of individuals and confidentiality of information. In order to cover those circumstances, the minimum content of written acknowledgments set out below also address the collection or disclosure of PI, coded information and de-identified information by a DI Unit (as applicable).

6.5	**Written Acknowledgement re: Collection**
	
	6.5.1 Identify and define the required content of a written acknowledgement applicable to the collection of PI, coded information and/or de-identified information by a DI Unit.
	
	6.5.2 At a minimum, a written acknowledgement applicable to the collection of PI, coded information and/or de-identified information by a DI Unit must include (as applicable):
	
	1. identification of the DI Unit collecting and the person, entity or organization (and the administrative area of the person, entity or organization if the DI Unit is within the same person, entity or organization) disclosing the PI;
	2. a description of the role and responsibilities of the DI Unit under *FIPPA* and a reference to the statutory authority for the collections and uses identified (if applicable);
	3. a general description of the PI, coded information and/or de-identified information to be collected (e.g., education records, Ontario secondary school grades from 2012 – 2014);
	4. the specific time period over which collection will take place (e.g., monthly for two years);
	5. the retention period for the PI, coded information and/or de-identified information;
	6. the intended scope and purpose of DI Unit analysis;
	7. the method for secure retention, transfer and disposal or destruction of the PI, coded information or de-identified information;
	8. if the PI and/or coded information will be linked to other information, the nature and source of any information to which it will be linked, how any linkages will be conducted and why the linkages are required for the identified purposes; and
	9. a statement that:
	    a. in the case of PI and/or coded information, other information, namely de-identified information, will not serve the purpose;
	    b. no more PI and/or coded information will be used than is reasonably necessary to meet the purpose; and
	    c. all persons who have access to the PI and/or coded information will be aware of and agree to comply with the terms and conditions of the written acknowledgement prior to being given access to the PI and/or coded information.

6.6	**Written Acknowledgement re: Disclosure** **6.6.1** Identify and define the required content of a written acknowledgement when a DI Unit is disclosing PI, coded information and/or de-identified information. **6.6.2** At a minimum, a written acknowledgement applicable to the disclosure of PI, coded information and/or de-identified information by a DI Unit must include (as applicable): 1. identification of the DI Unit disclosing and the person, entity or organization (and the administrative area of the person, entity or organization if the DI Unit is within the same person, entity or organization) collecting the PI, coded information and/or de-identified information; 2. a description of the role and responsibilities of the DI Unit under *FIPPA* and a reference to the statutory authority for the disclosures identified (if applicable); 3. a general description of the PI, coded information and/or de-identified information to be disclosed (e.g., education records, Ontario secondary school grades from 2012 – 2014); 4. the source(s) of the PI, coded information and/or de-identified information; 5. the retention period for the PI, coded information and/or de-identified information; 6. the intended scope and purpose of the use of the PI, coded information and/or de-identified information; 7. the method for secure retention, transfer and disposal or destruction of the PI, coded information and/or de-identified information; 8. a statement that: a. in the case of PI and/or coded information, other information(i.e., de-identified information) will not serve the defined purpose; b. no more PI and/or coded information is being collected and will be used than is reasonably necessary to meet the purpose; and c. any de-identified information will not be used, alone or in combination with other information, to identify an individual; 9. that all persons who have access to the PI and/or coded information will be aware of, and agree to comply, with the terms and conditions of the written acknowledgement prior to being given access to the PI or coded information; and 10. whether the PI, coded information and/or de-identified information may be further disclosed and, if so, the written acknowledgement must also: a. address the conditions under which such disclosure may occur; and b. require that any person, entity or organization to which the de-identified information is further disclosed will agree to not use the information, alone or in combination with other information, to identify an individual.
6.7	**6.7.1** Develop and maintain a log of written acknowledgements obtained by the DI Unit.

	6.7.2 At a minimum, the log must include: 1. the name of the person, entity or organization (including the administrative area of the person, entity or organization if the DI Unit is within the same person, entity or organization) from whom the PI, coded information and/or de-identified information was collected or disclosed; 2. the name of individual who gave the written acknowledgement on behalf of the person, entity or organization; 3. whether PI, coded information and/or de-identified information was collected or disclosed; 4. the date the PI, coded information and/or de-identified information was collected or disclosed; and 5. the nature of the PI, coded information and/or de-identified information subject to the written acknowledgement.
6.8	Where a DI Unit is disclosing de-identified information without either a DSA under Requirement 6.1 or a written acknowledgment under Requirement 6.4, the DI Unit must require the person, entity or organization to which de-identified information will be disclosed to confirm in writing that the de-identified information will not be used, alone or in combination with other information, to identify an individual.
6.9	Requirements 6.1, 6.4 and 6.8 do not apply where: 1. a DI Unit is disclosing PI, coded information and/or de-identified information to a member of the same DI Unit who needs access to the PI, coded information and/or de-identified information in the performance of their duties in connection with this Part; 2. the information to be disclosed has been de-identified to the extent necessary for a release to the public; or 3. a person is exercising the right of access under s. 10 of *FIPPA* or an individual is exercising the rights of access and correction under s. 47 of *FIPPA*.

SECURE RETENTION AND TRANSFER

This standard outlines requirements for DI Units to put in place safeguards to ensure a safe, protective technology environment for the secure retention and transfer of PI and coded information. Specifically, DI Units must adopt administrative, technical and physical safeguards to protect the system components and information assets of their DI Environment from attempts to attack, breach or access them in an unauthorized manner.

OVERARCHING REQUIREMENTS

To ensure the secure retention and transfer of PI and coded information under the Part, DI Units must:

7. Ensure that the DI Environment is only accessible to members who require access to it in the performance of their duties under the Part.
8. Implement physical security measures that are reasonable in the circumstances to protect PI and coded information from theft, loss and unauthorized use and disclosure.
9. Implement security measures that are reasonable in the circumstances to protect PI and coded information retained and/or transferred in electronic format from theft, loss and unauthorized use and disclosure.
10. Ensure PI and coded information are only accessed remotely and/or retained on mobile devices in approved circumstances.
11. Conduct threat and risk assessments and keep and review audit logs as reasonable in the circumstances.
12. Develop and implement a process to manage changes to the DI Environment.
13. Ensure that PI and coded information are appropriately backed up in a manner that allows it to be fully recovered, and that the DI Unit has an effective business continuity and disaster recovery plan.
14. Respond to privacy and security breaches in a timely and appropriate manner.

RELEVANT PROVISIONS OF THE PART

The requirements for the secure retention and transfer of PI are outlined in accordance with the following provisions of the Part:

- Security and retention – s. 49.11 (1) (a-c)
  - Security requirements (2)
  - Notice of theft, loss, etc., to individual (3)
  - Notice to Commissioner (4)
- Data standards – s. 49.14 (1) (a) (iv)

SPECIFIC REQUIREMENTS

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

7.1	Identify and define:
	1. business roles that require access to the DI Environment in the performance of their duties;
	2. responsibilities of those business roles;
	  a. at a minimum, business roles must be segregated to ensure that operational functions are separated from security and audit functions, such that no single member has end-to-end control over a process;
	  i. where duties cannot be segregated across multiple distinct members due to lack of available human resources (e.g., in smaller DI Units), other appropriate controls such as monitoring of activities and management supervision must be enhanced to achieve the same effect;
	3. the access needs for each business role to the DI Environment (including parts thereof);
	4. the business role(s) assigned to each member;
	5. the minimum level of privileges required for accessing the DI Environment;
	6. the requirements and conditions that must be satisfied to permit access to the DI Environment, including all requirements in the Part, the Data Standards, the Practices and Procedures, other applicable provisions of *FIPPA* and its regulations, and agreements and acknowledgements made pursuant to them;
	7. the conditions and restrictions imposed on each business role, such as read, create, update or delete limitations, and the circumstances in which the conditions and restrictions will be imposed;
	8. the circumstances in which access will be approved, suspended, revoked or otherwise terminated; and
	9. the purposes for which members are permitted and not permitted to use the DI Environment which, at a minimum, must only permit the DI Environment to be used for DI Unit business under the Part and other approved purposes.

7.2	Ensure members only access the DI Environment where: 1. it is authorized for defined purposes and circumstances and all conditions, requirements and restrictions have been satisfied; 2. the identified purpose for the access to PI and/or coded information cannot be accomplished without the PI and/or coded information; 3. no more PI and/or coded information will be accessed than is reasonably necessary to meet the identified purpose; 4. reasonable steps in the circumstances have been taken to ensure access to the DI Environment is authorized, including: a. only assigning one member to each user ID or access account (i.e. no sharing of accounts between members);

	b. establishing password/passphrase strength, protection, use, confidentiality and change requirements; c. establishing a process for handling repeated failed access attempts, including the number of failed attempts that will result in a denial of access; d. establishing a process for handling idle sessions, including the length of time idle that will require re-authentication; e. establishing requirements for the use of multi-factor authentication; f. periodically reviewing and enhancing the segregation of duties among business roles, particularly as they relate to security, database administration, de-identification, linkage and the collection, use and disclosure of PI and/or coded information; and g. immediately revoking access where a member's employment, contractual or other relationship with the DI Unit has ended, or a review determines that the member's access rights to the DI Environment or any part thereof is no longer required.
7.3	**7.3.1** Develop and maintain a log of members that have been granted approval to access the DI Environment. **7.3.2** At a minimum, the log must identify: 1. the name of each member; 2. the business role assigned to the member; 3. the name of the member who approved the access; 4. the date that access was granted; and 5. the termination date or the date of the next review of access. **7.3.3** The log must be internally reviewed annually. **Note:** This may be a standalone log or may be combined the log of members with physical access to the DI Unit under Requirement 8.3, and/or the log of members approved to remotely access PI and coded information or retain PI and coded information on mobile devices under Requirement 10.3.
7.4	**7.4.1** Require DI Unit members to sign a confidentiality agreement at the commencement of their employment, contractual or other relationship with the DI Unit and on an annual basis thereafter. **7.4.2** Members must comply with the terms of the confidentiality agreement.

7.5	Ensure that confidentiality agreements executed by members contain appropriate provisions, including, at a minimum: 1. the status of the DI Unit under *FIPPA* and the duties and responsibilities arising from this status, including the definitions of PI, coded information and de-identification; 2. that individuals executing the confidentiality agreement are members of the DI Unit and outline the responsibilities associated with this status; 3. a requirement that members comply with the Part, its regulations, the Data Standards, the Practices and Procedures developed and implemented by the DI Unit, other applicable provisions of *FIPPA* and its regulations, and agreements and acknowledgements made pursuant to them; 4. an acknowledgement that members have read, understood and agree to comply with the terms of the confidentiality agreement; 5. the purposes for which members are permitted to collect, use and disclose PI, coded information and/or de-identified information and any limitations, conditions and restrictions; 6. a prohibition on members collecting, using and disclosing PI, coded information and/or de-identified information, except as permitted in the confidentiality agreement or, in the case of disclosure, as required by law; 7. a prohibition on members collecting, using or disclosing PI and/or coded information if other information will serve the purpose, and from collecting, using or disclosing more PI and/or coded information than is reasonably necessary for the purpose; 8. a requirement that members securely return all property of the DI Unit including PI, coded information and de-identified information, and all physical access mechanisms (such as identification cards, access cards and keys), on or before the date of termination of the employment, contractual or other relationship with the DI Unit or where a review determines the property or physical access mechanisms are no longer required for the member's responsibilities for the DI Unit; 9. a requirement that members notify the DI Unit at the first reasonable opportunity of an actual or suspected privacy or security breach; 10. that compliance with the confidentiality agreement will be internally reviewed and address the manner in which compliance will be reviewed; 11. appropriate sanctions for privacy and security breaches committed by the member, including potential dismissal; 12. members' obligations to facilitate the exercise of a right of access under s. 10 of *FIPPA* and the rights of access and correction under s. 47 of *FIPPA*; and 13. a prohibition on members using de-identified information, alone or in combination with other information, to identify an individual.

7.6	Only permit members to access the DI Environment after they have executed the required confidentiality agreement at the commencement of their employment, contractual or other relationship with the DI Unit.
7.7	**7.7.1** Develop and maintain a log of executed confidentiality agreements within the DI Unit. **7.7.2** At minimum, the log must include: 1. the name of each member; 2. the dates of commencement and termination of their employment, contractual or other relationship with the DI Unit; and 3. the dates that the confidentiality agreements were executed.
7.8	**7.8.1** A DI Unit that enters into any arrangement with a person, entity or organization who supplies services related to the collection, linkage, use, disclosure, de-identification, retention, transfer, disposal or destruction of PI, coded information or de-identified information, and who is not a member of the DI Unit, must ensure that it executes a written agreement with such person, entity or organization. **7.8.2** At a minimum, the written agreement must contain the restrictions identified in this requirement: 1. the person, entity or organization must not use any PI, coded information or de-identified information to which it has access in the course of providing the services to the DI Unit except for the purpose of providing the services and only to the extent necessary for such purpose; 2. the person, entity or organization must not disclose any PI, coded information or de-identified information to which it has access in the course of providing the services to the DI Unit; 3. the person, entity or organization must comply with all requirements in the Part, the Data Standards, the Practices and Procedures, other applicable provisions of *FIPPA* or its regulations, or agreements or acknowledgments made pursuant to them as would be applicable to a member of the DI Unit; and 4. the person, entity or organization must not permit its employees or any person acting on its behalf to be able to have access to the PI, coded information or de-identified information unless the employee or person acting on its behalf agrees in writing to comply with the restrictions that apply to the person, entity or organization who supplies services under this requirement.

Requirement 8: Implement physical security measures that are reasonable in the circumstances to protect PI and coded information from theft, loss and unauthorized use and disclosure.	
8.1	Identify and define the reasonable physical security measures that must be implemented to protect PI and coded information from theft, loss and unauthorized use and disclosure, including: 1. locks, alarms and restricted or monitored access to the premises of the DI Unit and locations within the premises where PI and/or coded information is retained; 2. a process to control access by visitors to the DI Unit, which must include measures to identify, screen and supervise visitors; 3. security measures for workspaces, devices and storage media used when working remotely, and related procedures that need to be followed; 4. physical security measures applicable to the secure retention and transfer of PI, coded information and de-identified information on non-electronic storage media (if any); 5. the specific methods that must be used to retain and transfer PI, coded information and de-identified information on non-electronic storage media (if any); and 6. the conditions, requirements and restrictions applicable to the specific methods, including all requirements in: a. the Part; b. the Data Standards; c. the Practices and Procedures; d. other applicable provisions of *FIPPA* and its regulations; and e. agreements and acknowledgements made pursuant to them.
8.2	Ensure that: 1. only authorized members and visitors access the physical premises of the DI Unit and locations within the premises where PI, coded information and/or de-identified information is retained, and all conditions, requirements and restrictions have been satisfied; 2. any identified weaknesses or vulnerabilities in the DI Unit's physical security measures are resolved in a timely manner based on their level of severity; 3. physical access to the premises of the DI Unit and locations within the premises where PI, coded information and/or de-identified information is retained is immediately revoked where a member's employment, contractual or other relationship with the DI Unit has ended, or a review determines that the member's access rights to the premises or any part thereof is no longer required; 4. members securely return all property of the DI Unit including PI and coded information, and all physical access mechanisms (such as identification cards, access cards and keys), on or before the date of termination of the employment, contractual or other relationship with the DI Unit or where a

	review determines the property or physical access mechanisms are no longer required for the member's responsibilities for the DI Unit; and 5. the retention and transfer of PI, coded information and/or de-identified information on non-electronic storage media (if any) is authorized for defined purposes and circumstances, and all conditions, requirements and restrictions have been satisfied.
8.3	**8.3.1** Develop and maintain a log of members with physical access to the DI Unit. **8.3.2** At a minimum, the log must include: 1. the name(s) of the member(s); 2. the name(s) of the member(s) who approved the access; 3. the date that access was granted; and 4. the termination date of the access, if applicable. **Note:** This may be a standalone log or may be combined with the log of members granted access to the DI Environment under Requirement 7.3, and/or the log of members approved to remotely access PI and coded information or retain PI and coded information on mobile devices under Requirement 10.3.

Requirement 9: Implement security measures that are reasonable in the circumstances to protect PI and coded information retained and/or transferred in electronic format from theft, loss and unauthorized use and disclosure.	
9.1	Identify and define the reasonable security measures that must be implemented to protect PI and coded information from theft, loss and unauthorized use and disclosure, which must include, at a minimum: 1. placing all system components that are part of the DI Environment in an internal network zone, segregated from the remainder of the network; **Note:** Network segregation may be achieved through a combination of technologies such as virtual local area networks (VLANs), firewalls, access control lists, etc., that should be determined specifically for a DI Unit's operations, applications and infrastructure. 2. firewalls to manage and ensure only authorized network traffic is allowed into and out of the DI Environment; 3. mechanisms to identify where and when PI and coded information is at risk of threats and vulnerabilities, and how the information would be affected by these threats and vulnerabilities; 4. vulnerability management practices and controls to effectively identify, assess, remediate and mitigate any security weaknesses in the DI Environment; a. penetration testing must be conducted at least annually and after any significant changes to the DI Environment; b. vulnerability scanning must be conducted at least quarterly and after any significant changes to the DI Environment;

	5. controls to effectively monitor and detect any attempts to gain unauthorized access to the DI Environment, including a process for the deployment of anti-malware controls; 6. authenticated connections, strong cryptography and secure protocols to transfer information; and 7. the specific methods that must be used to securely retain and transfer PI and coded information, and the conditions, restrictions and requirements applicable to the specific methods, including all requirements in: a. the Part; b. the Data Standards; c. the Practices and Procedures; d. other applicable provisions of *FIPPA* and its regulations; and e. agreements and acknowledgements made pursuant to them.
9.2	Ensure that: 1. the retention and transfer of PI and/or coded information is authorized for defined purposes and circumstances, and all conditions, requirements and restrictions have been satisfied; and 2. any identified weaknesses or vulnerabilities in the DI Unit's security measures are resolved in a timely manner based on their level of risk.

Requirement 10: Ensure PI and coded information are only accessed remotely and/or retained on mobile devices in approved circumstances.	
10.1	Identify and define: 1. the requirements or conditions that must be satisfied to permit PI and coded information to be accessed remotely and/or on mobile devices, including all requirements in the Part, the Data Standards, the Practices and Procedures, other applicable provisions of *FIPPA* and its regulations, and agreements and acknowledgements made pursuant to them; 2. any restrictions that may apply to remote access to, and/or retention of, PI and coded information on mobile devices; 3. the methods for secure remote access and/or secure retention on mobile devices and related procedures that need to be followed; 4. the types of devices that may be used for access and/or retention; and 5. the purposes for which PI and coded information may be remotely accessed and/or retained on a mobile device.
10.2	Ensure members remotely access PI and/or coded information, and/or retain PI and/or coded information, on a mobile device only where: 1. it is authorized for defined purposes and circumstances, and all conditions, requirements and restrictions have been satisfied;

	2. remote access and/or retention on a mobile device of PI and/or coded information is provided only to those members who need remote access and/or mobile retention to carry out authorized functions; 3. PI and coded information are only remotely accessed and/or retained on authorized devices (e.g., enterprise supplied and managed); 4. the identified purpose for the access to, and/or retention of, PI and/or coded information cannot reasonably be accomplished without access to, and/or retention of, the PI and/or coded information; 5. no more PI and/or coded information will be accessed or retained than is reasonably necessary to meet the identified purpose; 6. in the case of remote access to PI and/or coded information, members are prohibited from copying, moving or saving PI and/or coded information onto storage media from remote connections; 7. in the case of retention of PI and/or coded information on a mobile device, PI and/or coded information retained must be strongly encrypted with a strong password/passphrase, and the device must have an automatic lock and screensaver (if applicable) enabled after a period of inactivity; and 8. reasonable steps in the circumstances have been taken to ensure all remote access to, and/or retention on mobile devices of, PI and/or coded information is authorized, including: a. immediately revoking remote access rights where a member's employment, contractual or other relationship with the DI Unit has ended, or a review determines that the member's remote access rights to the DI Environment or any part thereof is no longer required.
10.3	**10.3.1** Develop and maintain a log of all members within the DI Unit approved to remotely access PI and coded information and/or retain PI and coded information on mobile devices. **10.3.2** At a minimum, the log must include: 1. the name and contact information of the member; 2. whether the member is approved to remotely access, and/or retain on a mobile device, PI and/or coded information; 3. name of the member who approved the remote access and/or retention on mobile device; 4. a description of the program applications and the information that the user is authorized to access remotely and/or retain on a mobile device; 5. the purpose for which access and/or retention was approved; and 6. the date of approval. **Note:** This may be a standalone log or may be combined with the log of members granted access to the DI Environment under Requirement 7.3, and/or the log of members with physical access to the DI Unit under Requirement 8.3.

Requirement 11: Conduct threat and risk assessments and keep and review audit logs as reasonable in the circumstances.	
11.1	Identify and define the circumstances or events where a threat and risk assessment (TRA) is required; 1. at a minimum, a TRA must be conducted before the DI Unit becomes operational and upon any significant changes to the DI Environment; and 2. at least annually, the most recent TRA(s) must be reviewed and updated, as necessary, to address any applicable changes to the threat landscape, emerging trends and new technologies.
11.2	**11.2.1** Identify and define the required content of a TRA. **11.2.2** At a minimum, a TRA must include: 1. a description of all in-scope information assets; 2. identification of risks, including the potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability; and 3. recommended protective measures, including enhancements or changes to the DI Unit's administrative, technical and physical safeguards to eliminate or reduce the threats and vulnerabilities identified, based on severity of risk.
11.3	Ensure that recommendations resulting from TRAs are prioritized and addressed to eliminate or reduce identified threats and vulnerabilities in a timely manner based on severity of risk.
11.4	**11.4.1** Develop and maintain a log of TRAs. **11.4.2** At a minimum, the log must include: 1. the date(s) that the TRA was completed or updated, or is expected to be completed or updated; 2. the name(s) of the member(s) responsible for completing/updating or ensuring the completion/update of the TRA; 3. the recommendations arising from the TRA; 4. the name(s) of the member(s) responsible for addressing each recommendation; 5. the date that each recommendation was, or is expected to be, addressed; and 6. how each recommendation was, or is expected to be, addressed.
11.5	**11.5.1** Identify and define the information that must be logged to capture and enable detection and monitoring of privacy and security breaches. **11.5.2** At a minimum, the DI Unit must develop and maintain a log that includes: 1. user IDs or member access accounts; 2. date and time of each access to the DI Environment; 3. identity of device(s);

	4. successful and failed attempts to access the DI Environment, including all instances where PI and/or coded information is viewed, handled or otherwise dealt with; 5. files accessed, including a reference to the PI and/or coded information viewed, handled or otherwise dealt with to determine which individual's PI and/or coded information was viewed, handled or otherwise dealt with, if applicable; 6. a description of the type of information viewed, handled or otherwise dealt with; 7. the name of the member who viewed, handled or otherwise dealt with the information; 8. changes to system configurations; 9. use of system utilities; and 10. notifications from security control systems. **Note:** The information maintained within the log under this requirement must be adequately protected in order to prevent the risk of inappropriately leaking sensitive information.

Requirement 12: Develop and implement a process to manage changes to the DI Environment.	
12.1	**12.1.1** Identify and define a secure process to manage vendor-supplied and requested changes to the DI Environment. **12.1.2** The process to manage changes to the DI Environment must include, at a minimum, a process for: 1. the regular review, monitoring and routine deployment of vendor-supplied changes (e.g., security patches); 2. requesting changes; 3. determining whether or not the change should be implemented and the criteria to be considered in making this decision; 4. determining the priority of the change, when the change must be implemented, and the criteria to be considered when making these decisions; and 5. testing of changes.
12.2	For each change, develop and maintain documentation that includes, at a minimum: 1. a description of the change; 2. the date the change became available (e.g., in the case of security patches) or was requested; 3. the name(s) of the member(s) requesting the change; 4. the rationale for the change; 5. the priority and impact of the change; 6. the information system, technology, equipment, resource, application or program to which the change relates;

	7. the required approvals for the change; 8. whether the change was approved or denied, the reason for the approval or denial and the name(s) of the member(s) who approved or denied the change; 9. the date, if any, when the change was tested, the member(s) responsible for testing, and whether or not the testing was successful; 10. the name(s) of the member(s) responsible for implementing the change; 11. the time frame for implementation of the change; and 12. the date the change was implemented, if approved.

Requirement 13: Ensure that PI and coded information is backed up in a manner that allows it to be fully recovered, and that the DI Unit has an effective business continuity and disaster recovery plan.	
13.1	Identify and define: 1. the nature and types of back-up storage media maintained by the DI Unit; 2. the frequency with which information is backed-up; 3. the circumstances in which backed-up information is required to be made available; and 4. the processes, including related procedures that need to be followed, for back-up and recovery methods as well as their testing.
13.2	**13.2.1** Identify and define a business continuity and disaster recovery plan in the event of short and long-term business interruptions, and threats to the operating capabilities of the DI Unit, including natural, human, environmental and technical interruptions and threats. **13.2.2** The business continuity and disaster recovery plan must include, at a minimum, a process for: 1. internal notification of the interruption or threat, and any external persons, entities or organizations that must be notified of short and long-term business interruptions and threats to the operating capabilities of the DI Unit, including an up-to-date contact list for notification; 2. assessing the severity of the interruption or threat; 3. determining the circumstances the business continuity and disaster recovery plan will be activated and the process for activation; 4. conducting an initial assessment of the interruption or threat; 5. conducting a detailed damage assessment and assessing the expected effort required to resume, recover and restore infrastructure elements, information systems and services; 6. determining the priority to be utilized in resumption and recovery of each critical application and business function; 7. identification of all critical applications and business functions, hardware and software, software licences, recovery media, equipment, system network diagrams, hardware configurations, software configuration settings,

	configuration settings for database systems and network settings for firewalls, routers, domain name servers, email servers, etc.; and 8. testing, maintaining, assessing and amending the business continuity and disaster recovery plan.
13.3	**13.3.1** Ensure that the back-up and recovery methods, and business continuity and disaster recovery plan, are tested on an annual basis, at a minimum. **13.3.2** Document and address the testing conducted and any findings and recommendations arising from such testing in a timely manner.

Requirement 14: Respond to privacy and security breaches in a timely and appropriate manner.	
14.1	Identify, report internally, contain, provide notification of, investigate and remediate, actual or suspected privacy and security breaches in a prompt and timely manner. Implement escalation procedures as needed.
14.2	Identify and define: 1. the procedures to be followed to identify, report, contain, notify, investigate and remediate actual or suspected privacy or security breaches, including criteria for escalation within the DI Unit; 2. the procedures to be followed when an actual or suspected breach is both a privacy breach and a security breach; 3. the procedures to be followed in determining whether an actual privacy or security breach has occurred; 4. a process for determining when notification to the affected individuals and to the IPC is required; 5. the manner in which notification must be provided (e.g., verbally or in writing) and the information to be communicated to affected individuals and the IPC; a. at a minimum, the information to be communicated must include: i. the scope of the breach; ii. the nature of the information at issue; iii. measures implemented to contain the breach; and iv. further investigation and actions that will be taken; and 6. a process for addressing the recommendations resulting from investigations of privacy or security breaches to eliminate or reduce the risk of future privacy and security breaches.
14.3	Ensure that: 1. members report all actual or suspected privacy and security breaches at the first reasonable opportunity; 2. when investigating a privacy or security breach, all reasonable steps are taken to eliminate and reduce the risk of future privacy and security breaches and

	that, in doing so, the DI Unit considers all relevant factors, including whether it is necessary to: a. review and amend relevant administrative, technical and physical safeguards to enhance compliance; b. review, develop and implement new Practices and Procedures; c. update training for members; and d. test and evaluate remedial actions to determine if they have been implemented correctly, and if Practices and Procedures need to be modified; and 3. the DI Unit evaluates whether the notice to the individuals, the IPC and other relevant parties was effective (e.g., was it done in a timely manner, were the tone and content of the notice appropriate, and was there sufficient support provided to affected individuals?).
14.4	**14.4.1** Develop and maintain a log of privacy and security breaches. **14.4.2** At a minimum, the log must include: 1. the nature and scope of the breach (e.g., how many people are affected, type of PI involved, the extent of containment, etc.); 2. steps taken to manage the breach (e.g., containment and investigation, recommendations made); 3. the name(s) of the member(s) responsible for managing the breach and addressing each recommendation made; 4. plans to notify the individuals affected by the breach, the IPC and other parties, if necessary; 5. the timeline for ongoing management of the breach; and 6. relevant dates (e.g., date of breach (if known), date when breach identified or suspected, date notification provided to relevant parties, date recommendations addressed, etc.).

Guidance:

The Government of Ontario Information and Technology Standards (GO-ITS) are the official publications concerning standards, guidelines, technical reports and preferred practices adopted by the Government of Ontario. If a DI Unit is subject to the GO-ITS, the DI Unit should work with their respective I&IT Cluster and Cyber Security professionals in the development of the relevant Practices and Procedures.

The IPC also publishes guidance documents to promote compliance with Ontario's access and privacy laws. These publications provide detailed guidance on several requirements outlined in this standard and may be used by DI Units for additional support.

SECURE DISPOSAL AND SECURE DESTRUCTION

This standard outlines requirements for DI Units to ensure the secure disposal or destruction of PI, coded information and related storage media. Once securely disposed of or destroyed, PI and coded information is permanently removed from the relevant storage medium such that it cannot be reconstructed or retrieved in reasonably foreseeable circumstances.

OVERARCHING REQUIREMENTS

To ensure the secure disposal or destruction of PI and coded information under the Part, the DI Units must:

15. Dispose of or destroy PI, coded information and the storage media containing the information promptly and in a secure manner.
16. Retain and transfer PI, coded information and the storage media containing the information in a secure manner pending disposal or destruction.
17. Verify that PI, coded information and the storage media containing the information, has been disposed of or destroyed in a secure manner.

RELEVANT PROVISIONS OF THE PART

The requirements for the secure disposal and destruction of PI are outlined in accordance with the following provisions of the Part:

- Linking and de-identification – s. 49.6 (1) 4.
- Security and retention – s. 49.11 (1) (a), (c), (d)
  - Security requirements – (2)

SPECIFIC REQUIREMENTS

Requirement 15: Dispose of or destroy PI, coded information and the storage media containing the information promptly and in a secure manner.	
15.1	Identify and define the method(s) for secure disposal and secure destruction of PI, coded information and related storage media that will be used by the DI Unit. In making this determination, DI Units must consider the type of information and storage media (e.g., electronic and paper-based media).
15.2	**15.2.1** Identify and define the conditions under which PI, coded information and the storage media containing the information must be securely disposed of or destroyed. **15.2.2** The conditions must include, at a minimum: 1. when media are repurposed;

	2. when media reach end of life; or 3. when media are no longer in the custody or control of the DI Unit.

Requirement 16: Retain and transfer PI, coded information and the storage media containing the information in a secure manner pending disposal or destruction.	
16.1	Identify and define: 1. a physical area and clearly marked and locked container(s) for the secure retention of PI, coded information and related storage media pending their secure disposal or destruction; and 2. the procedure to be followed in securely transferring the PI, coded information and related storage media outside the DI Unit for secure disposal or destruction (if applicable).
16.2	Ensure that: 1. PI, 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 all requirements in: a. the Part; b. the Data Standards; c. the Practices and Procedures; d. other applicable provisions of *FIPPA* and its regulations; and e. agreements and acknowledgements made pursuant to them; 2. PI, coded information and related storage media intended for secure disposal or destruction are physically segregated from other information; 3. PI, coded information and related storage media intended for secure disposal or destruction are retained in a clearly marked and locked container(s) pending their secure disposal or destruction; and 4. in relation to each transfer of storage media outside the DI Unit for secure disposal or destruction, the DI Unit: a. documents the date, time and mode of transfer; b. maintains a repository of written confirmations evidencing receipt of the storage media; and c. maintains a detailed inventory of storage media related to each transfer.

Requirement 17: Verify that PI, coded information and the storage media containing the information, has been disposed of or destroyed in a secure manner.	
17.1	**17.1.1** Identify and define the required content of certificates of secure disposal or destruction. **17.1.2** At a minimum, certificates of secure disposal or destruction must include: 1. The DI Unit from which the storage media came;

	2. the manufacturer, model, or serial number (if electronic media); 3. the media type (paper-based or electronic); 4. the disposal or destruction method used; 5. the name(s) of the member(s) requesting the secure disposal or destruction; and 6. the name, position, address, contact and signature of the individual responsible for the disposition or destruction and the date of the disposition or destruction.
17.2	Identify and define: 1. the timeframe within which certificates of secure disposal or destruction must be obtained; and 2. the time period for which, and location where, certificates of secure disposal or destruction will be retained.
17.3	Ensure that: 1. a certificate of secure disposal or destruction is obtained for each storage media securely disposed of or destroyed, confirming the secure disposal or destruction of the PI, coded information and related storage media; 2. the DI Unit develops and maintains a log which, at a minimum, includes: a. the dates that PI, coded information and related storage media are transferred for secure disposal or destruction; and b. the dates that certificates of secure disposal or destruction are received; and 3. the identified secure disposal or destruction method(s) are periodically reviewed by the DI Unit to ensure they are effective.

Guidance:

Ontario Regulation 459: Disposal of Personal Information under *FIPPA* outlines requirements to protect the security and confidentiality of PI that is to be destroyed. If a DI Unit is subject to the regulation, the DI Unit should work with their respective records and information management and privacy professionals in the development of the relevant Practices and Procedures.

The IPC also publishes guidance documents to promote compliance with Ontario's access and privacy laws. These publications provide detailed guidance on several requirements outlined in this standard and may be used by DI Units for additional support.

RETENTION PERIOD

This standard outlines requirements for DI Units to retain PI and coded information for specified periods. A retention period is the overall length of time that information must be kept before it can and, in some cases, must be deleted. Under the Part, DI Units must retain PI for a period as set out in the Data Standards.

OVERARCHING REQUIREMENTS

To ensure that PI and coded information under the Part are retained for the specified periods in accordance with the Part, DI Units must:

18. Implement retention requirements for PI and coded information.

RELEVANT PROVISIONS OF THE PART

The requirements for the retention of PI are outlined in accordance with the following provisions of the Part:

- Linking and de-identification – s. 49.6 (1) 4.
- Same – s. 49.6 (2)
- Security and retention – s. 49.11 (1) (c)
- Data Standards – s. 49.14 (1) (a) (iv)

SPECIFIC REQUIREMENTS

Requirement 18: Implement retention requirements for PI and coded information.	
18.1	**18.1.1** Identify and define a process for determining the retention period for PI and coded information. 1. At a minimum, the process must consider the following factors: a. business or operational needs; b. legal and regulatory requirements; c. community and public expectations; and d. the privacy interests of individuals. **18.1.2** Identify and define a retention period for each class of PI. 1. At a minimum, PI in the record created by the DI Unit containing the minimal amount of PI necessary for the purpose of linking under Requirement 20.3 must be retained long enough to facilitate individuals exercising their rights of access and correction under s. 47 of *FIPPA*.

	18.1.3 Identify and define a retention period for coded information. 1. At a minimum, 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. **Note:** The purpose of the minimum retention period for coded information is to facilitate individuals exercising their rights of access and correction under s. 47 of *FIPPA*. In order for DI Units to identify the individual to whom coded information relates, DI Units must retain the minimal identifiers that relate to the specific subset of coded data. These minimal identifiers are retained in the record identified under Requirement 20.3.
18.2	**18.2.1** Retain original non-coded PI for a maximum period of 180 calendar days after its transformation into coded information to enable accurate linking, consistent with Requirement 20. **18.2.2** If the collection of a series of PI is necessary for coding to enable accurate linking, retain original non-coded PI for a maximum period of 180 calendar days after the last PI within the series is transformed into coded information. The time period between the first and last collection in a series of PI must not exceed one year. **18.2.3** The maximum retention periods may be extended where: 1. necessary as a result of exceptional or unforeseen circumstances; 2. the extension is for a defined length of time that is the minimum necessary for the original non-coded PI to be transformed into coded information to enable accurate linking; 3. notification detailing the reason for, and length of, the requested extension is provided in writing to the Chief Archivist of Ontario and the IPC at least 30 calendar days prior to the elapsing of the original retention period; and 4. the IPC approves of the extension in writing. **Note:** For greater clarity, these maximum retention periods do not apply to the record created by the DI Unit containing the minimal amount of PI necessary for the purpose of linking under Requirement 20.3.
18.3	Ensure that PI and coded information is deleted at the earlier of: 1. the expiry of maximum retention period(s) identified and defined by the DI Unit under Requirement 18.1; 2. the expiry of the maximum retention period(s) established under Requirement 18.2, as applicable; or 3. its retention is no longer necessary to fulfil the purpose for which it was collected or created, following the expiry of the minimum retention periods established under Requirement 18.1.

	Note: After the deletion of PI or coded information under this requirement, DI Units are not permitted to reconstruct or otherwise regain access to the deleted information.
18.4	For greater clarity, the retention periods in Requirements 18.1 – 18.3: 1. are exemptions to the retention period set out in s. 49.6 (1) 4 of the Part; and 2. specify the retention period for the purposes of s. 49.11 (1) (c) of the Part. **Note:** This requirement clarifies that the retention periods contained in this standard supersede the minimum and maximum retention periods specified in the above cited provisions of the Part. After the deletion of information in accordance with the retention requirements in this standard, PI, coded information and the storage media containing the information must further be disposed of or destroyed in a secure manner under Requirements 15, 16, and 17.
18.5	**18.5.1** Develop and maintain a log of the PI and coded information that has been deleted in accordance with its defined retention period. **18.5.2** At a minimum, the log must include: 1. a description of the PI or coded information; 2. a description of the applicable retention period; 3. the date the PI was collected and the date the PI was transformed into coded information (as applicable); and 4. the date the PI or coded information was deleted and the name(s) of the member(s) who deleted the PI or coded information. **Note:** This may be a standalone log or may be combined with the inventory of PI and coded information within the DI Unit under Requirement 5.4.

Guidance:

For applicable DI Units, they should ensure that retention and disposition of records is managed in accordance with the *Archives and Recordkeeping Act, 2006* (*ARA*). The DI Unit should work with their records and information management and privacy professionals to develop a records schedule for records containing PI, and other records created, received and maintained by the DI Unit for the purposes and requirements under this standard.

A records schedule describes the records managed by the DI Unit, specifies authorized retention periods, identifies records of enduring value, and specifies final disposition for records at the end of their retention period – either to be destroyed, transferred to the Archives of Ontario, or when necessary and feasible, to continue being retained by the DI Unit on behalf of the Archives. In accordance with the *ARA*, a records schedule must be approved by the Archivist of Ontario. However, a records schedule under the *ARA* must not require that records be kept beyond the applicable maximum retention periods set out in these Data Standards. Refer to Records Schedule Requirements for more detailed guidance.

DE-IDENTIFICATION AND LINKING

This standard outlines requirements for DI Units to implement an accurate, privacy-protective de-identification and linking process to ensure that the PI collected under the Part can be transformed and used for analysis, as permitted under the Part. It also requires that the de-identification process, in particular the transformation of PI into coded information, be undertaken as soon as reasonably possible in the circumstances.

OVERARCHING REQUIREMENTS

To ensure that PI collected under the Part is de-identified and linked in an accurate and privacy protective manner under the Part, DI Units must:

19. Segregate duties in relation to coding and linking.
20. As soon as reasonably possible in the circumstances, transform PI collected by the DI Unit into coded information.
21. Link coded information to other coded information, where necessary for analysis.
22. De-identify coded information prior to analysis.

RELEVANT PROVISIONS OF THE PART

The requirements for De-identification and Linkage are outlined in accordance with the following provisions of the Part:

- Meaning of de-identification – s. 49.1 (2)
- General rules re personal information – s. 49.3 (1)
  - Extent of information – (2)
- Linking and de-identification – s. 49.6 (1) (1-3)
  - Same (2)
- Limits on use of personal information – s. 49.7 (1)
- Limits on use of de-identified information – s. 49.8

SPECIFIC REQUIREMENTS

Requirement 19: Segregate duties in relation to coding and linking.	
19.1	Identify and define distinct roles for the coding and linking processes within the DI Unit. **Note:** The purpose of separating roles and duties in relation to coding and linking is to facilitate the protection of privacy by preventing a single member, at any given time,

	from having too high a concentration of access to PI. It is also consistent with the data minimization requirement under s. 49.3(2) of the Part.
19.2	Ensure the separation of these roles in the coding and linking processes using administrative, technical and physical safeguards that are reasonable in the circumstances. **Note:** Whenever duties cannot be segregated across multiple distinct members due to lack of available human resources (e.g., as the case may be in smaller DI Units), other appropriate safeguards such as monitoring of activities, audit trails and management supervision must be enhanced to achieve the same effect.

Requirement 20: As soon as reasonably possible in the circumstances, transform PI collected by the DI Unit into coded information.	
20.1	Identify and define the minimum common direct identifiers and indirect identifiers necessary to enable linking.
20.2	Ensure that direct identifiers are removed from PI and replaced with a secure internal code unique to the individual. **Note:** The outcome of this process is the creation of coded information. This is the start of the de-identification process to enable linking per s. 49.6(1) of the Part. Further, prior to analysis, the de-identification methodology under Requirement 22 must be applied to the coded information.
20.3	Develop and maintain an accurate and up-to-date mapping between each assigned internal code and the minimum common direct and indirect identifiers. **Note:** Direct identifiers removed from PI under Requirement 20.2 may be retained by the DI Unit for use in assigning internal codes and linking, as necessary. Any such identifiers must be segregated from coded information (e.g., in a database of identifiers used for mapping between each assigned internal code and the minimum common identifiers). This mapping between assigned internal codes and the minimum common identifiers will also facilitate DI Units responding to individuals exercising the rights of access and correction under s. 47 of *FIPPA*. The transformation of the PI in this requirement results in: the creation of coded information; the mapping between identifiers referred to above; and no other PI.

Requirement 21: Link coded information to other coded information, where necessary for analysis.	
21.1	Identify and define: 1. the methods that must be used to link coded information; 2. the risks to the accuracy of such linkages; and 3. how such risks to accuracy will be mitigated.
21.2	**21.2.1** Ensure: 1. that coded information is linked only in authorized circumstances and where all conditions, requirements and restrictions have been satisfied, including all requirements in the Part, the Data Standards, the Practices and Procedures, other applicable provisions of *FIPPA* and its regulations, and agreements and acknowledgements made pursuant to them; and 2. the accuracy of linkages of coded information using testing methods and procedures that are reasonable in the circumstances. **21.2.2** Periodically internally review linkages made to ensure they are accurate.

Requirement 22: De-identify coded information prior to analysis.	
22.1	**22.1.1** Identify and define the criteria to be used in calculating the risk of re-identification that, at a minimum, must address: 1. the data release type; 2. the identifiers that must be removed, masked or otherwise transformed; 3. the types of re-identification attacks to consider; and 4. the types of background information available to the data recipients. **22.1.2** Identify and define a risk-based de-identification methodology. **22.1.3** At a minimum, the methodology must make use of appropriate techniques, safeguards, metrics and procedures and include the following steps: 1. classify variables; 2. determine an acceptable re-identification risk threshold; 3. measure the data and context risks; 4. calculate the overall risk of re-identification; and 5. ensure the overall risk is less than or equal to the re-identification risk threshold.
22.2	Ensure that the de-identification methodology is applied to coded information prior to analysis so that:

	1. it is not reasonably foreseeable, in the circumstances, that an individual could be identified; and 2. the risk of re-identification is very low. **Note:** The two bullets above describe the same outcome but from different perspectives. The first tracks the statutory definition of what is to be achieved by de-identification, whereas the second provides a technical account more amenable to being quantified.
22.3	**22.3.1** Develop and maintain documentation of the application of the de-identification methodology to any coded information. **22.3.2** At a minimum, the documentation must include: 1. the data recipient(s) and release type; 2. a description of the coded information that was de-identified, including the specific data elements or fields; 3. the steps taken to de-identify the information; and 4. the analyses used to determine, measure and calculate the amount and kinds of de-identification techniques, safeguards, metrics and procedures that were applied.

PUBLIC NOTICE AND ANNUAL REPORTING

This standard outlines the minimum requirements for DI Units to ensure openness and transparency with respect to their information practices. Under the Part, DI Units must make information about how they collect, use and disclose PI publicly available. In particular, DI Units must create and publish documentation related to the notice of collection, use reporting, annual reporting and privacy complaints and inquiries.

OVERARCHING REQUIREMENTS

To ensure that the notice of collection, use reporting, annual reporting and privacy complaint and inquiries requirements under the Part are met, DI Units must:

23. Publish a notice of collection that relates to the PI to be collected under the Part.
24. Publish a complete list of notices of collection published by the DI Unit.
25. Publish a report on the use of PI to link and de-identify, and to conduct an audit.
26. Publish an annual report that relates to the collection, use, de-identification, linkage and disclosure of PI collected under the Part.
27. Respond to and address privacy complaints and inquiries from the public in a timely manner.

NOTICE OF COLLECTION

RELEVANT PROVISIONS OF THE PART

The requirements for the notice of collection are outlined in accordance with the following provisions of the Part:

- Notice of Collection – s. 49.10

SPECIFIC REQUIREMENTS FOR NOTICE OF COLLECTION

Requirement 23: Publish a notice of collection that relates to the PI to be collected under the Part.	
23.1	Publish a notice that includes the information set out in Requirements 23.2 to 23.8 prior to each new collection of PI. **Note:** A new collection is when PI is collected from a source for the first time. An ongoing collection is when the same data elements of PI are collected from the same source on a defined basis (e.g., the same data elements of PI are collected every month for two years).

	If a collection of PI is part of an ongoing collection of the same PI from the same source, a separate notice of collection is not required each time the same data elements of PI are collected. For example, if PI is to be collected every month for two years, the notice of collection published prior to the first month's collection should define the frequency and time period for the collection. A new notice of collection is not required when an ongoing collection continues in subsequent months.
23.2	Cite the legal authority that permits the collection by referring to the specific section(s) under the Part that authorizes the collection and other relevant legislation. For example: Personal information is being collected indirectly to facilitate the evaluation of programs and services funded by the Ministry of (X) in accordance with s. 49.2 of *FIPPA* and subject to the conditions set out under s. 49.4 of *FIPPA*.
23.3	Describe the types of PI to be collected. The description must include details on the scope of the PI collected including sector, date range and demographic/population characteristics. For example: Transportation records, including motor vehicle collisions and injury and death claims, between March 2019 and March 2020 of licenced drivers in Ontario. The collection will take place quarterly over the course of the one-year period defined.
23.4	State the source(s) and dataset(s) from where PI is to be collected. For example, expanding on the example from Requirement 23.3: • Motor Vehicle Collisions on Provincial Highways (Ministry of Transportation) • Fatal and Injury Collisions by Initial Impact Type (Ministry of Transportation) • Motor Vehicle Collisions on Provincial Highways (Municipalities - Collision Reporting Centres) • Auto Insurance Claims for Injury (Financial Services Regulatory Authority) • Auto Insurance Claims for Deaths (Financial Services Regulatory Authority)
23.5	Describe the purpose(s) for which the PI is to be collected and used, including the general nature of the linkages that may be made. The purpose for collection must be in accordance with the permitted purposes set out in s. 49.2 of *FIPPA*. The use of PI must include its de-identification and may include the linkage of PI, as well as the conducting of audits, as applicable, as set out in s. 49.7(1). For example: The DI Unit is collecting PI for the purpose of planning for the delivery of programs and services. The PI collected will be de-identified and linked to better understand road user safety and vehicle insurance requirements under provincial jurisdiction. Variables from motor vehicle collisions, deaths and insurance claims will be linked.

23.6	Identify the purposes for which PI may be disclosed and any known purposes (at the time of collection) for which the PI will be disclosed. For example: PI will be disclosed to members of the DI Unit within the Ministry of (X) who needs access to the information in the performance of their duties in connection with the Part. The PI will also be disclosed to the inter-ministerial DI Unit within the Ministry of (Y). The DI Unit within the Ministry of (X) may further disclose PI it collects: • to another inter-ministerial DI Unit and/or an extra-ministerial DI Unit; • as required by law; • to an institution or law enforcement agency in Canada in relation to an investigation; • for the purpose of a proceeding before a court or tribunal; • to the Information and Privacy Commissioner of Ontario; or • for a research purpose.
23.7	Include the title, email, mailing address and telephone number of a DI Unit member(s) who can answer any questions about the collection, use and disclosure of PI under the Part.
23.8	Include an email, mailing address and telephone number for the IPC, with a description of the IPC's functions under s. 49.12.
23.9	**23.9.1** Publish the notice in English and French on a Government of Ontario website or, in the case of an extra-ministerial DI Unit, the person's or entity's website. **23.9.2** Ensure that the notice of collection uses clear and easy to understand language.
23.10	For ongoing collections of PI, update the published notice of collection, as soon as reasonably possible to ensure that it continues to accurately describe the collection.

Requirement 24: Publish a complete list of notices of collection published by the DI Unit.	
24.1	**24.1.1** Develop and maintain a list of notices of collection published by the DI Unit. **24.1.2** At a minimum, the list must include: 1. the date of initial publication of each notice of collection; 2. a description of the projects undertaken by the DI Unit using the information referenced in each notice of collection (e.g., improving health outcomes through attachment to a primary care provider);

	3. the sources of PI referenced in each notice of collection; 4. the date each notice of collection was last updated; and 5. a link to each notice of collection.
24.2	**24.2.1** Publish the list in English and French on a Government of Ontario website or, in the case of an extra-ministerial DI Unit, the person's or entity's website. **24.2.2** Ensure that the list uses clear and easy to understand language.

REPORTING ON USE

RELEVANT PROVISIONS OF THE PART

The requirements for reporting on use are outlined in accordance with the following provisions of the Part:

- Limits on use of personal information – s. 49.7 (1)
  - Extra-ministerial data integration unit (1.1)
  - Reporting on Use (2)
- Data standards – s. 49.14 (1) (a) (iii)

SPECIFIC REQUIREMENTS FOR REPORTING ON USE

Requirement 25: Publish a report on the use of PI to link and de-identify, and to conduct an audit.	
25.1	At minimum, the report must include: 1. the list of the DI Unit's PI and coded information developed and maintained under Requirement 25.3; and 2. descriptions of audits undertaken under s.49.7(1)(b). **Note:** DI Units may combine this report on use with the annual report outlined in Requirement 26 (below).
25.2	**25.2.1** Publish the report on uses of PI at least annually in English and French on a Government of Ontario website or, in the case of an extra-ministerial DI Unit, the person's or entity's website. **25.2.2** Ensure that the report uses clear and easy to understand language.
25.3	**25.3.1** Develop and maintain a list of datasets retained by the DI Unit of: 1. identifiers retained for use in assigning internal identifiers and linking under Requirement 20.3; and

	2. coded information. **25.3.2** At a minimum, the list must include: 1. name of the dataset; 2. description of the dataset; 3. date range of the dataset; 4. the specific data elements or fields contained in the dataset; 5. source(s) of information in the dataset; and 6. the projects undertaken by the DI Unit using the dataset. **Note:** The datasets of original non-coded PI collected by the DI Unit do not need to be included on this list as they will be reflected in the Notices of Collection, but the coded information derived from these datasets must be included.

ANNUAL REPORT

RELEVANT PROVISIONS OF THE PART

The requirements for the Annual Report are outlined in accordance with the following provisions of the Part:

- Annual Report – s. 49.13 (1)
  - Same (1.1)
  - Contents of Report (2)

SPECIFIC REQUIREMENTS FOR ANNUAL REPORT

Requirement 26: Publish an annual report that relates to the collection, use, de-identification, linkage and disclosure of PI collected under the Part.	
26.1	Ensure that an annual report is published on or before April 1 in the year following the report coverage period that includes the information set out in Requirements 26.2 to 26.6. The annual report must cover the period from January 1 to December 31.
26.2	Describe the types of PI that were collected, used and disclosed.
26.3	Describe the purpose(s) for which the PI was collected, used and disclosed including additional contextual details, where possible.
26.4	Describe the nature of the linkages of coded information that have been made, including with reference to the list developed and maintained under Requirement 25.3.

26.5	Include a summary of how de-identified information was used and disclosed, including with reference to the projects undertaken by the DI Unit included in the list developed and maintained under Requirement 25.3.
26.6	Describe how the DI Unit's Practices and Procedures meet the requirements in the Part, and enable the privacy protective and secure collection, use, de-identification, linkage, disclosure, retention, transfer and disposal/destruction of PI.
26.7	**26.7.1** Publish the annual report in English and French on a Government of Ontario website or, in the case of an extra-ministerial DI Unit, the person's or entity's website. **26.7.2** Ensure that the annual report uses clear and easy to understand language.

PRIVACY COMPLAINTS AND INQUIRIES

RELEVANT PROVISIONS OF THE PART

The requirements for privacy complaints and inquiries are outlined in accordance with the following provisions of *FIPPA* Part III.1:

- Security and retention – s. 49.11 (1)
  - Security requirements (2)
  - Notice to Commissioner (4)

SPECIFIC REQUIREMENTS FOR PRIVACY COMPLAINTS AND INQUIRIES

Requirement 27: Respond to and address privacy complaints and inquiries from the public in a timely manner.	
27.1	**27.1.1** Identify and define how a member of the public may make a privacy complaint and inquiry related to the activities of the DI Unit. **27.1.2** At a minimum, the process must include: 1. how a complaint or inquiry may be made (e.g., via email, mail, over telephone, etc.); 2. the information requested from the individual making the complaint or inquiry; and 3. the title and contact information of the individual to whom a complaint or inquiry may be directed.
27.2	**27.2.1** 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.

	27.2.2 At minimum, the procedures must include: 1. the information to be provided to persons exercising their right of access under s. 10 of *FIPPA* and/or individuals exercising their rights of access and correction under s. 47 of *FIPPA*, including the information on where and to whom requests may be made; 2. that where a complaint or inquiry relates to an actual or suspected privacy or security breach, it will also be addressed in accordance with the DI Unit's breach management protocol under Requirement 14; 3. that individuals making a complaint or inquiry must receive a response to the complaint or inquiry advising them of what action(s), if any, will be or have been taken to resolve the complaint or inquiry (this may take place at various stages in the process); 4. that individuals making a complaint or inquiry must be advised that they may make a complaint to the IPC and provided with contact information for the IPC, and a description the IPC's functions under s. 49.12 of the Part; and 5. the process for determining when notification must be provided to the IPC, based on the scope of the complaint or inquiry and other relevant factors. **27.2.3** Publish details of the process in English and French on a Government of Ontario or, in the case of an extra-ministerial DI Unit, the person or entity's website. **27.2.4** Use clear and easy to understand language in the details of the process.
27.3	**27.3.1** Develop and maintain a log of privacy complaints received by the DI Unit. **27.3.2** At a minimum, the log must include: 1. the date that the complaint was received; 2. the nature of the complaint; 3. the action(s) taken to resolve the complaint and the date the individual making the complaint was advised of the action(s); 4. the time frame within which the complaint was addressed; and 5. the outcome of the complaint or inquiry (including any recommendations made following an investigation, the time frame within which such recommendations must be addressed, the name(s) of the member(s) responsible for addressing them, and the dates recommendations have been addressed).

PUBLICATION OF OTHER DOCUMENTS

To foster transparency and accountability, DI Units should make publicly available other documents relevant to the policies, procedures and operations of the DI Unit. These may include a reference to relevant open information publications, documentation relating to reviews by the IPC, and frequently asked questions.

GLOSSARY OF TERMS

Term	Definition
Coded information	PI from which direct identifiers have been removed and replaced with an internal code.
De-identifying	"De-identifying" within the meaning of the Part.
Delete	The removal of all electronic references to information or, in the case of non-electronic storage media, physical access to information.
DI Environment	All associated system components and information assets of a DI Unit's technology environment, including: • hardware, software, applications, security systems, network appliances and servers; and • PI, coded information, de-identified information, logs and authentication data.
DI Unit	A "ministry data integration unit," "inter-ministerial data integration unit" or "extra-ministerial data integration unit" within the meaning of the Part.
Direct identifier	Variables that provide an explicit link to a data subject and can directly identify an individual. Examples may include name, address, email address, telephone number, fax number, credit card number, license plate number, vehicle identification number, social insurance number, health card number, medical record number, device identifier, biometric identifiers, internet protocol (IP) address number and web universal resource locator (URL).
FIPPA	The *Freedom of Information and Protection of Privacy Act, 1990*.
Indirect identifier	Variables that may not directly identify an individual, but can still be used for indirect re-identification. These identifiers can be used, either by themselves or in combination with other available information, to identify an individual. Examples may include gender, date of birth or age, event dates (e.g., death, admission, procedure, discharge, visit), locations (e.g., postal codes, building names, regions), ethnic origin, country of birth, languages spoken, aboriginal status,

	visible minority status, profession, marital status, level of education, total years of schooling, criminal history, total income and religious denomination.
Linking	A method of bringing information from different sources together about the same individual.
Member	A "member" of a DI Unit within the meaning of the Part.
Personal information (PI)	"Personal information" within the meaning of *FIPPA*.
Privacy breach	Any theft or loss of PI or coded information or any collection, use or disclosure of PI or coded information that is not permitted under the Part, the Data Standards, the Practices and Procedures, other applicable provisions of *FIPPA* or its regulations, and agreements and acknowledgements made pursuant to them.
Privacy complaints	Concerns or complaints relating to a DI Unit's compliance with: • the Part; • the Data Standards; • the Practices and Procedures; • other applicable provisions of *FIPPA* or its regulations; or • agreements or acknowledgments made pursuant to them.
Secure disposal or destruction	The permanent removal of information from a storage medium such that its reconstruction or retrieval is not reasonably foreseeable in the circumstances.
Security breach	An event where: • there is an actual or potential breach of confidentiality, integrity or availability of the DI Unit's DI Environment, or the DI Environment is otherwise put at increased risk; or • there has been a contravention of the Part, the Data Standards, the Practices and Procedures, other applicable provisions of *FIPPA* or its regulations, or agreements or acknowledgments made pursuant to them relating to: – secure retention, secure transfer, secure disposal/destruction; or – de-identification and linking.

Storage media	The underlying physical medium on which information is stored, typically classified into two forms: non-electronic and electronic. Examples of non-electronic storage media include paper printouts and handwritten notes. Examples of electronic storage media include computer hard drives, copier and printer hard drives, removable solid drives including memory, disks and USB flash drives, mobile phones and magnetic tapes.
The Part	Part III.1 (Data Integration) of *FIPPA*.