

Ontario Public Service Data Integration Data Standards

Ministry of Public and Business Service Delivery and Procurement
October 2026

Table of Contents

Introduction	4
Purpose	4
Effective Date.....	5
Legal Authority	5
Application	5
Scope.....	6
Personal Health Information.....	6
Independent Oversight.....	7
Periodic Review	7
Data Integration Principles	8
Terms.....	9
Definitions	9
Data Integration Requirements	12
Prior to Data Collection and Acquisition	13
1. Governance and Accountability	13
2. Privacy and Security Training.....	15
3. Privacy Risk Management.....	17
4. Privacy Breach Reporting.....	19
5. Security Controls and Cyber Risk Management.....	21
Data Collection and Acquisition.....	24
6. Lawfulness and Purpose Specification	24
7. Data Minimization	25
8. Privacy-preserving Data Linkage	26
Prior to Data Release.....	27
9. De-identification.....	27
10. Agreements.....	28
Post Data Release	29
11. Data Retention and Destruction	29
12. Public Reporting	29

13.	Additional Extra-Ministerial Data Integration Unit Requirements	30
14.	Accountabilities and Responsibilities	31
	Appendix A: Related Legislation, Policies, Standards, and Guidelines	36

Introduction

The Government of Ontario collects and manages a wide range of data, including personal information, to deliver public services, administer lawfully authorized programs, and enforce laws. Where authorized, this information may also be used to monitor and evaluate the effectiveness of government initiatives. While this information can provide useful insights, in isolation it has limited utility.

However, combining datasets from multiple sources to create new and enriched datasets – a process known as *data integration* – can significantly increase the analytical value of information and generate insights that would not be possible from individual datasets alone.

When conducted appropriately, data integration provides a more comprehensive understanding of societal needs, assists in answering complex policy questions, informs policy development, and supports meaningful and continuous improvement of programs and services in areas such as health, social services, housing, and education by making better use of data that is already available.

While data integration provides significant public value, it can also introduce privacy risks when combining data about individuals. To protect the privacy of individuals while enabling responsible data integration practices, in 2019, the Government of Ontario amended the *Freedom of Information and Protection of Privacy Act, 1990* (FIPPA) to include requirements for the responsible, secure and privacy-protective data integration in Part III.1 of FIPPA.

To further support privacy-protective data integration, the Ontario Public Service (OPS) Data Integration Data Standards ('the Standards'), established under Part III.1 of FIPPA, provide a comprehensive, privacy-first, framework for designated Data Integration Units (DIUs) to support safe, secure, privacy-protective and accountable data integration.

This approach promotes access to timely, reliable and actionable findings derived from government-held information while protecting privacy and maintaining public trust.

Purpose

The Standards set out specific requirements and key practical steps that require the DIUs to protect the privacy, confidentiality and security of personal information throughout the entire data integration lifecycle, from project initiation and approval, to data collection and acquisition, linkage and de-identification, access to and analysis of data, and public reporting.

The Standards take a privacy-by-design approach to managing risks by requiring the DIUs to incorporate privacy considerations into the planning, design, governance, implementation and ongoing management of data integration activities, business processes and IT systems.

By adhering to these Standards, the DIUs ensure that data integration is managed in a way that supports public trust, reduces privacy and security risk, and promotes transparency and government accountability.

Effective Date

These Standards take effect in October 2026 and replace the OPS Data Integration Data Standards issued in April 2021.

Legal Authority

The Standards are established by the Chief Digital and Data Officer (CDDO) under the authority of Section 49.14(1) of Part III.1 of FIPPA.

The Standards operate alongside, and should be read in conjunction with, all applicable Government of Ontario corporate policies, standards, and directives relating to information management, information technology, cyber security, privacy and recordkeeping.

The Standards should be implemented in a manner that is consistent with existing legal obligations, restrictions and requirements, including those set out in FIPPA, the *Personal Health Information Protection Act, 2004* (PHIPA), the *Archives and Recordkeeping Act, 2006*, the *Anti-Racism Act, 2017* and/or other applicable legislation and associated regulations.

If these Standards conflict with FIPPA, its regulations, PHIPA, the *Archives and Recordkeeping Act, 2006*, the *Anti-Racism Act, 2017*, or any other applicable law or regulation, the legal requirement takes precedence.

Application

These Standards apply to all government ministries and external organizations that have been designated as a “data integration unit” (DIU) in Ontario Regulation (O. Reg.) 366/19: Data Integration under FIPPA. This includes:

- Ministry data integration units (MDIUs);
- Inter-ministerial data integration units (IMDIUs);
- Extra-ministerial data integration units (EMDIUs);

All MDIUs, IMDIUs, and EMDIUs (collectively referred to as “DIUs”) are required to comply with these Standards pursuant to section 49.14(4) of Part III.1 of FIPPA.

These Standards do not apply to personal information matching activities that are governed by other statutes or legal authorities outside Part III.1 of FIPPA (e.g., data integration governed under *the Anti-Racism Act, 2017*). Such activities remain subject to the statutory requirements, safeguards and limitations established under their respective authorities.

Ministries that are not designated as a DIU but conduct data integration activities under other legal authorities, may use these Standards as guidance to support consistent, secure and privacy-protective practices.

Scope

The Standards establish requirements for designated DIUs for how they collect, link, de-identify, use, retain and dispose of personal information under Part III.1 of FIPPA.

Data integration activities may only be conducted for the purposes authorized under section 49.2 of Part III.1 of FIPPA, specifically, to support analysis relating to a) the management or allocation of resources, b) the planning for the delivery of programs and services provided or funded by the Government of Ontario, and c) the evaluation of those programs and services. Individual privacy rights and public interest considerations must be appropriately assessed and protected before data collection is authorized.

Results of the data integration will not be used to identify an individual person or household, target individuals, make decisions about individual eligibility for services or benefits, or create disadvantage for specific people or groups whose information is involved. Datasets for analytical purposes will be de-identified in accordance with the requirements in Part III.1 of FIPPA and the Standards.

Personal Health Information

FIPPA’s definition of personal information in section 2(1) includes information relating to an individual’s medical, psychiatric, or psychological history. Part III.1 of FIPPA also permits, in specified circumstances, the collection of personal health information from entities regulated under the *Personal Health Information Protection Act, 2004* for authorized data integration purposes, subject to the conditions and restrictions established in Part III.1 of FIPPA and these Standards. Accordingly, references to personal information in these Standards may include personal health information, unless the context indicates otherwise.

Independent Oversight

The Office of the Information and Privacy Commissioner of Ontario (IPC) provides independent oversight of institutions subject to FIPPA, and the DIUs operating under Part III.1 of FIPPA and the Standards.

The IPC may assess DIUs' compliance with Part III.1 of FIPPA and the Standards, make recommendations, issue orders, and/or require corrective measures (e.g., order to discontinue the practice or procedures, change the practice or procedures, destroy personal information collected or retained under the practice or procedures, implement a new practice or procedures) to ensure compliance with privacy protection requirements in Part III.1 of FIPPA and the Standards in accordance with sections 49.12(1) - (7) of Part III.1 of FIPPA.

The IPC may also make comments or recommendations concerning the privacy implications of data integration activities under Part III.1 of FIPPA and these Standards consistent with section 49.14.1 of Part III.1 of FIPPA.

Periodic Review

The Government of Ontario will periodically review the Standards to ensure that they continue to fulfill the requirements set out under section 49.14(1) of Part III.1 of FIPPA. The CDDO will oversee the periodic review. All relevant parties, the DIUs and the IPC will be consulted before any significant amendments are made to the Standards.

Data Integration Principles

The following principles are intended to guide the DIUs in interpreting and applying these Standards.

Principle 1 - Strategic Asset

Manage information as a strategic asset to maximize its value, usability, and evidence-based decision-making.

Principle 2 – Accountability

Protect personal and sensitive information used in data integration and maintain clear accountability for its appropriate handling during data integration activities.

Principle 3 – Public Interest

Undertake data collection for a legitimate public purpose and ensure that privacy rights of affected individuals are carefully assessed and protected.

Principle 4 – Proportionality and Necessity

Ensure all data integration activities are necessary for authorized purpose(s), justified, and proportionate to the intended analytical objective.

Principle 5 – Data Privacy and Security

Embed robust privacy and security controls throughout the data integration lifecycle and protect personal information from unauthorized access, disclosure, loss or misuse.

Principle 6 - Accuracy

Produce accurate, reliable, and high-quality outputs, and actively identify and mitigate bias, discrimination, and inequitable outcomes.

Principle 7 – Transparency

Conduct data integration activities transparently and demonstrate accountability to support and maintain public trust.

Terms

The following terms are used throughout these Standards to indicate the level of obligation associated with a requirement:

Must: a mandatory requirement that must be met.

Should: a recommended requirement that is expected to be followed. Where an alternative approach is adopted, the rationale, associated risks, and approvals should be documented.

Definitions

The following definitions are provided to support the consistent interpretation and application of these Standards. Where a term is defined in applicable legislation, the legislative definition prevails.

Term	Definition
Accountable Executive	An ADM or Director-level executive, or its delegate, of the ministry/organization where the DIU is located.
Accountable Ministry	The ministry responsible for establishing accountability arrangements and supporting the governance of an EMDIU under Part III.1 of FIPPA.
Chief Digital and Data Officer (CDDO)	The Chief Digital and Data Officer appointed under section 3(1) of the <i>Simpler, Faster, Better Services Act, 2019</i> .
Data Integration IT System	The technology environment used to support data integration activities, including associated infrastructure, applications, databases, networks, storage and backup media, security controls, and information assets.
Data Integration Activities	Collection, use, linking, de-identification, analysis, disclosure, retention, or disposal of personal information under Part III.1 of FIPPA for the authorized purposes set out in section 49.2 of Part III.1 of FIPPA.
Data Integration Unit (DIU)	An MDIU, IMDIU or EMDIU designated under Ontario Regulation 366/19: Data Integration made under FIPPA.
De-identified Information	Information from which information that identifies an individual, or could reasonably be used to identify an individual, has been removed.

Term	Definition
De-identification	As described in section 49.1(2) of Part III.1 of FIPPA, a process of removal of information that identifies an individual, or could reasonably be used, alone or with other information, to identify an individual.
DIU Manager	The management-level official designated to oversee compliance with Part III.1 of FIPPA and these Standards, as well as the daily operations of the DIU.
DIU Member	For an MDIU and an IMDIU, an officer, employee or agent of the ministry in which the unit is located who works as part of the unit; and For an EMDIU, an officer, employee or agent of the person or entity who works as part of the unit, as defined in Part III.1 of FIPPA.
Extra-ministerial Data Integration Unit (EMDIU)	A person or entity, or an administrative division of a person or entity, that is designated as an extra-ministerial data integration unit in O. Reg. 366/19: Data Integration under FIPPA.
Head of Institution	The accountable minister for the ministry in which the DIU is located responsible for overseeing the administration and compliance with Part III.1 of FIPPA, its regulations, and the Standards.
Information derived from personal information	Information that is created, transformed, linked, aggregated, or otherwise derived from personal information collected under Part III.1 of FIPPA. Where information derived from personal information includes information that identifies an individual or information that could be used, either alone or in combination with other information, to identify an individual based on what is reasonably foreseeable in the circumstances, it remains subject to Part III.1 of FIPPA, the Standards, and applicable legislative, regulatory and enterprise-wide requirements with respect to privacy, security, retention, disposition, and destruction.
Inter-ministerial Data Integration Unit (IMDIU)	An administrative division of a ministry that is designated as an IMDIU in O. Reg. 366/19: Data Integration under FIPPA.
Ministry Data Integration Unit (MDIU)	An administrative division of a ministry that is designated as an MDIU in O. Reg. 366/19: Data Integration under FIPPA.
Part III.1 of FIPPA	Part III.1 Data Integration of the <i>Freedom of Information and Protection of Privacy Act, 1990</i> (FIPPA).

Penetration Test	An evaluation method that is used to test a system, application or network in order to determine if any vulnerabilities exist that could potentially be exploited.
Personal Information	Information relating to an identifiable individual as defined in section 2(1) of FIPPA.
Personal Health Information	Personal health information as defined in section 4(1) of the <i>Personal Health Information Protection Act, 2004</i> .
Privacy Breach	The theft, loss, or unauthorized collection, use, disclosure, retention, or disposal of personal information contrary to law, these Standards, or authorized information management practices.
Privacy Impact Assessment	A process used to identify, assess, and address privacy risks associated with the collection, use, disclosure, retention, or disposal of personal information.
Security Breach	An incident that compromises, or could reasonably compromise, the confidentiality, integrity, or availability of information, systems, or services used for data integration activities.
Senior Officer	In respect of an EMDIU, the administrative head of the organization or another officer designated in the regulations as the senior officer. Where an EMDIU is not an institution, or part of an institution, its senior officer is deemed to be the head of the institution for the purposes of Part III.1 of FIPPA.
Threat Risk Assessment	A process used to identify and assess threats, vulnerabilities, and risks to information, systems, and services, and to determine appropriate safeguards.
Vulnerability Scan	A process used to determine existing weaknesses or gaps in an information system's protection efforts.

Data Integration Requirements

This section defines mandatory standards the DIUs must follow to comply with Part III.1 of FIPPA and to support secure and privacy-protective data integration.

The requirements apply to every stage of managing personal information throughout the data integration lifecycle from planning and preparation to collection, data linkage, de-identification, analysis and reporting.

These Standards should be read and applied in conjunction with applicable legislative and regulatory requirements, relevant Government of Ontario corporate policies, standards, and directives relating to information management, information technology, cyber security, privacy and recordkeeping.

These Standards are supported by enterprise tools, guidance, training and assurance mechanisms that promote ongoing compliance, continuous improvement, risk management and auditability.

Prior to Data Collection and Acquisition

1. Governance and Accountability

- 1.1. The DIUs must establish clear responsibilities and accountability structures for the proper management and compliance of data integration activities with Part III.1 of FIPPA, these Standards, applicable legislation, regulations, policies, and standards and best practices relating to data integration.
- 1.2. The head of the government institution, or the Accountable Executive of the ministry or organization where the DIU is located, or their delegate, must designate or identify an official, at the management level (the “DIU manager”) responsible for overseeing compliance with Part III.1 of FIPPA, these Standards, and applicable legislation, regulations, policies, and standards and best practices relating to data integration, as well as daily operations of a DIU.
- 1.3. The DIU manager must ensure that, prior to undertaking any data integration activity, the DIU complies with Part III.1 of FIPPA, these Standards, any applicable legislation, regulations, policies, standards and best practices relating to data integration.
- 1.4. If non-compliance is identified, the DIU manager must ensure that appropriate and timely remedial action is taken. The DIU manager should consult with program managers, legal counsel, privacy, security and recordkeeping teams, as necessary, for the proper application of all provisions in Part III.1 of FIPPA and these Standards.
- 1.5. The DIU manager must ensure that decisions, decision-making processes, approvals, and any other evidence of compliance with Part III.1 of FIPPA and these Standards are documented and maintained and must be able to produce such evidence upon request for audit, review, investigation or reporting purposes. Examples of evidence may include attestations, privacy and security assessments, policies, practices and procedures.
- 1.6. The DIU manager must develop and document an impartial and confidential process for DIU members to report operational gaps or deficiencies, as well as actual or suspected incidents of non-compliance with Part III.1 of FIPPA and/or these Standards without the fear of reprisal. The responsibilities for investigating wrongdoing must be delegated to an independent party outside the DIU with appropriate authority, capacity, and expertise.

- 1.7. The DIU manager should assign roles and responsibilities for all data integration activities, including, but not limited to:
- Developing, implementing, monitoring and updating policies, procedures and practices, as needed, relating to data integration activities;
 - Following privacy-protective linking and de-identification practices;
 - Evaluating re-identification risks;
 - Reporting privacy breaches and security incidents;
 - Addressing quality or technical issues;
 - Applying disclosure controls;
 - Overseeing privacy and security assessments, and data sharing arrangements.
- 1.8. All DIU members must sign a confidentiality agreement at the commencement of their employment, or other relationship with the DIU, and prior to receiving access to personal information.
- 1.9. At a minimum, the confidentiality agreement should include:
- Confirmation that individuals executing the confidentiality agreement are members of the DIU, and the responsibilities associated with their particular role;
 - A requirement that the DIU members comply with Part III.1 of FIPPA, these Standards, and other applicable legislation, regulations, policies, standards and best practices relating to data integration;
 - An acknowledgement that the DIU members have read, understood and agree to comply with the terms of the confidentiality agreement;
 - An explanation of the purposes for which personal information may be collected, and how this information is permitted to be used under Part III.1 of FIPPA and the Standards;
 - Restrictions on access, use, and disclosure of personal information;
 - The prohibition against using or attempting to use de-identified information, alone or in combination with other information, to identify an individual pursuant to section 49.8 of Part III.1 of FIPPA;
 - A requirement that the DIU members to notify the DIU manager at the first reasonable opportunity of an actual or suspected privacy or security breach;
 - DIU members' role in facilitating an access to or correction of information request, or a privacy complaint under FIPPA;

- A requirement that DIU members securely return all property belonging to the DIU, including all physical access mechanisms (e.g., identification / access cards and keys), on or before the date of termination of the employment, or other relationship with the DIU, or where the DIU manager determines the property or physical access mechanisms are no longer required to carry out responsibilities with respect to data integration.
- 1.10. The DIU manager must ensure the DIU's ongoing compliance with Part III.1 of FIPPA and these Standards by regularly monitoring and evaluating the unit's practices, procedures, privacy and security controls to ensure they remain effective, appropriate, and compliant, and are updated as necessary.
 - 1.11. The Accountable Executive for the DIU must provide an annual compliance attestation to the CDDO, at the beginning of each fiscal year, confirming that the DIU's data integration practices have been assessed against Part III.1 of FIPPA and these Standards and comply with all the requirements.
 - 1.12. Compliance attestations must include specific information concerning the DIUs' compliance with Part III.1 of FIPPA and these Standards, including, but not limited to, a summary of all privacy breaches and complaints received in the prior year, or a statement that there were no such breaches or complaints.

2. Privacy and Security Training

- 2.1 The DIU manager must ensure that all DIU members understand their responsibilities for protecting individuals' privacy as well as the safeguards and controls available to protect personal information.
- 2.2 All DIU members, including all full-time, part-time, temporary and contract employees, must successfully complete mandatory privacy and security training prior to receiving access to personal information, followed by annual refreshers.
- 2.3 Training must be tailored to data integration activities, reflect the specific privacy and security risks associated with data integration, relate to specific DIU members' roles, be tracked, documented, and updated, as necessary.
- 2.4 At a minimum, the initial privacy and security training should include:

- An overview of DIU's duties and responsibilities for privacy and security protections under Part III.1 of FIPPA, these Standards, and other applicable legislation, regulations, policies, standards and best practices relating to data integration;
- An explanation of the purposes for which personal information may be collected, and how this information is permitted to be used under Part III.1 of FIPPA and these Standards;
- Restrictions on access, use and disclosure of personal information;
- A prohibition on re-identifying information that has been de-identified;
- Administrative, technical and physical safeguards implemented by the DIU to protect personal information against theft, loss and unauthorized collection, use or disclosure and against unauthorized copying, modification or disposal, and DIU members' duties in implementing these safeguards;
- The purposes of notices of collection, data sharing agreements, and annual reports, and their key provisions;
- Explanation of DIU's protocols for privacy breaches and management response to security incidents, and related duties and responsibilities imposed on DIU members in identifying, reporting, containing and participating in the investigation and remediation of privacy breaches and security incidents;
- A process for managing an access to or correction of information request, or a privacy complaint made under FIPPA.

2.5 An annual refresher privacy and security training should include emerging privacy and security risks, technological developments, evolving legal and regulatory requirements, Government of Ontario privacy and security policies and standards, and best practices relevant to data integration activities.

2.6 At a minimum, the annual refresher privacy and security training should address:

- Any new privacy and security policies, standards, practices and procedures, as well as significant amendments to existing privacy and security policies, standards, practices and procedures;
- Any relevant changes since the last training, including findings and recommendations arising from privacy and security assessments, audits, and the investigation of privacy breaches, security incidents and privacy complaints;
- Orders, decisions, guidelines, fact sheets and best practices issued by the IPC.

- 2.7 The DIU manager is responsible for ensuring that initial and annual refresher privacy and security training has been provided to all DIU members.

3. Privacy Risk Management

- 3.1 The DIUs must ensure that privacy risks are proactively identified, effectively mitigated, and continuously monitored.
- 3.2 The DIUs must complete a Privacy Impact Assessment (PIA) on the IT infrastructure, business processes, and data flows involved in data integration activities before collecting personal information.
- 3.3 The DIUs must complete a project-specific PIA before collecting personal information or document why an existing PIA remains sufficient for the proposed data integration activities.
- 3.4 The DIUs must update a PIA when substantial modifications are made to the DIU's existing activities that involve personal information, including:
- a) use of a new or modified technology or business process that involves collection, linking, de-identification, access or disclosure of personal information;
 - b) significant change to the purpose for which personal information is used or disclosed;
 - c) involvement of any other institution or any third party under a contractual agreement or a data sharing arrangement with the DIU;
 - d) Standards or legislative change(s) to Part III.1 of FIPPA that affect how personal information is managed;
 - e) when the DIU manager determines that a PIA is warranted given the high complexity or potential risks associated with the use of personal information.
- 3.5 At a minimum, a PIA should include:
- A description of the data integration project, and/or program, process, IT system(s) being assessed;
 - Confirmation that the proposed collection, use and disclosure of personal information are authorized under Part III.1 of FIPPA;
 - The purpose(s) for which personal information will be collected, used, and linked, as required under section 49.2 of Part III.1 of FIPPA;

- An explanation of why collection of personal information is necessary, and why the purpose(s) cannot reasonably be achieved using de-identified information, aggregate information or publicly available information;
- Confirmation that collection of personal information is in the public interest, as required under section 49(4) 4. of Part III.1 of FIPPA;
- The type(s) of personal information that will be collected, the sources from which it will be collected, the confirmation that those sources are authorized under section 49.4(1) or (2) of Part III.1 of FIPPA, and whether it will be linked with other information, including the nature and sources of that information;
- A description of how personal information will flow through the data integration process, and the specific roles of DIU members who will have access to this information;
- Any limitations or restrictions imposed on the collection, use, linkage, or disclosure of personal information and information derived from personal information;
- Whether personal information will be de-identified and the de-identification process that will be used to reduce the risk of re-identification;
- Confirmation that the notice relating to the personal information has been published online and meets the requirements of section 49.10 of Part III.1 of FIPPA;
- The administrative, technical and physical safeguards and practices that will be used to protect personal information, information derived from personal information, and de-identified information, and an assessment of any risks to individuals in the event of a theft, loss or unauthorized use or disclosure;
- The measures the DIU will implement to,
 - a) prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information, information derived from personal information, and de-identified information from occurring, and
 - b) mitigate the risks to individuals in the event of such an occurrence.
- The period of time that personal information, information derived from personal information, and de-identified information will be retained for.

3.6 The DIUs must implement risk mitigation measures identified in the PIA before collecting personal information or, if it is not possible to implement mitigations

measures before collecting the personal information, within a reasonable time after collecting the information.

- 3.7 Where a DIU determines that a recommended mitigation measure will not be implemented, the DIUs must provide the rationale and identify any residual privacy risks, and alternative mitigation measures adopted to effectively mitigate those risks.
- 3.8 The DIUs must document strategies used to prevent, reduce and mitigate the identified risks and track implementation of all PIA recommendations in a Risk Mitigation Plan.
- 3.9 When an update is required, the DIUs must include any additional prevention and mitigation measures needed to address new or increased risks.
- 3.10 The DIUs should obtain an approval of the PIA from the Accountable Executive for the DIU prior to the collection of personal information.
- 3.11 The DIUs must provide a copy of the PIA to the IPC, if requested.
- 3.12 The DIU manager should establish a schedule to periodically review the PIA to ensure risk mitigation measures remain current and effective.

4. Privacy Breach Reporting

- 4.1 The DIUs must rapidly identify, mitigate and respond to privacy breaches or any incidents resulting from theft, loss or unauthorized use, access or disclosure of personal information.
- 4.2 The DIUs should develop a Privacy Breach Response Protocol to ensure the DIU can rapidly address incidents like privacy breaches, security incidents, or system vulnerabilities.
- 4.3 The Privacy Breach Response Protocol should:
 - Designate roles and backups responsible for responding to such incidents;
 - Define and document the specific order of steps for responding to such incidents;

- Use an escalation matrix to map issue severity to the appropriate response level;
 - Establish communication channels for effective notification, including when to notify Legal Counsel, IT/Security team, executive leadership, the affected individuals and the IPC;
 - Include procedures for immediate containment and recovery;
 - Document all decisions, actions, and notifications.
- 4.4 The DIUs should run annual tabletop exercises to simulate real-world privacy incidents, and to ensure the DIU members know exactly who to notify in the event of a breach.
- 4.5 In the event of a privacy breach involving personal information collected under Part III.1 of FIPPA, the DIUs must promptly assess the nature and scope of the breach and determine whether notification obligations are triggered under section 49.11(3) and (4) of Part III.1 of FIPPA.
- 4.6 Where notification is required, the DIUs must notify affected individuals and the IPC at the first reasonable opportunity and in accordance with legislative requirements in section 49.11(3) and (4) of Part III.1 of FIPPA.
- 4.7 The DIUs should coordinate with the cyber security, technology, privacy, legal and other relevant teams throughout the privacy breach response and remediation activities, as necessary.
- 4.8 If a privacy breach occurs with a third-party vendor, the DIUs must work with the vendor as soon as possible to respond to the breach and provide notice to the affected individuals and the IPC, as appropriate. The DIU remains accountable for ensuring that appropriate containment, investigation, remediation, and notification activities occur.
- 4.9 The DIUs should conduct post-breach root cause analysis to identify contributing factors, assess the effectiveness of response measures, implement corrective actions designed to prevent recurrence, and track metrics like resolution time and escalation rate to improve processes. Lessons learnt should be documented and incorporated into governance, training, and policies and procedures, as necessary.

- 4.10 The DIUs must maintain a record of all thefts or losses of personal information, and all uses or disclosures not permitted by Part III.1 of FIPPA and these Standards, including:
- The nature, scope, and timeline of the breach, including the date of the breach, if known, and the date it was detected, and a summary of how it was discovered;
 - The type, sensitivity, and volume of personal information involved;
 - The number of individuals affected, or estimated, and an assessment of the actual or potential harms arising from the breach (e.g., identity theft, financial loss, reputational harm, discrimination, or loss of privacy);
 - Corrective actions and remediation measures taken, or planned, to reduce and further prevent unauthorized access, use, disclosure, loss, or theft of personal information;
 - The findings and recommendations arising from the investigation;
 - Notice of theft, loss, or unauthorized use or disclosure to the affected individual(s) and the IPC in accordance with section 49.11(3) and (4);
 - The name and role of the DIU member(s) responsible for managing the breach, implementing corrective actions, and monitoring remediation activities.

5. Security Controls and Cyber Risk Management

Note: *It is beyond the scope of these Standards to provide an exhaustive list of security controls and technical safeguards that must be implemented by the DIUs. This section includes a minimum set of requirements for DIUs that must be supplemented by the Government of Ontario Information Technology Standards (GO-ITS), relevant corporate policies and directives.*

It is the responsibility of the DIU manager to address the full scope of enterprise-wide security requirements of IT system(s) for data integration, including risk assessments, selection of safeguards and controls, ongoing monitoring, management review, and continuous improvement and oversight.

- 5.1 The DIUs must assess privacy and security risks at all stages of the data integration lifecycle and implement appropriate measures to safeguard information in accordance with the enterprise-wide security controls, technical safeguards, relevant corporate policies, directives and standards.

- 5.2 The DIUs must ensure IT system(s) for data integration are aligned with approved enterprise digital, data, and security architectures and platforms.
- 5.3 The DIUs must implement appropriate security controls and technical safeguards to protect personal information, information derived from personal information and de-identified information. The security measures must be appropriate and proportional with the sensitivity level of the information processed and maintained in the IT systems for data integration.
- 5.4 Where the DIU is not subject to Government of Ontario information technology and cyber security requirements, corporate policies and standards, the accountable ministry must assess equivalency of safeguards, operating model and document any required mitigations before collection begins.
- 5.5 The DIUs external to the OPS must implement security controls and technical safeguards that are equivalent to, or exceed, Government of Ontario security requirements. These DIUs must be able to demonstrate compliance upon request through appropriate assessments, attestations, audits, and other evidence acceptable to the Government of Ontario.
- 5.6 The DIUs must ensure that all data sets involved in data integration activities are classified and handled in accordance with the corporate information sensitivity classification requirements.
- 5.7 Transmitted and stored personal information that has been classified as 'High Sensitivity' must be protected using encryption (in transit and at rest) of a type and strength sufficient to withstand attacks in accordance with enterprise-wide general security and cryptography requirements. Encryption keys or passwords must be appropriately protected and managed.
- 5.8 The DIUs must complete a Threat Risk Assessment (TRA) for IT system(s) for data integration. The DIUs must periodically review and refresh the TRA if there is a significant change to IT system(s) for data integration, business processes, legal or threat environment or after major security incidents, as part of ongoing risk management and security governance to ensure the assessment remains current and valid.
- 5.9 The DIUs must conduct vulnerability scans and penetration tests in accordance with the enterprise-wide requirements to continuously identify,

assess, remediate, mitigate and monitor vulnerabilities in IT system(s) for data integration.

- 5.10 The DIU manager must identify and document authorized users, their roles, and their associated access privileges prior to granting access to IT system(s) for data integration in accordance with the enterprise-wide direction for identity and access management.
- 5.11 The DIU manager must ensure that access to personal information, information derived from personal information, de-identified information, and IT system(s) for data integration is limited to authorized DIU members who require access to perform duties related to data integration activities according to the principle of least privilege.
- 5.12 The DIU manager must ensure that no single DIU member has excessive access to personal information, information derived from personal information or de-identified information through segregation of duties and functional separation of roles in order to reduce the likelihood of unauthorized modification, or other misuse of information.
- 5.13 The DIU manager must evaluate where access can be granted to de-identified data instead of personal information to minimize exposure to sensitive information where operationally feasible.
- 5.14 The DIUs must implement audit logs to verify that only authorized users access personal information, information derived from personal information, and de-identified information. Information captured and retained in the audit logs must be in accordance with enterprise-wide security requirements.
- 5.15 The DIU manager must ensure that access privileges are regularly reviewed and revoked when no longer needed.
- 5.16 The DIUs must develop and implement a Security Incident Management process and clearly identify DIU roles and responsibilities for reporting cyber security events and incidents in accordance with the enterprise-wide direction for managing cyber security risks.

- 5.17 All suspected or confirmed security breaches involving personal information, information derived from personal information, or de-identified information must be immediately reported to appropriate enterprise authorities in accordance with enterprise-wide incident management and escalation process.

Data Collection and Acquisition

6. Lawfulness and Purpose Specification

- 6.1 Where collection of personal information is authorized under Part III.1 of FIPPA, the DIUs must be clear about what information requirements they have and for what purpose they are collecting that information.
- 6.2 For each new data integration project, the DIU must assess, confirm, and document that the collection of personal information is necessary to meet one or more purposes set out in section 49.2 of Part III.1 of FIPPA.
- 6.3 The DIU must assess whether the specified purpose(s) can be reasonably achieved by using existing, de-identified information, aggregate information or publicly available information.
- 6.4 The DIU must confirm and document that the collection of personal information is in the public interest after considering the privacy interests of affected individuals and the manner in which their personal information will be protected, as required under section 49(4) 4. of Part III.1 of FIPPA.
- 6.5 The DIU must ensure personal information is collected only from authorized entities set out in Part III.1 of FIPPA and confirm that no restrictions apply to the collection of personal information. The DIU should document the data sources, the data owners, and the types of data collected for each DI project.
- 6.6 The DIUs must consider the impact on individuals' right to privacy by conducting tests of necessity, effectiveness, proportionality, and minimal intrusiveness (the "four-part test") to ensure that collection of personal information is justifiable.

- 6.7 The DIUs must ensure that all data integration projects involving the collection and linking of personal information receive the required approval from the DIU manager and/or Accountable Executive for the DIU prior to the start of the project.
- 6.8 The DIUs must publish a notice of collection on a government website with respect to the proposed collection of personal information under Part III.1 of FIPPA. The notice must meet the content requirements in section 49.10 of Part III.1 of FIPPA and be accurate, accessible and kept up to date.

7. Data Minimization

- 7.1 The DIUs must not collect personal information under Part III.1 of FIPPA, use or disclose that information, if other information will serve the purpose of collection, use or disclosure.
- 7.2 The DIUs must take reasonable steps to ensure that the minimum amount and type of personal information is collected, used and disclosed for data integration projects.
- 7.3 Where collection of personal information is authorized, the DIU must work with the requesting entity and data provider to determine the type of personal information data elements that need to be extracted from source systems to ensure only minimal information is collected.
- 7.4 The data files collected and stored must contain only the relevant personal information required to support the overall purpose(s) of collection under Part III.1 of FIPPA. Personal information that is not required must not be collected, transferred, copied, or retained within the DIU.
- 7.5 The DIU should maintain an inventory of all personal information collected and describe the purposes for collection, specific data elements, the sources, and document data minimization decisions.

8. Privacy-preserving Data Linkage

- 8.1 The DIUs must ensure methods used to perform data linkage are privacy-protective, secure, robust and trustworthy. All one-to-one record-level linkage activities involving personal information collected under Part III.1 of FIPPA must be conducted within IT system(s) for data integration.
- 8.2 Technical procedures for data integration must have clearly documented work processes which adhere to the requirements in these Standards and Part III.1 of FIPPA.
- 8.3 The DIU must establish and document the required approval process for data linkage activities.
- 8.4 The DIUs must ensure that secure linking environment(s), governance and risk mitigation requirements are in place as identified in previous sections.
- 8.5 The DIUs must ensure that direct identifiers (e.g., name, date of birth, IDs) are stored and processed separately from analytical/statistical information. No single DIU member, with the exception of the system administrator, should have access to both simultaneously without authorization from the DIU manager or the Accountable Executive within a DIU.
- 8.6 The DIUs must replace direct identifiers with a project-specific data linkage key as early as possible in the data integration workflow. Linkage keys and associated identifier mappings must be maintained separately from direct identifiers.
- 8.7 The DIUs must conduct regular quality assessments of linkage processes to identify and mitigate linkage errors to ensure accuracy of linkage processes, and the validity of analyses and interpretation of results.

Prior to Data Release

9. De-identification

- 9.1 The DIUs must use appropriate de-identification methods to ensure that individuals cannot be reasonably identified from the release of de-identified information.
- 9.2 The DIUs must use de-identification techniques that are commensurate to privacy risks.
- 9.3 The DIUs must consider factors such as the sensitivity of data, the potential harm that could result from re-identification, the granularity of data, whether the data will be released publicly and publicly available information that could be linked with the data and used to re-identify individuals, among others.
- 9.4 The DIUs must determine the acceptable level of residual re-identification risk for every new data release, taking into account the factors mentioned above.
- 9.5 The DIUs must reduce the risk of re-identifying the individual(s) from the data, alone or in combination with other reasonably foreseeable sources of information, to an acceptable level.
- 9.6 The DIUs must continuously monitor re-identification risks throughout the data integration project. Where re-identification risk has crossed the acceptable threshold, the DIU must implement appropriate mitigation measures and consult privacy, security, and legal teams, as necessary.
- 9.7 The DIUs must document the de-identification methods and decisions, safeguards, re-identification risk assessment results, and approved risk-threshold decisions for every new data integration project.
- 9.8 The DIUs must ensure that de-identification techniques remain effective, up to date, and defensible over time through regular monitoring, testing and improvement.

- 9.9 The DIUs must not disclose personal information, linkage files, or any information that could reasonably enable record-level linkage or re-identification outside the DIU, except as permitted in section 49.9 of Part III.1 of FIPPA.

10. Agreements

- 10.1 When sharing de-identified information, the DIUs must ensure appropriate data sharing arrangements are in place ahead of disclosure.
- 10.2 Data sharing agreements must describe how de-identified information will be safeguarded by the receiving entity and include procedures to be followed in the event of a privacy breach or a security incident.
- 10.3 The data sharing agreement must include provisions prohibiting the receiving entity from re-identifying individuals and from onward sharing of de-identified information.
- 10.4 In addition to the above requirements, the data sharing agreement should include information relating to:
- The institutions or legal entities entering the data sharing agreement, including the DIU type, and its associated duties and responsibilities under Part III.1 of FIPPA;
 - Details of de-identified information (e.g., dataset format, volume etc.) and the purpose(s) for which it will be disclosed;
 - The process that will be used to securely transfer the de-identified information;
 - The manner in which the de-identified information will be securely retained;
 - The retention period for de-identified information, and whether it will be securely deleted, destroyed, or returned following the expiration of the retention period, and the mandatory protocol for securely deleting, destroying, or returning de-identified information.

Post Data Release

11. Data Retention and Destruction

- 11.1 The DIUs must ensure personal information, information derived from personal information and de-identified information are retained and securely disposed of in accordance with legislative requirements and enterprise-wide policies and standards.
- 11.2 The DIUs must retain personal information collected under Part III.1 of FIPPA, information derived from personal information and de-identified information in accordance with legislative requirements and approved retention schedules.
- 11.3 Personal information collected under Part III.1 of FIPPA must be retained for at least one year after last use, or in accordance with an approved retention period, and not longer than necessary to achieve the authorized purposes under Part III.1 of FIPPA.
- 11.4 The DIUs must dispose of personal information, information derived from personal information and de-identified information following the expiration of the retention period, using authorized disposition processes in accordance with enterprise-wide requirements, applicable records schedules, and secure destruction protocols.
- 11.5 The DIUs must document destruction decisions and supporting evidence confirming that personal information is retained for at least one year after last use, or in accordance with an approved retention period, and all copies of the information have been securely disposed of from all IT systems for data integration, including vendor environments, following the expiration of the retention period.

12. Public Reporting

- 12.1 The DIUs must publish an annual report describing the collection, linkage, use, de-identification, disclosure and public interest of data integration activities on a Government of Ontario website, or on a publicly accessible website for an

EMDIU, in accordance with sections 49.13(1)(1.1) and (2) of Part III.1 of FIPPA. The reports should use clear and easy to understand language.

- 12.2 If an access or a correction to information request or a privacy complaint is received, the DIU should work with the Freedom-of-Information Coordinator to coordinate a necessary response in timely and compliant manner.
- 12.3 Where a privacy complaint identifies a potential privacy risk or non-compliance with Part III.1 of FIPPA or these Standards, the DIU must document the issue, assess its impact, and implement appropriate corrective or mitigation measures.

13. Additional Extra-Ministerial Data Integration Unit Requirements

***Note:** The Extra-ministerial Data Integration Units (EMDIUs) may operate outside the Government of Ontario legislative and policy framework but are authorized to collect, use, link, and de-identify personal information under Part III.1 of FIPPA. As such, additional privacy controls and security safeguards are required to ensure equivalent levels of privacy protection, security, accountability, and transparency.*

Before an EMDIU collects personal information under Part III.1 of FIPPA, the accountable ministry must:

- 13.1 **Confirm equivalency:**
Assess and document that the EMDIU's governance, safeguards, processes, and technical environment provide a level of protection that is equivalent to, or exceeds, Government of Ontario security requirements.
- 13.2 **Establish formal agreements:**
Enter into a written agreement (e.g., Transfer Payment Agreement, contract, memorandum of understanding, or other binding instrument) that clearly sets out roles, responsibilities, controls, safeguards, and compliance requirements necessary to protect personal information collected under Part III.1 of FIPPA.
- 13.3 **Define applicable requirements:**
Specify in the agreement the policies, standards, and safeguards the EMDIU must meet, including privacy, security, recordkeeping, and data management requirements equivalent to OPS expectations, as applicable.

- 13.4 **Confirm compliance:**
The agreement must include confirmation of EMDIU's overall compliance under section 49.14(4) with the purpose, functions, and requirements set out in Part III.1 of FIPPA and the Standards.
- 13.5 **Restrict use and access:**
Ensure that personal information is collected, used, and disclosed only for the permitted purpose under Part III.1 of FIPPA, and prohibit any unauthorized uses.
- 13.6 **Secure environment:**
Ensure that personal information is managed within appropriately secured and segregated environments, with controls to prevent unauthorized access, use, or modification.
- 13.7 **Establish breach and change notification requirements:**
Require the EMDIU to immediately report any actual or suspected privacy or security breach and notify the accountable ministry of any material changes to business processes, data flows, or technical infrastructure that may impact privacy or security.
- 13.8 **Audit practices:**
Establish the right of the accountable ministry to conduct periodic or discretionary audits to assess compliance with Part III.1 of FIPPA and the Standards and require the EMDIU to fully cooperate with such audits.

14. Accountabilities and Responsibilities

14.1 Head of Institution (MDIU, IMDIU) / Senior Officer (EMDIU)

Accountable for:

- ensuring that all data integration activities carried out by a designated DIU comply with Part III.1 of FIPPA, the Standards, applicable legislation, regulations, policies, standards and best practices,
- for an EMDIU, ensuring compliance with requirements established through agreements with the accountable ministry, including audit rights, notification obligations, privacy protections and security safeguards,

- ensuring a delegation of authority for FIPPA is inclusive of data integration responsibilities.

14.2 **Accountable Ministry (EMDIU)**

Responsible for:

- establishing oversight arrangements to support confidence that the EMDIU maintains protections equivalent to Part III.1 of FIPPA and the Standards.

14.3 **Accountable Executive**

Accountable for:

- ensuring personal information is collected, used, linked, de-identified, disclosed, retained and disposed of in accordance with Part III.1 of FIPPA and the Standards, applicable legislation, regulations, policies, standards and best practices,
- ensuring data integration activities are undertaken in accordance with authorized purposes and in the public interest,
- identifying and mitigating access, privacy, security and recordkeeping risks across the DIU, and ensuring remedial measures are taken when non-compliance or privacy/security risks are identified,
- for an EMDIU, ensuring compliance with requirements established through agreements with the accountable ministry, including audit rights, notification obligations, privacy protections and security safeguards.
- providing an annual compliance attestation to the CDDO, at the beginning of each fiscal year, confirming compliance with Part III.1 of FIPPA and the Standards,
- approving PIAs for data integration activities.

14.4 **DIU Manager**

Accountable for:

- operational oversight, compliance management, and implementation of privacy controls and security safeguards within a DIU,
- compliance with Part III.1 of FIPPA and the Data Standards, and applicable policies/standards before any data integration activity is undertaken,
- establishing and maintaining documented policies, procedures, controls and operational practices to support privacy-protective and secure data integration practices,

- assigning roles and responsibilities for data linkage, de-identification, re-identification risk assessment, breach management, privacy and security assessments,
- executing confidentiality agreements for all DIU members,
- developing, implementing and documenting privacy and security training for all DIU members,
- ensuring privacy, security and cyber risk assessments and mitigation plans are completed before data collection, and linkage activities begin.
- managing privacy breaches, security incidents, reporting obligations, corrective actions, and notifications to the affected individuals and the IPC where required,
- maintaining documentation and evidence demonstrating compliance for audits, reviews, investigations, and annual reporting,
- working with the Information and Privacy Commissioner of Ontario in their investigation of privacy breaches if requested.

14.5 **DIU Member**

Accountable for:

- performing authorized data integration activities in compliance with all applicable legal, privacy, security and operational requirements, policies and standards,
- following established DIU policies, processes and procedures related to privacy, security, de-identification etc.,
- protecting personal information and de-identified information from unauthorized access, use, disclosure, modification, loss or destruction,
- immediately reporting actual or suspected:
 - Privacy breaches
 - Security incidents
 - Operational deficiencies
 - Instances of non-compliance with Part III.1 of FIPPA, the Standards, applicable legislation, policies, standards,
- completing mandatory privacy training on the requirements and best practices for data integration,
- participating in audits, reviews, and investigations if required.

14.6 Chief Digital and Data Officer

Accountable for:

- establishing, maintaining and overseeing the Standards,
- identifying and designating an ADM-level role accountable for fulfilling these responsibilities. If no ADM is delegated, these responsibilities remain with CDDO,
- providing enterprise-wide direction, guidance, and governance for the DIUs,
- receiving and reviewing annual compliance attestations from DIUs,
- supporting the implementation of these Standards, including providing frameworks, advice, standards, guidance, and tools as required,
- requesting information from the DIUs, as needed, to support the CDDO in the annual reporting to the IPC.
- reporting to the IPC on the DIU activities on an annual basis or as required,
- overseeing the periodic review of the Standards and propose updates as required.

14.7 Chief Information Officer(s) (CIO)

Responsible for:

- ensuring information and data-related risks, design considerations and requirements such as privacy protection, information security, access and recordkeeping are integrated into the design of ministry technology projects and procurements and are subsequently operationalized and monitored,
- ensuring that recordkeeping, access and privacy considerations and requirements are integrated into the IT project governance processes for designing and delivering IT systems, services and products, including when procuring third-party products,
- providing business owners with technical and logistical support necessary to implement this policy,
- supporting the planning and implementation of content management systems, and provide ongoing support where deployed,
- provide all support necessary for the administration and management of the information technology components of the ministry's IT systems so that recordkeeping, access and privacy obligations may be met.

14.8 **Chief Information Security Officer (CISO)**

Responsible for:

- providing enterprise direction, standards, and guidance related to cyber security for DIUs,
- supporting the identification, assessment, and mitigation of security and cyber risks associated with data integration activities,
- supporting security assessments, incident response activities, and remediation efforts related to DIU operations,
- advising on security safeguards and controls required to protect personal and de-identified information.

14.9 **Information and Privacy Commissioner of Ontario (IPC)**

Accountable for:

- providing independent oversight and assessing whether the requirements of Part III.1 of FIPPA and the Standards are being complied with, as necessary,
- requiring corrective actions, where authorized under Part III.1 of FIPPA, to address non-compliance identified through reviews and investigations,
- making comments or recommendations on the privacy implications of any matter related to Part III.1 of FIPPA and the Standards.

Appendix A: Related Legislation, Policies, Standards, and Guidelines

This appendix provides a non-exhaustive list of key legislation, regulations, policy instruments, standards, directives, and guidelines that inform and support the work of the DIUs.

Legislation	• <i>Anti-Racism Act, 2017.</i> • <i>Archives and Recordkeeping Act, 2006.</i> • <i>Child, Youth and Family Services Act, 2017 (Part X).</i> • <i>Enhancing Digital Security and Trust Act, 2024.</i> • <i>Personal Health Information Protection Act, 2004.</i>
Regulations	• O. Reg. 366/19 Data Integration under FIPPA • R.R.O. 1990, Reg. 460: General under FIPPA • R.R.O. 1990, Reg. 459: Disposal of Personal Information under FIPPA
Related Policy Instruments	• Corporate Policy on Recordkeeping, Access and Privacy. • Corporate Policy on Cyber Security and Cyber Risk Management (CSCRM). • Corporate Policy on Information Sensitivity Classification (ISC). • Corporate Policy on the Government of Ontario's Identity and Credential Assurance (GO-ICA). • Government of Ontario Public Key Infrastructure Policy (GO-PKI). • Digital and Data Directive. • Acceptable Use of Information Technology (IT) Resources Policy. • Governance and Management of Information Technology Directive. • Governance and Management of Information and Data Assets Directive.
OPS Risk Management Resources	• Enterprise Risk Management Directive. • OPS Risk Assessment Methodology.

OPS Security Standards	• GO-ITS 25.0 General Security Requirements. • GO-ITS 25.1 Security Requirements for Routers and Switches. • GO-ITS 25.5 Security Requirements for Wireless LANs. • GO-ITS 25.6 Security Requirements for Firewalls. • GO-ITS 25.7 Security Requirements for Remote Access Services. • GO-ITS 25.8 Security Requirements for Servers. • GO-ITS 25.10 Security Requirements for Mobile Devices. • GO-ITS 25.11 Security Design Requirements. • GO-ITS 25.12 Security Requirements for the Use of Cryptography. • GO-ITS 25.13 Security Requirements for Web Applications. • GO-ITS 25.18 Data Centre Physical Security Standards. • GO-ITS 25.20 Disposal, Loss and Incident Reporting of Computerized Devices and Digital Storage Media. • GO-ITS 25.21 Cloud First Principles and Security Requirements. • GO-ITS 35 Ontario Public Service Enterprise Change Management Standard. • GO-ITS 37 Enterprise Incident Management Process. • GO-ITS 42 Security Requirements for Enterprise Vulnerability Management.
Related OPS Standards	• Anti-Racism Data Standards – Data Standards for the Identification and Monitoring of Systemic Racism.
OPS Guidance	• OPS Guidance on Completing Privacy Impact Assessments (PIA) for Freedom of Information and Protection of Privacy Act (FIPPA) Institution (2025). • OPS Guidance on Privacy Breach Reporting for Freedom of Information and Protection of Privacy Act (FIPPA) Institution (2025).
IPC Guidance	• IPC De-identification Guidelines for Structured Data (2025). • IPC Planning for Success: Privacy Impact Assessment Guide for Ontario's public institutions (2025).