Ontario

Normes d’intégration des données de la fonction publique de l’Ontario

Ministère des Services gouvernementaux et des Services aux consommateurs
Avril 2021

Ontario

Table des matières

INTRODUCTION 1
EXIGENCES GÉNÉRALES 5
COLLECTE, UTILISATION ET DIVULGATION 15
CONSERVATION ET TRANSFERT EN TOUTE SÉCURITÉ 28
ÉLIMINATION ET DESTRUCTION EN TOUTE SÉCURITÉ 44
PÉRIODE DE CONSERVATION 48
ANONYMISATION ET ÉTABLISSEMENT DE LIENS 52
AVIS PUBLIC ET RAPPORT ANNUEL 56
GLOSSAIRE DES TERMES 65

HISTORIQUE DU DOCUMENT

Date	Conclusion
Avril 2021	Création : Normes de données d’intégration des données de la fonction publique de l’Ontario v1.0

Ontario

NORMES D'INTÉGRATION DES DONNÉES DES SERVICES PUBLICS DE L'ONTARIO

INTRODUCTION

La Partie III.1 Intégration des données (la « Partie ») de la *Loi de 1990 sur l'accès à l'information et la protection de la vie privée* (la *Loi sur l'AIPVP*) permet au gouvernement de l'Ontario et à d'autres organisations désignées de mieux exploiter l'information entre les ministères et les autres organisations financées par les fonds publics. Elle permet le développement et l'intégration d'ensembles de données intersectorielles et sectorielles afin de mieux comprendre comment les programmes et services gouvernementaux peuvent être mieux fournis aux Ontariens.

Ces dispositions relatives à l'intégration des données ont été introduites en 2019 et fournissent au gouvernement les outils nécessaires pour créer un service public davantage axé sur les données. Cette Partie prévoit la désignation de services ministériels d'intégration des données, de services interministériels d'intégration des données et de services extraministériels d'intégration des données (collectivement appelées « services d'intégration des données »). En vertu de cette Partie, les services d'intégration des données peuvent indirectement recueillir des renseignements personnels (RP) pour établir des liens afin de créer et de permettre l'accès à des ensembles de données anonymisées à des fins d'analyse en relation avec :

- la gestion ou l'affectation des ressources;
- la planification de la prestation des programmes et des services fournis ou financés par le gouvernement de l'Ontario;
- l'évaluation de ces programmes et services.

Compte tenu de ces autorités, il est primordial de maintenir la confiance du public et de s'assurer que les services d'intégration des données agissent de manière responsable pour le succès de la Partie. Pour garantir la transparence, la responsabilité et la protection de la vie privée, la Partie prévoit un ensemble de règles et de garanties qui régissent la manière dont les services d'intégration des données recueillent, établissent des liens, utilisent, divulguent, anonymisent, conservent, transfèrent et éliminent les RP. De plus, elle définit un rôle de surveillance pour le commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP), qui est chargé d'examiner les pratiques et les procédures des services d'intégration des données, entre autres.

Pour affiner et déterminer davantage son ensemble de règles et de garanties, la Partie exige l'élaboration de normes relatives aux données, qui sont énoncées dans le présent document (les « normes relatives aux données »). Ces normes contiennent un ensemble minimum d'exigences pour promouvoir une gestion responsable des RP tout au long de son cycle de vie dans le cadre de la Partie. En complétant les exigences de la Partie, les normes relatives aux données garantissent une approche cohérente et efficace de la transparence, de la responsabilité et de la protection de la vie privée dans tous les services d'intégration des données. Dans certains cas, les services d'intégration des données peuvent être tenus d'aller

au-delà des protections particulières prévues dans les normes relatives aux données afin de satisfaire aux obligations plus larges imposées par la Partie.

Les normes relatives aux données sont réparties dans les catégories suivantes :

1. Exigences générales
2. Collecte, utilisation et divulgation
3. Conservation et transfert en toute sécurité
4. Élimination et destruction en toute sécurité
5. Période de conservation
6. Anonymisation et établissement de liens
7. Avis public et rapport annuel

LES TYPES DE RENSEIGNEMENTS SOUMIS AUX NORMES RELATIVES AUX DONNÉES

Les normes de données s'appliquent aux RP tout au long de son cycle de vie dans le cadre de la Partie. Toutefois, il est important de clarifier les types de RP ainsi que les étapes du cycle de vie qui sont incluses.

Le cycle de vie des RP dans le cadre de la Partie comprend son anonymisation à différents niveaux. Le processus d'anonymisation implique la création de renseignements se situant sur un spectre d'identifiabilité entre le RP original collecté par les services d'intégration des données et les renseignements qui ont été anonymisés à un seuil acceptable avant qu'ils puissent être mis à disposition par les services d'intégration des données pour analyse. Aux fins des présentes normes relatives aux données, les « renseignements codés » désignent les renseignements inclus dans ce spectre.

Les renseignements codés peuvent techniquement être compris comme un type de renseignements rendus anonymes. Les renseignements codés sont des RP dont les identifiants directs ont été supprimés et remplacés par un code interne propre à la personne. Les identifiants directs ne sont pas perdus, mais sont séparés et gardés en sécurité par les services d'intégration des données. Dans la mesure où les services d'intégration des données peuvent récupérer les renseignements codés grâce à un code interne, ils sont considérés comme plus proches des RP d'origine sur le spectre d'identifiabilité. Par conséquent, ils sont généralement traités de la même manière que les RP et, entre autres, ils sont soumis aux droits individuels d'accès et de correction de RP en vertu de la *Loi sur l'AIPVP*. Les services d'intégration des données conservent les renseignements codés afin de préparer des ensembles de données qui seront finalement entièrement anonymisés et mis à disposition pour analyse. Afin de protéger les renseignements codés des risques liés à une désanonymisation non autorisée, de nombreuses exigences relatives aux normes de données doivent s'appliquer à la fois aux RP et aux renseignements codés.

Les renseignements codés entre les mains d'une personne, d'une entité ou d'une organisation qui n'a pas accès aux identifiants directs peuvent ou non être considérés comme anonymisés. Les renseignements sont anonymisés lorsqu'ils sont dépouillés de toute information permettant d'identifier une personne et qui pourrait être utilisée, seule ou avec d'autres renseignements, pour identifier une personne selon ce qui est raisonnablement prévisible dans

les circonstances. Le fait de déterminer si les RP ont été anonymisés à un seuil acceptable pour diffusion dépend du contexte et des garanties. Des renseignements peuvent être considérés comme anonymisés dans un certain contexte avec des garanties précises en place (p. ex., s'ils sont communiqués à une autre partie du même Ministère pour analyse dans un environnement strictement contrôlé), mais identifiables dans un contexte différent sans ces garanties (p. ex., s'ils sont communiqués au public sans aucun contrôle en place).

Même les renseignements anonymisés présentent un risque résiduel de désanonymisation. Par conséquent, pour protéger la vie privée, les normes relatives aux données s'appliquent à certains renseignements anonymisés dans certains contextes afin de les protéger contre les risques raisonnablement prévisibles de désanonymisation. Par exemple, des restrictions s'appliquent à la diffusion de renseignements anonymisés en dehors des services d'intégration des données. De même, les normes relatives à la conservation, au transfert et à l'élimination/la destruction en toute sécurité, à l'anonymisation et à l'établissement de liens, ainsi qu'aux atteintes à la vie privée et à la sécurité, doivent également être interprétés comme protégeant les renseignements anonymisés des risques raisonnablement prévisibles de désanonymisation.

Toutefois, sous réserve de l'exigence selon laquelle aucune personne ou entité ne doit utiliser ou tenter d'utiliser des renseignements qui ont été anonymisés en vertu de la Partie pour identifier un particulier, la réglementation des renseignements anonymisés dans les normes relatives aux données ne devrait pas étouffer la diffusion de renseignements statistiques généraux. À ce titre, les normes relatives aux données ne doivent pas être interprétées comme imposant des restrictions sur les renseignements qui ont été anonymisés dans la mesure nécessaire pour une diffusion au public. Cela garantit que les normes relatives aux données ne réglementent pas indûment la diffusion publique de renseignements statistiques généraux ou de données ouvertes, lorsque les renseignements sont suffisamment anonymisés et mis à la disposition de quiconque pour être téléchargés ou utilisés sans aucune condition.

RENSEIGNEMENTS PERSONNELS SUR LA SANTÉ

En vertu de la *Loi sur l'AIPVP*, la définition des RP comprend des renseignements sur les antécédents médicaux, psychiatriques ou psychologiques d'un particulier. La Partie permet également la collecte de renseignements personnels sur la santé auprès de personnes et d'entités régies par la *Loi de 2004 sur la protection des renseignements personnels sur la santé*, dans des circonstances limitées. Ainsi, les références aux RP dans le cadre des normes relatives aux données comprennent des renseignements personnels sur la santé d'une personne, à moins que le contexte n'indique le contraire.

AUTORITÉ LÉGALE

Les normes relatives aux données sont élaborées par le ministre responsable, c.-à-d. le ministre du gouvernement et des services aux consommateurs. L'alinéa 49.14(1)(a) de la *Loi sur l'AIPVP* exige que le ministre prépare un projet de normes relatives aux données, notamment des pratiques et des procédures (Pratiques et procédures) à adopter lors de la collecte, de l'utilisation et de la divulgation des RP, de l'anonymisation et de l'établissement de liens avec des RP, de la présentation de rapports publics sur l'utilisation des RP, de la conservation et de l'élimination en toute sécurité des RP conformément à la Partie. Ces normes relatives aux données ont été fournies au CIPPV et approuvées par ce dernier en vertu de l'alinéa 49.14(1)(b)[1].

Afin de faire preuve de diligence raisonnable et de fournir des preuves de conformité, les normes relatives aux données éclairent l'élaboration et la mise en œuvre nécessaires de mesures de reddition de comptes et de garanties administratives sous la forme de pratiques et de procédures. À ce titre, les normes relatives aux données comprennent des exigences en matière de pratiques et de procédures qui doivent être abordées au sein de chaque service d'intégration des données.

APPLICATION

Comme le stipule le paragraphe 49.14(4) de la *Loi sur l'AIPVP*, tous les membres de tous les services d'intégration des données doivent se conformer aux normes relatives aux données. Tous les membres doivent également se conformer à la Partie, aux pratiques et procédures élaborées et mises en œuvre par leur service d'intégration des données, aux autres dispositions applicables de la *Loi sur l'AIPVP* et de ses règlements, ainsi qu'aux accords et reconnaissances conclus en vertu de ceux-ci.

[1] Voir https://www.ipc.on.ca/decisions/integration-des-donnees?lang=fr

EXIGENCES GÉNÉRALES

Cette norme décrit les exigences générales pour les services d'intégration des données afin de garantir que toutes les normes relatives aux données sont effectivement mises en œuvre et correctement documentées. Les mesures de reddition de comptes et les exigences de formation visent à améliorer la conformité et la cohérence des pratiques, ainsi qu'à maintenir l'intégrité opérationnelle dans tous les services d'intégration des données.

L'objectif de la mise en œuvre des normes relatives aux données est de créer un cadre de gouvernance et de reddition de comptes en matière de protection de la vie privée. Ce cadre permet aux services d'intégration des données d'avoir une approche globale, efficace et cohérente pour prévenir, déterminer, examiner, consigner, suivre, examiner et résoudre les cas de non-conformité ou les risques de non-conformité avec :

- la Partie;
- les normes relatives aux données;
- les pratiques et procédures;
- les autres dispositions applicables de la *Loi sur l'AIPVP* et de ses règlements;
- les accords et les reconnaissances faits en vertu de ceux-ci.

Un élément essentiel de ce cadre, tel que défini dans les normes relatives aux données, est le suivi ou l'enregistrement cohérent et systématique de toutes les conclusions et recommandations résultant des examens, évaluations et enquêtes des services d'intégration des données pour s'assurer qu'elles sont traitées en temps opportun.

EXIGENCES ABOLUES

Pour s'assurer que les services d'intégration de données se conforment à la Partie, les services d'intégration de données doivent :

1. élaborer, documenter et mettre en œuvre des pratiques et des procédures qui répondent à chacune des exigences énoncées dans la Partie, ses règlements et les normes relatives aux données.
2. offrir à tous les membres une formation initiale et annuelle de sensibilisation à la protection de la vie privée et à la sécurité.
3. déterminer et définir un processus impartial permettant aux membres de signaler les lacunes ou insuffisances opérationnelles, ainsi que les cas réels ou présumés de non-conformité des autres membres.
4. effectuer une évaluation des facteurs relatifs à la vie privée (EFVP) afin de déterminer, d'analyser et d'atténuer les risques éventuels pour la vie privée, le cas échéant.

DISPOSITIONS PERTINENTES DE LA PARTIE

Ces exigences générales sont décrites conformément aux dispositions suivantes de la Partie :

- Pratiques et procédures – art. 49.12
- Normes relatives aux données – alinéa 49.14(1)(a)

EXIGENCES PARTICULIÈRES

Exigences 1 : Élaborer, documenter et mettre en œuvre des pratiques et des procédures qui répondent à chacune des exigences énoncées dans la Partie, ses règlements et les normes relatives aux données.	
1.1	Pour chaque exigence énoncée dans la Partie, ses règlements et les normes relatives aux données, décrire ce qui suit dans les Pratiques et procédures : 1. les lignes hiérarchiques des membres, leurs fonctions, leurs rôles, toute délégation de pouvoir et le rôle du membre responsable du respect de l'exigence; 2. les structures internes de reddition de comptes, les processus et les exigences d'approbation, notamment le rôle du membre ayant le pouvoir d'accorder l'approbation, et comment et à qui cette approbation sera communiquée; 3. l'obligation de documenter les décisions relatives aux RP et/ou aux renseignements codés; 4. le contenu minimum de la documentation, y compris les avis/notifications, les renseignements, les accords, les reconnaissances et les certificats qui doivent être remplis, fournis ou faits, par qui, et comment et à qui ils doivent être communiqués; 5. le contenu minimum et la méthode, la nature et le format des communications; 6. les délais applicables; 7. les mesures correctives à prendre lorsque l'obligation de retourner un article ou un renseignement, ou d'obtenir ou de fournir un avis, un renseignement, un accord, une reconnaissance ou un certificat, n'est pas respectée.
1.2	**1.2.1** Se conformer à la Partie, aux normes relatives aux données, aux pratiques et procédures, aux autres dispositions applicables de la *Loi sur l'AIPVP* et de ses règlements, ainsi qu'aux accords et reconnaissances faits en vertu de ceux-ci. Cette exigence s'applique à tous les membres et à toutes les activités des services d'intégration des données. **1.2.2** Les services d'intégration des données doivent exercer leur pouvoir discrétionnaire d'une manière qui soit raisonnable dans les circonstances, lorsqu'une exigence donne aux services d'intégration des données le pouvoir discrétionnaire de déterminer comment elle sera mise en œuvre.

1.3	**1.3.1** Les services d'intégration des données doivent examiner en interne tout registre, toute liste, tout inventaire ou toute documentation qu'ils sont tenus d'élaborer et de tenir à jour en vertu des normes relatives aux données afin de s'assurer qu'il ou elle est à jour et de détecter les cas de non-conformité ou les risques de non-conformité aux exigences pertinentes. Ces examens doivent être effectués périodiquement, ou comme indiqué dans les normes relatives aux données. **Note :** Cette exigence s'applique aux exigences suivantes : 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 et 27.3. **1.3.2** Lorsqu'un examen interne d'un registre, d'une liste, d'un inventaire ou d'une documentation particulière détermine un cas de non-conformité ou un risque de non-conformité, il faut y remédier en temps opportun. **1.3.3** Les services d'intégration des données doivent documenter ces examens, notamment les suivants : 1. le registre, la liste, l'inventaire ou la documentation examinés; 2. la date de l'examen interne; 3. le(s) nom(s) du (des) membre(s) chargé(s) de réaliser l'examen; 4. tout cas de non-conformité ou tout risque de non-conformité détecté; 5. les recommandations découlant de l'examen; 6. le(s) nom(s) du (des) membre(s) chargé(s) de traiter chaque recommandation; 7. la date à laquelle chaque recommandation a été, ou devrait être, traitée; 8. comment chaque recommandation a été, ou devrait être, traitée.
1.4	**1.4.1.** En plus de l'examen des registres, des listes, des inventaires et des documents particuliers conformément à l'exigence 1.3, effectuer un examen interne des pratiques et procédures et de leur mise en œuvre, au moins une fois tous les trois ans, pour s'assurer de ce qui suit : 1. Ils sont à jour; 2. Ils continuent à répondre à chacune des exigences énoncées dans la Partie, à ses règlements, aux normes relatives aux données, et aux accords et reconnaissances faits en vertu de ces derniers; 3. Il existe une cohésion entre les pratiques et procédures mises en œuvre au sein des services d'intégration des données; 4. Les recommandations découlant des examens, des évaluations et des enquêtes sont mises en œuvre en temps opportun; 5. Le service d'intégration des données et ses membres se conforment à la Partie, à ses règlements, aux normes relatives aux données, aux pratiques et aux procédures, ainsi qu'à tout accord et toute reconnaissance faits en vertu de ceux-ci.

	1.4.2. Réviser les pratiques et procédures afin de répondre à toute recommandation découlant de l'examen interne des pratiques et procédures et de leur mise en œuvre en temps opportun.
1.5	**1.5.1** Élaborer et tenir à jour un registre des examens internes effectués sur les pratiques et procédures et leur mise en œuvre. **1.5.2** Le registre doit au moins inclure ce qui suit : 1. la nature, l'étendue et le type de l'examen effectué, notamment la manière dont l'échantillonnage a été effectué; 2. la date à laquelle l'examen a été effectué; 3. le(s) nom(s) du (des) membre(s) chargé(s) de réaliser l'examen; 4. tout cas de non-conformité ou tout risque de non-conformité détecté; 5. les recommandations découlant de l'examen; 6. le(s) nom(s) du (des) membre(s) chargé(s) de traiter chaque recommandation; 7. la date à laquelle chaque recommandation a été, ou devrait être, traitée; 8. comment chaque recommandation a été, ou devrait être, traitée.

Exigences 2 : Offrir à tous les membres une formation initiale et annuelle de sensibilisation à la protection de la vie privée et à la sécurité.	
2.1	**2.1.1** Exiger de tous les membres qu'ils suivent une formation complète et à jour de sensibilisation à la protection de la vie privée et à la sécurité au début de leur emploi, de leur relation contractuelle ou autre avec les services d'intégration des données et, par la suite, au moins une fois par an, pour comprendre leurs obligations en vertu de la *Loi sur l'AIPVP*, notamment les suivantes : 1. la Partie; 2. les normes relatives aux données; 3. les pratiques et procédures; 4. les autres dispositions applicables de la *Loi sur l'AIPVP* et de ses règlements; 5. les accords et les reconnaissances faites en vertu de ceux-ci. **2.1.2** La formation doit comprendre au minimum ce qui suit : 1. La définition des RP, des renseignements codés et des renseignements anonymisés; 2. L'autorité pour la collecte, l'utilisation et la divulgation des RP et des renseignements codés; 3. Les fins pour lesquelles il est permis de recueillir, d'utiliser et de divulguer des RP, des renseignements codés et des renseignements anonymisés, ainsi que toutes les limitations, conditions et restrictions applicables; 4. La nature des renseignements recueillis par le service d'intégration des données et auprès de qui ces renseignements sont généralement recueillis;

	5. Les procédures à suivre lors de la divulgation de RP, de renseignements codés et de renseignements anonymisés en dehors du service d'intégration des données; 6. Les devoirs et responsabilités du membre concernant les atteintes à la vie privée et à la sécurité et les conséquences de leur non-respect; 7. Les mesures de protection administratives, techniques et physiques mises en place pour protéger les RP et les renseignements codés contre le vol, la perte et l'utilisation ou la divulgation non autorisée, notamment la manière sécurisée dont ces renseignements doivent être conservés, transférés et éliminés ou détruits; 8. Les devoirs et responsabilités liés à la mise en œuvre de ces garanties administratives, techniques et physiques; 9. Les interdictions suivantes, pour les membres : a. collecter et utiliser des RP, des renseignements codés et des renseignements anonymisés, sauf dans les cas autorisés par l'entente de confidentialité que les membres doivent signer; b. divulguer ces renseignements, sauf si l'entente de confidentialité le permet ou si la loi l'exige; 10. Le processus à suivre dans les cas suivants : a. Les renseignements anonymisés sont divulgués en vertu d'un droit d'accès prévu à l'article 10 de la *Loi sur l'AIPVP*; b. Les RP ou les renseignements codés sont divulgués en vertu des droits d'accès et de correction prévus à l'article 47 de la *Loi sur l'AIPVP;* 11. Les limites de l'utilisation de renseignements anonymisés conformément à l'article 49.8 de la Partie. **2.1.3** Le contenu de la formation doit être en rapport avec les fonctions particulières des membres afin de s'assurer que ces derniers comprennent comment appliquer les pratiques et procédures dans leur emploi quotidien, leurs relations contractuelles ou autres avec les services d'intégration des données.
2.2	Ne permettre aux membres d'accéder à l'environnement d'intégration des données qu'après avoir suivi la formation initiale requise en matière de sensibilisation à la sécurité et à la protection de la vie privée.
2.3	Veiller à ce que le matériel de formation soit périodiquement révisé et mis à jour afin qu'il : 1. continue à répondre aux exigences définies dans la Partie, aux normes relatives aux données, aux pratiques et procédures, aux autres dispositions applicables de la *Loi sur l'AIPVP* et de ses règlements, ainsi qu'aux accords et reconnaissances faits en vertu de ceux-ci; 2. reflète toutes les conclusions et recommandations applicables résultant des examens, des évaluations et des enquêtes menés par les services d'intégration des données.

2.4	**2.4.1** Veiller à ce que les membres chargés de traiter les atteintes réelles ou présumées à la vie privée et à la sécurité, ou de mettre en œuvre le plan de continuité des opérations et de reprise après sinistre, effectuent périodiquement des exercices de simulation. Ces exercices sont menés à des fins de formation et pour déterminer les améliorations recommandées aux pratiques et procédures des services d'intégration des données. **2.4.2** Veiller à ce que toute recommandation découlant de ces exercices de simulation soit mise en œuvre en temps opportun.
2.5	**2.5.1** Élaborer et tenir un registre des formations de sensibilisation des membres à la protection de la vie privée et à la sécurité. **2.5.2** Le registre doit au moins inclure ce qui suit : 1. le nom de chaque membre; 2. la date à laquelle le membre a suivi la formation initiale sur la protection de la vie privée et la sécurité; 3. les dates auxquelles le membre a suivi une formation continue sur la protection de la vie privée et la sécurité.

Exigences 3 : Déterminer et définir un processus impartial permettant aux membres de signaler les lacunes ou insuffisances opérationnelles, ainsi que les cas réels ou présumés de non-conformité des autres membres.	
3.1	Le processus doit au moins permettre aux membres de déclarer : 1. les lacunes ou insuffisances des pratiques et procédures du service d'intégration des données, des processus opérationnels, des mesures et contrôles de sécurité et de protection de la vie privée et des structures de reddition des comptes; 2. les cas réels ou présumés de non-respect de la Partie par d'autres membres, des normes relatives aux données, des pratiques et procédures, des autres dispositions applicables de la *Loi sur l'AIPVP* et de ses règlements, et des accords et reconnaissances faits en vertu de ceux-ci. **Note :** L'objectif de ce processus est de définir la manière dont les membres peuvent exprimer leurs préoccupations concernant des actes répréhensibles réels ou présumés au sein des services d'intégration des données sans crainte ni risque de représailles.
3.2	**3.2.1** Veiller à ce que : 1. le processus de rapport soit confidentiel et détermine les rôles et responsabilités applicables ainsi que les prochaines étapes nécessaires pour répondre aux préoccupations soulevées en temps opportun;

	2. les rapports ne soient pas faits à une personne impliquée dans l'affaire ou ayant une autorité directe sur les personnes ou les activités des services d'intégration des données impliqués dans l'affaire ni réalisés par une telle personne. **3.2.2** Si les préoccupations donnent lieu à une atteinte réelle ou présumée à la vie privée ou à la sécurité, le service d'intégration des données doit répondre à la préoccupation conformément à l'exigence 14.
3.3	**3.3.1** Élaborer et tenir un registre des rapports des membres en vertu de l'exigence 3. **3.3.2** Le registre doit au moins inclure ce qui suit : 1. une description des lacunes ou des insuffisances ou des cas de non-conformité réels ou présumés signalés; 2. la date du rapport; 3. le(s) nom(s) du (des) membre(s) chargé(s) de donner suite au rapport; 4. les mesures prises en réponse au rapport, y compris les dates auxquelles elles ont été achevées ou devraient l'être.

Exigences 4 : Effectuer une évaluation de l'impact sur la protection de la vie privée (EIVP) afin de déterminer, d'analyser et d'atténuer les risques éventuels pour la vie privée, le cas échéant.	
4.1	**4.1.1** Déterminer et définir les circonstances ou les événements qui déclencheraient une EIVP ou la mise à jour d'une EIVP au sein des services d'intégration des données. **4.1.2** Il faut effectuer une EIVP au moins avant : 1. une nouvelle collecte de RP; 2. la mise en œuvre d'une nouvelle technologie, d'un nouveau programme, processus ou système lié aux activités des services d'intégration des données dans le cadre de la Partie qui pourrait porter atteinte à la vie privée des personnes ou à la confidentialité des renseignements. **4.1.3** Il faut effectuer une mise à jour de l'EIVP au moins avant : 1. un changement dans la collecte continue de RP; 2. une modification d'un programme, d'un processus, d'une technologie ou d'un système lié aux activités des services d'intégration des données dans le cadre de la Partie où la modification pourrait porter atteinte à la vie privée des personnes ou à la confidentialité des renseignements.

	Note : On parle de nouvelle collecte lorsque les RP sont collectés auprès d'une source pour la première fois. On parle de collecte continue lorsque les mêmes éléments de données des RP sont recueillis auprès de la même source sur une base définie (p. ex., les mêmes éléments de données de RP sont recueillis chaque mois pendant deux ans). Une nouvelle EIVP n'est pas nécessaire à chaque nouvelle instance d'une collection qui fait partie d'une collection en cours. Toutefois, si une collection de RP en cours doit être modifiée avant que le changement ne soit mis en œuvre, les services d'intégration des données doivent mettre à jour leur évaluation des risques en effectuant une analyse delta pour déterminer les nouveaux risques éventuels et les recommandations correspondantes (c.-à-d. les mesures d'atténuation). Si aucune EIVP n'a été réalisée auparavant sur le programme, le processus, la technologie ou le système à modifier, une nouvelle EIVP doit être réalisée. Bien que les EIVP soient généralement réalisées en relation avec les RP, il peut également y avoir des circonstances dans lesquelles une EIVP doit être réalisée en relation avec des renseignements codés ou anonymisés (p. ex., lorsqu'il y a un changement dans un programme, un processus, une technologie ou un système traitant des renseignements codés ou anonymisés qui peut créer de nouveaux risques pour la vie privée). Pour tenir compte de ces circonstances, le contenu minimum d'une EIVP comprend des références à des renseignements codés et anonymisés (le cas échéant).
4.2	**4.2.1** Déterminer et définir le contenu requis d'une EIVP. **4.2.2** Une EIVP doit au moins comprendre ce qui suit : 1. une description de la collection de RP et/ou du programme, du processus, de la technologie ou du système en question; 2. la nature et le type de RP, de renseignements codés et/ou de renseignements anonymisés recueillis, utilisés ou divulgués; 3. les sources des RP, les renseignements codés et/ou les renseignements anonymisés; 4. la ou les finalités pour lesquelles les RP, les renseignements codés et/ou les renseignements anonymisés sont recueillis, utilisés ou divulgués; 5. la raison pour laquelle les RP et/ou les renseignements codés sont nécessaires aux fins déterminées (c.-à-d. par opposition à la possibilité d'utiliser des renseignements anonymisés); 6. les flux de RP, de renseignements codés et/ou de renseignements anonymisés (c.-à-d. qui y aura accès, quand et dans quel but); 7. l'autorité légale pour chaque collecte, utilisation et divulgation déterminée dans l'EIVP; 8. toute limitation imposée à la collecte, à l'utilisation et/ou à la divulgation des RP, des renseignements codés et/ou des renseignements anonymisés;

	9. si les RP et/ou les renseignements codés sont ou seront liés à d'autres renseignements, la nature et la source de tout renseignement auquel ils seront liés, la manière dont les liens seront établis et la raison pour laquelle les liens sont nécessaires pour l'objectif déterminé; 10. si les RP et/ou les renseignements codés seront ou non anonymisés et le processus d'anonymisation; 11. la durée de conservation des renseignements codés et/ou des renseignements anonymisés des RP; 12. la manière sécurisée dont les RP et/ou les renseignements codés sont, ou seront, conservés, transférés et éliminés ou détruits; 13. les risques pour la vie privée des personnes ou la confidentialité des renseignements découlant de la collecte de RP et/ou du programme, du processus, de la technologie ou du système, et une évaluation des risques pour la vie privée ou la confidentialité; 14. des recommandations pour traiter et éliminer ou réduire les risques déterminés en matière de vie privée et/ou de confidentialité; 15. les mesures de protection administratives, techniques et physiques mises en œuvre ou proposées, pour se prémunir contre les risques liés à la vie privée et/ou à la confidentialité. **4.2.3** Donner la priorité aux recommandations résultant des EIVP et y donner suite afin de traiter et d'éliminer les risques liés à l'atteinte à la vie privée et/ou à la confidentialité en temps opportun.
4.3	**4.3.1** Élaborer et tenir un registre des EIVP réalisées ou en cours de réalisation au sein des services d'intégration des données. **4.3.2** Le registre doit au moins inclure ce qui suit : 1. une description de la collection de RP et/ou du programme, du processus, de la technologie ou du système en question; 2. la ou les dates auxquelles l'EIVP a été complétée ou mise à jour ou est censée être complétée ou mise à jour; 3. le(s) nom(s) du (des) membre(s) chargé(s) de compléter/mettre à jour ou d'assurer l'achèvement ou la mise à jour de l'EIVP; 4. les recommandations découlant de l'EIVP; 5. le(s) nom(s) du (des) membre(s) chargé(s) de traiter chaque recommandation; 6. la date à laquelle chaque recommandation a été, ou devrait être, traitée; 7. comment chaque recommandation a été, ou devrait être, traitée.
4.4	**4.4.1** Élaborer et tenir un registre de tous les cas où il est déterminé qu'une EIVP ne sera pas effectuée ou mise à jour en ce qui concerne les changements ou la mise en œuvre d'un programme, d'un processus, d'une technologie ou d'un système liés aux activités des services d'intégration des données en vertu de la Partie.

	4.4.2 Le registre doit au moins comprendre ce qui suit : 1. le programme, le processus, la technologie ou le système mis en œuvre ou modifié; 2. la date à laquelle la détermination a été faite; 3. la raison pour laquelle une EIVP n'a pas été réalisée ou mise à jour; 4. le(s) nom(s) du (des) membre(s) chargé(s) de faire cette détermination.

COLLECTE, UTILISATION ET DIVULGATION

Cette norme décrit les exigences minimales que les services d'intégration des données doivent respecter lors de la collecte, de l'utilisation et de la divulgation de RP, de renseignements codés et de renseignements anonymisés, le cas échéant. Les services d'intégration des données doivent prendre des mesures raisonnables pour assurer la protection de la vie privée, respecter leurs obligations légales et veiller à ce que les personnes, entités et organisations avec lesquelles ils interagissent fassent de même.

EXIGENCES ABOLUES

Pour s'assurer que les services d'intégration de données se conforment à la Partie, les services d'intégration de données doivent :

5. Recueillir, utiliser et divulguer des RP, des renseignements codés et/ou des renseignements anonymisés uniquement en conformité avec les exigences applicables de la Partie, les normes relatives aux données, les pratiques et procédures, les autres dispositions applicables de la *Loi sur l'AIPVP* et de ses règlements, et les accords et reconnaissances conclus en vertu de ceux-ci.
6. Exécuter une entente de partage de données ou obtenir un accusé de réception écrit lors de la collecte ou de la divulgation de RP, de renseignements codés et/ou de renseignements anonymisés, le cas échéant.

DISPOSITIONS PERTINENTES DE LA PARTIE

Les exigences relatives à la collecte, à l'utilisation et à la divulgation des RP, des renseignements codés et des renseignements anonymisés sont décrites conformément aux dispositions suivantes de la Partie :

- But de la collecte de renseignements personnels - art. 49.2
- Règles générales : renseignements personnels - par. 49.3(1)
  - Quantité de renseignements (2)
- Collecte de renseignements personnels - art. 49.4(1)
  - Collecte de renseignements personnels : service ministériel d'intégration des données (2)
  - Exigences supplémentaires (3)
  - Divulgation au service (4)
  - Incompatibilité (5)
  - Idem (5.1)
  - Collecte de renseignements exclus
- Restrictions sur la collecte - par. 49.5(1)
  - Collecte de renseignements personnels sur la santé (1.1)
  - Définitions (2)

- Établissement de liens et anonymisation - par. 49.6(1)
  - Idem (2)
- Restrictions en matière d'utilisation des renseignements personnels - par. 49.7(1)
  - Service extraministériel d'intégration des données (1.1)
  - Rapport sur l'utilisation (2)
- Restrictions en matière d'utilisation des renseignements anonymisés - art. 49.8
- Divulgation de renseignements personnels - sous-alinéa 49.9(1)
  - Exception (2)
- Avis de collecte - art. 49.10
- Normes relatives aux données - sous-alinéa 49.14(1)(a)(i)
- Règlements - par. 49.15(1)
  - Service interministériel d'intégration des données (2)

Autres dispositions pertinentes de la *Loi sur l'AIPVP* :

- Documents constitués dans le cadre de la Partie III.1 par. 10(1.1)
- Champ d'application de la Partie - Idem - par. 37(2)
- Demandes et mode d'accès (Exception : art. 25) - par. 48(2.1)

EXIGENCES PARTICULIÈRES

Exigences 5 : Recueillir, utiliser et divulguer des RP, des renseignements codés et/ou des renseignements anonymisés uniquement conformément aux exigences applicables de la Partie, aux normes relatives aux données, aux pratiques et procédures, aux autres dispositions applicables de la *Loi sur l'AIPVP* et de ses règlements, et aux accords et reconnaissances conclus en vertu de ceux-ci.	
Collecte	
5.1	Déterminer et définir : 1. les exigences et/ou conditions qui doivent être satisfaites pour permettre la collecte de RP et de renseignements codés, notamment toutes les exigences de la Partie, les normes relatives aux données, les pratiques et procédures, les autres dispositions applicables de la *Loi sur l'AIPVP* et de ses règlements, et les accords et reconnaissances faits en vertu de ceux-ci; 2. les types de personnes et d'entités auprès desquelles des RP et/ou des renseignements codés peuvent être recueillis; 3. le(s) but(s) pour lequel/lesquels des RP et/ou des renseignements codés sont recueillis; 4. toute restriction qui pourrait s'appliquer à la collecte de RP et/ou de renseignements codés.
5.2	Veiller à ce que les RP et/ou les renseignements codés ne soient recueillis que dans les cas suivants :

	1. Ils sont autorisés à des fins et dans des circonstances définies, et toutes les conditions, exigences et restrictions ont été respectées; 2. l'objectif de la collecte ne pourrait pas être atteint autrement par la collecte d'autres renseignements (comme la collecte de renseignements anonymisés); 3. on ne recueillera pas plus de RP et/ou de renseignements codés que ce qui est raisonnablement nécessaire pour atteindre les objectifs de la collecte; 4. le ministre ou une personne désignée par le ministre (ou le cadre supérieur dans le cas d'un service extraministériel d'intégration des données) a pris en compte les intérêts des personnes concernées en matière de protection de la vie privée et la manière dont leurs RP et/ou renseignements codés seront protégés; 5. le ministre ou une personne désignée par le ministre (ou l'officier supérieur dans le cas d'un service extraministériel d'intégration des données) a déterminé qu'il est dans l'intérêt public de collecter les RP et/ou les renseignements codés.
5.3	Élaborer et tenir à jour une description des éléments suivants : 1. la finalité pour laquelle les RP et/ou les renseignements codés sont recueillis; 2. la nature et le type de RP et/ou de renseignements codés recueillis; 3. les entités auprès desquelles des RP et/ou des renseignements codés sont recueillis (c.-à-d. la source); 4. les entités auprès desquelles des RP et/ou des renseignements codés ne peuvent être recueillis en vertu de l'article 49.5 de la Partie; 5. les moyens par lesquels les RP et/ou les renseignements codés sont recueillis (p. ex., par transfert sécurisé, par courrier électronique, par messagerie, etc.)
5.4	**5.4.1** Développer et maintenir un inventaire des RP et des renseignements codés au sein du service d'intégration des données. **5.4.2** L'inventaire doit au moins comprendre ce qui suit : 1. l'objectif de la collecte des RP ou des renseignements codés; 2. les éléments de données ou champs particuliers contenus dans les RP ou les renseignements codés (p. ex., sexe, date de naissance ou âge, dates d'événements, lieux, etc. ;) 3. la ou les source(s) des RP ou des renseignements codés; 4. la nécessité des RP ou des renseignements codés par rapport à l'objectif déterminé. **5.4.3** Il faut effectuer des examens internes de l'inventaire chaque année.

Usage	
5.5	Déterminer et définir : 1. les exigences et conditions qui doivent être satisfaites pour permettre l'utilisation de RP et/ou de renseignements codés, notamment toutes les exigences de la Partie, les normes relatives aux données, les pratiques et procédures, les autres dispositions applicables de la *Loi sur l'AIPVP* et de ses règlements, et les accords et reconnaissances faits en vertu de ceux-ci; 2. les fins pour lesquelles les RP et/ou les renseignements codés peuvent être utilisés, notamment l'utilisation des RP et/ou des renseignements codés dans le but de faciliter un droit d'accès et de correction en vertu de l'article 47 de la *Loi sur l'AIPVP*; 3. toute restriction qui pourrait s'appliquer à l'utilisation des RP et/ou des renseignements codés.
5.6	Veiller à ce que les RP et/ou les renseignements codés ne soient utilisés que dans les cas suivants : 1. À des fins et dans des circonstances définies, et toutes les conditions, exigences et restrictions ont été respectées; 2. Si le(s) but(s) de l'utilisation ne pouvaient pas être atteints autrement en utilisant d'autres renseignements (p. ex., en utilisant des renseignements anonymisés); 3. On n'utilisera plus de RP et/ou de renseignements codés sauf si cet usage est raisonnablement nécessaire pour atteindre le(s) but(s) de l'utilisation; 4. Il est limité au minimum nécessaire et aux RP et/ou renseignements codés les moins identifiables possibles pour l'exercice de leurs responsabilités en matière de RP; 5. Il est limité aux membres qui en ont besoin pour s'acquitter de leurs responsabilités au sein des services d'intégration des données; 6. La durée pendant laquelle l'utilisation est autorisée a été définie et ne dépassera pas un délai raisonnablement nécessaire pour atteindre l'objectif déterminé.
5.7	Interdire aux membres d'utiliser des renseignements codés, seuls ou avec d'autres renseignements, pour identifier une personne, sauf dans les cas expressément déterminés et définis dans l'exigence 5.5.

Divulgation	
5.8	Déterminer et définir : 1. les exigences et conditions qui doivent être satisfaites pour permettre la divulgation de RP, de renseignements codés et/ou de renseignements anonymisés, y compris toutes les exigences de la Partie, les normes relatives aux données, les pratiques et procédures, les autres dispositions applicables de la *Loi sur l'AIPVP* et de ses règlements, et les accords et reconnaissances faits en vertu de ceux-ci; 2. les types d'entités auxquelles des RP, des renseignements codés et/ou des renseignements anonymisés peuvent être divulgués; 3. la finalité pour laquelle les RP, les renseignements codés et/ou les renseignements anonymisés peuvent être divulgués; 4. Le processus à suivre dans les cas suivants : a. Les renseignements anonymisés sont divulgués en vertu d'un droit d'accès prévu à l'article 10 de la *Loi sur l'AIPVP*; b. Les RP et/ou les renseignements codés sont divulgués en vertu des droits d'accès et de correction prévus à l'article 47 de la *Loi sur l'AIPVP*.
5.9	Veiller à ce que les membres ne divulguent des RP, des renseignements codés et/ou des renseignements anonymisés que dans les cas suivants : 1. À des fins et dans des circonstances définies, et toutes les conditions, exigences et restrictions ont été respectées; 2. Dans le cas de RP et/ou de renseignements codés, l'objectif déterminé ne peut raisonnablement être atteint sans divulguer les RP et/ou les renseignements codés; 3. Pas plus de RP et/ou de renseignements codés ne seront divulgués que ce qui est raisonnablement nécessaire pour atteindre l'objectif déterminé. **Note :** Les services d'intégration des données peuvent divulguer des RP, des renseignements codés et/ou des renseignements anonymisés aux membres d'un même service d'intégration des données qui ont besoin d'accéder à ces renseignements dans l'exercice de leurs fonctions en vertu de la présente Partie. Les services d'intégration des données doivent aborder la question de la divulgation des RP et/ou des renseignements codés à leurs propres membres dans leurs pratiques et procédures élaborées pour les besoins particuliers à utiliser dans le cadre des exigences 5.5 à 5.7. Les exigences particulières d'utilisation prévues aux points 5.5 à 5.7 ne s'appliquent pas aux renseignements anonymisés. Ainsi, la divulgation de renseignements anonymisés aux membres peut, ou non, être traitée dans les conditions particulières d'utilisation, à la discrétion des services d'intégration des données.

Exigences 6 : Exécuter une entente de partage de données ou obtenir un accusé de réception écrit lors de la collecte ou de la divulgation de RP, de renseignements codés et/ou de renseignements anonymisés, le cas échéant.	
6.1	**6.1.1** Exécuter une entente de partage de données en ce qui concerne la collecte ou la divulgation de RP, de renseignements codés et/ou de renseignements anonymisés lorsqu'il est raisonnablement nécessaire de protéger la vie privée des personnes et la confidentialité des informations. **6.1.2** Une entente de partage de données est, au minimum, raisonnablement nécessaire et doit être exécutée dans les cas suivants : 1. la collecte de RP et/ou de renseignements codés auprès d'une source extérieure à la personne, l'entité ou l'organisation dans laquelle se trouvent les services d'intégration des données (p. ex., le ministère); 2. la divulgation de RP et/ou de renseignements codés à un autre service d'intégration des données en dehors de la personne, de l'entité ou de l'organisation dans laquelle le service d'intégration des données est situé; 3. la divulgation de RP et/ou de renseignements codés à un chercheur. **6.1.3** Les ententes de partage des données requises doivent être remplies, approuvées et exécutées avant que les RP, les renseignements codés et/ou les renseignements anonymisés ne soient recueillis ou divulgués. **Note :** Une entente de partage de données sera généralement exécutée lorsqu'un service d'intégration des données collecte ou divulgue des RP et/ou des renseignements codés. Toutefois, il peut y avoir des circonstances dans lesquelles une entente de partage de données doit être exécutée concernant la collecte ou la divulgation de renseignements anonymisés par un service d'intégration des données. Par exemple, lorsqu'il s'agit d'une mesure de protection administrative requise dans le cadre du processus d'anonymisation ou raisonnablement nécessaire dans les circonstances. Dans ces circonstances particulières impliquant des renseignements anonymisés, les exigences ci-dessous s'appliquent à la collecte ou à la divulgation de renseignements anonymisés par un service d'intégration des données.
6.2	**6.2.1** Déterminer et définir le contenu requis d'une entente de partage de données. Le contenu doit être conforme à l'avis de collecte de renseignements personnels dans la norme relative à l'avis public et aux rapports annuels. **6.2.2** L'entente de partage des données doit, au minimum, comprendre ce qui suit : 1. les parties à l'entente de partage des données et leurs rôles, notamment le nom de la partie qui collecte des RP, des renseignements codés et/ou des renseignements anonymisés, et de la partie qui divulgue des RP, des renseignements codés et/ou des renseignements anonymisés;

	2. une description du statut des services d'intégration des données en vertu de la *Loi sur l'AIPVP* et des devoirs et responsabilités découlant de ce statut, notamment les définitions des RP, des renseignements codés et de l'anonymisation; 3. l'autorité statutaire pour la collecte, l'utilisation et la divulgation déterminée dans l'entente de partage des données; 4. les détails de la RP, les renseignements codés et/ou les renseignements anonymisés à recueillir ou à divulguer; 5. la ou les sources des RP, des renseignements codés et/ou des renseignements anonymisés; 6. le ou les objectifs pour lesquels les RP, les renseignements codés et/ou les renseignements anonymisés seront recueillis ou divulgués; 7. la ou les fins auxquelles la RP, les renseignements codés et/ou les renseignements anonymisés seront utilisés, y compris s'ils seront liés à d'autres renseignements; 8. si les RP et/ou les renseignements codés seront liés à d'autres renseignements, la nature et la source de tout renseignement auquel ils seront liés, la manière dont les liens seront établis et la raison pour laquelle les liens sont nécessaires pour le ou les objectifs déterminés; 9. la période particulière au cours de laquelle la collecte ou la divulgation aura lieu (p. ex., chaque mois pendant deux ans); 10. la durée de conservation des RP, des renseignements codés et/ou des renseignements anonymisés; 11. si les RP et/ou les renseignements codés seront anonymisés et le processus d'anonymisation; 12. la manière précise dont les RP et/ou les renseignements codés seront conservés en toute sécurité, y compris s'ils seront conservés sous une forme identifiable; 13. le processus particulier qui sera utilisé pour transférer en toute sécurité (y compris le retour, le cas échéant) les RP, les renseignements codés et/ou les renseignements anonymisés; 14. si les RP, les renseignements codés et/ou les renseignements anonymisés seront renvoyés, éliminés ou détruits en toute sécurité après la période de conservation ou à la date de fin prévue dans l'entente de partage de données et le délai dans lequel cela doit être fait; 15. le processus particulier qui sera utilisé pour éliminer ou détruire en toute sécurité les RP, les renseignements codés et/ou les renseignements anonymisés; 16. une exigence selon laquelle les atteintes réelles ou présumées à la vie privée et à la sécurité liées à l'entente de partage de données doivent être signalées aux autres parties à l'entente de partage de données à la première occasion raisonnable, y compris la méthode de notification et les contacts clés; 17. une exigence selon laquelle des mesures raisonnables doivent être prises pour contenir les atteintes à la vie privée et à la sécurité liées à l'entente de partage de données;

	18. les conséquences des atteintes à la vie privée et à la sécurité et si la conformité à l'entente de partage de données fera l'objet d'un audit et, le cas échéant, le mode d'audit; 19. les conditions, exigences et restrictions pertinentes, notamment les suivantes : a. si les RP, les renseignements codés et/ou les renseignements anonymisés peuvent être divulgués par la partie collectrice; b. lorsque les RP, les renseignements codés et/ou les renseignements anonymisés peuvent être divulgués ultérieurement par la partie qui les collecte, les restrictions concernant l'utilisation et la divulgation ultérieures des RP, des renseignements codés et/ou des renseignements anonymisés; i. ces restrictions doivent, au minimum, prévoir que toute personne, entité ou organisation à laquelle des renseignements anonymisés sont communiqués ultérieurement s'engage à ne pas utiliser ces renseignements, seuls ou avec d'autres renseignements, pour identifier une personne; c. les RP, les renseignements codés et/ou les renseignements anonymisés ne seront conservés que le temps nécessaire pour atteindre les objectifs pour lesquels ils ont été collectés ou que la loi l'exige; d. les RP et/ou les renseignements codés recueillis ou divulgués en vertu d'une entente de partage de données doivent être nécessaires aux fins pour lesquelles ils ont été recueillis ou divulgués; e. Les RP et/ou les renseignements codés ne seront collectés, utilisés ou divulgués que si d'autres renseignements, à savoir des renseignements anonymisés, ne permettent pas d'atteindre l'objectif; f. il ne sera pas collecté, utilisé ou divulgué davantage de RP et/ou de renseignements codés que ce qui est raisonnablement nécessaire pour atteindre l'objectif; g. des mesures raisonnables seront prises pour protéger les RP et/ou les renseignements codés contre le vol, la perte et l'utilisation ou la divulgation non autorisée et les mesures raisonnables particulières qui doivent être prises; h. les renseignements anonymisés ne seront pas utilisés, seuls ou avec d'autres renseignements, pour identifier une personne; i. toutes les personnes qui auront accès aux RP et/ou aux renseignements codés connaissent et acceptent de respecter les conditions de l'entente de partage de données avant d'avoir accès aux RP et/ou aux renseignements codés.
6.3	**6.3.1** Créer et tenir un registre des ententes de partage de données exécutés par le service d'intégration des données. **6.3.2** Le registre doit au moins inclure ce qui suit :

	1. le nom de la personne, de l'entité ou de l'organisation auprès de laquelle les RP, les renseignements codés et/ou les renseignements anonymisés ont été recueillis, ou à laquelle les RP, les renseignements codés et/ou les renseignements anonymisés ont été divulgués; 2. la date à laquelle la collecte ou la divulgation des RP, des renseignements codés et/ou des renseignements anonymisés a été approuvée; 3. la date d'exécution de l'entente de partage de données; 4. la date à laquelle les RP, les renseignements codés et/ou les renseignements anonymisés ont été recueillis ou divulgués; 5. la nature des RP, des renseignements codés et/ou des renseignements anonymisés visés par l'entente de partage de données; 6. la période de conservation des RP, des renseignements codés et/ou des renseignements anonymisés déterminée dans l'entente de partage de données, ou la date de fin de l'entente de partage de données; 7. si les RP, les renseignements codés et/ou les renseignements anonymisés seront renvoyés en toute sécurité, ou seront éliminés ou détruits en toute sécurité, après la période de conservation ou la date de fin prévue dans l'entente de partage de données; 8. la date effective ou prévue à laquelle les RP, les renseignements codés et/ou les renseignements anonymisés sont renvoyés en toute sécurité ou éliminés ou détruits en toute sécurité.
6.4	**6.4.1** Lorsqu'une entente de partage de données n'est pas exécutée, obtenir une reconnaissance écrite en rapport avec une collecte ou une divulgation de RP, de renseignements codés et/ou de renseignements anonymisés lorsqu'il est raisonnablement nécessaire de protéger la vie privée des personnes et la confidentialité des renseignements. **6.4.2** Au minimum, une reconnaissance écrite est raisonnablement nécessaire et doit être obtenue dans les cas suivants : 1. Collecte de RP et/ou de renseignements codés à partir d'une zone située en dehors du service d'intégration des données, mais concernant la personne, l'entité ou l'organisation dans laquelle se trouve le service d'intégration des données; 2. Divulgation de renseignements anonymisés à un secteur extérieur au service d'intégration des données, mais concernant la personne, l'entité ou l'organisation dans laquelle se trouve le service d'intégration des données. **6.4.3** Un service d'intégration des données peut, ou non, exiger qu'une reconnaissance écrite soit officiellement exécutée (c.-à-d. signée), selon ce qui est raisonnablement nécessaire dans les circonstances. **6.4.4** La partie qui divulgue des RP, des renseignements codés et/ou des renseignements anonymisés au service d'intégration des données, ou qui recueille des RP, des renseignements codés et/ou des renseignements anonymisés auprès du

	service d'intégration des données, doit fournir une attestation écrite avant que les RP, les renseignements codés et/ou les renseignements anonymisés ne soient recueillis et/ou divulgués. **Note :** Outre les deux circonstances minimales particulières mentionnées ci-dessus dans lesquelles une reconnaissance écrite doit être obtenue, il peut y avoir d'autres circonstances dans lesquelles une reconnaissance écrite est raisonnablement nécessaire pour protéger la vie privée des personnes et la confidentialité des renseignements. Outre les deux circonstances minimales particulières mentionnées ci-dessus dans lesquelles une reconnaissance écrite doit être obtenue, il peut y avoir d'autres circonstances dans lesquelles une reconnaissance écrite est raisonnablement nécessaire pour protéger la vie privée des personnes et la confidentialité des renseignements.
6.5	**Accusé de réception écrit concernant : Collecte** **6.5.1** Déterminer et définir le contenu requis d'un accusé de réception écrit applicable à la collecte de RP, de renseignements codés et/ou de renseignements anonymisés par un service d'intégration des données. **6.5.2** Un accusé de réception écrit applicable à la collecte de RP, de renseignements codés et/ou de renseignements anonymisés par un service d'intégration des données doit au moins inclure (selon le cas) ce qui suit : 1. L'identification du service d'intégration des données qui collecte et de la personne, de l'entité ou de l'organisation (et la zone administrative de la personne, de l'entité ou de l'organisation si le service d'intégration des données correspond à la même personne, entité ou organisation) qui divulgue les RP; 2. Une description du rôle et des responsabilités du service d'intégration des données en vertu de la *Loi sur l'AIPVP* et une référence à l'autorité statutaire pour les collections et les utilisations déterminées (le cas échéant); 3. Une description générale du RP, des renseignements codés et/ou des renseignements anonymisés à recueillir (p. ex., dossiers scolaires, notes de l'école secondaire de l'Ontario de 2012 à 2014); 4. La période particulière pendant laquelle la collecte aura lieu (p. ex., tous les mois pendant deux ans); 5. La durée de conservation des RP, des renseignements codés et/ou des renseignements anonymisés; 6. La portée et l'objectif prévus de l'analyse des services d'intégration des données; 7. La méthode permettant de conserver, de transférer et d'éliminer ou de détruire en toute sécurité les RP, les renseignements codés ou les renseignements anonymisés; 8. Si les RP et/ou les renseignements codés seront liés à d'autres renseignements, la nature et la source de tout renseignement auquel ils seront

	liés, la manière dont les liens seront établis et la raison pour laquelle les liens sont nécessaires aux fins déterminées 9. Une déclaration dans laquelle se trouve les éléments suivants : a. Dans le cas des RP et/ou des renseignements codés, d'autres renseignements, à savoir des renseignements anonymisés, ne serviront pas; b. Il n'y aura pas plus de RP et/ou de renseignements codés que ce qui est raisonnablement nécessaire pour atteindre l'objectif; c. Toutes les personnes qui ont accès aux RP et/ou aux renseignements codés connaissent et acceptent de respecter les conditions de la reconnaissance écrite avant d'avoir accès aux RP et/ou aux renseignements codés.
6.6	**Accusé de réception écrit concernant : La divulgation** **6.6.1** Déterminer et définir le contenu requis d'un accusé de réception écrit lorsqu'un service d'intégration des données divulgue des RP, des renseignements codés et/ou des renseignements anonymisés. **6.6.2** Un accusé de réception écrit applicable à la divulgation de RP, de renseignements codés et/ou de renseignements anonymisés par un service d'intégration des données doit au moins inclure (selon le cas) : 1. l'identification du service d'intégration des données qui divulgue et de la personne, de l'entité ou de l'organisation (et de la zone administrative de la personne, de l'entité ou de l'organisation si le service d'intégration des données correspond à la même personne, entité ou organisation) qui collecte les RP, les renseignements codés et/ou les renseignements anonymisés; 2. une description du rôle et des responsabilités du service d'intégration des données en vertu de la *Loi sur l'AIPVP* et une référence à l'autorité statutaire pour les divulgations déterminées (le cas échéant); 3. une description générale des RP, des renseignements codés et/ou des renseignements anonymisés à divulguer (p. ex., dossiers scolaires, notes de l'école secondaire de l'Ontario de 2012 à 2014); 4. la ou les sources des RP, des renseignements codés et/ou des renseignements anonymisés; 5. la durée de conservation des RP, des renseignements codés et/ou des renseignements anonymisés; 6. la portée et la finalité prévues de l'utilisation des RP, des renseignements codés et/ou des renseignements anonymisés; 7. la méthode permettant de conserver, de transférer et d'éliminer ou de détruire en toute sécurité les RP, les renseignements codés et/ou les renseignements anonymisés; 8. Une déclaration dans laquelle se trouve les éléments suivants :

	a. dans le cas de RP et/ou de renseignements codés, d'autres renseignements (c.-à-d. des renseignements anonymisés) ne serviront pas l'objectif défini; b. la collecte et l'utilisation de RP et/ou de renseignements codés ne dépassent pas ce qui est raisonnablement nécessaire pour atteindre l'objectif; c. tout renseignement anonymisé ne servira pas, seul ou avec d'autres renseignements, à identifier une personne; 9. toutes les personnes qui ont accès aux RP et/ou aux renseignements codés connaissent et acceptent de respecter les conditions de la reconnaissance écrite avant d'avoir accès aux RP ou aux renseignements codés; 10. si les RP, les renseignements codés et/ou les renseignements anonymisés peuvent faire l'objet d'une divulgation ultérieure et, dans l'affirmative, l'accusé de réception écrit doit également : a. Comprendre les conditions dans lesquelles une telle divulgation peut avoir lieu; b. exiger que toute personne, entité ou organisation à laquelle les renseignements anonymisés sont divulgués ultérieurement accepte de ne pas utiliser ces renseignements, seuls ou avec d'autres renseignements, pour identifier une personne.
6.7	**6.7.1** Établir et tenir un registre des reconnaissances écrites obtenues par le service d'intégration des données. **6.7.2** Le registre doit au moins comprendre ce qui suit : 1. Le nom de la personne, de l'entité ou de l'organisation (y compris la zone administrative de la personne, de l'entité ou de l'organisation si le service d'intégration des données correspond à la même personne, entité ou organisation) auprès de laquelle les RP, les renseignements codés et/ou les renseignements anonymisés ont été recueillis ou divulgués; 2. Le nom de la personne qui a donné la reconnaissance écrite au nom de la personne, de l'entité ou de l'organisation; 3. Si des RP, des renseignements codés et/ou des renseignements anonymisés ont été recueillis ou divulgués; 4. La date à laquelle les RP, les renseignements codés et/ou les renseignements anonymisés ont été recueillis ou divulgués. 5. La nature des RP, des renseignements codés et/ou des renseignements anonymisés faisant l'objet de l'accusé de réception écrit.
6.8	Lorsqu'un service d'intégration des données divulgue des renseignements anonymisés sans avoir obtenu d'entente de partage des données en vertu de l'exigence 6.1 ou de la reconnaissance écrite en vertu de l'exigence 6.4, il doit exiger que la personne, l'entité ou l'organisation à laquelle les renseignements anonymisés seront divulgués confirme par écrit que les renseignements anonymisés ne seront pas utilisés, seuls ou avec d'autres renseignements, pour identifier une personne.

6.9	Les exigences 6.1, 6.4 et 6.8 ne s'appliquent pas aux cas suivants : 1. Un service d'intégration des données divulgue des RP, des renseignements codés et/ou des renseignements anonymisés à un membre du même service d'intégration des données qui doit avoir accès aux RP, aux renseignements codés et/ou aux renseignements anonymisés dans l'exercice de ses fonctions liées à la présente Partie; 2. Les renseignements à divulguer ont été anonymisés de sorte qu'ils puissent être communiqués au public; 3. Une personne exerce son droit d'accès en vertu de l'article 10 de la *Loi sur l'AIPVP* ou un particulier exerce ses droits d'accès et de correction en vertu de l'article 47 de *la Loi sur l'AIPVP*.

CONSERVATION ET TRANSFERT EN TOUTE SÉCURITÉ

La présente norme décrit les exigences que doivent respecter les services d'intégration des données pour mettre en place des mesures de protection afin de garantir un environnement technologique sécuritaire et protecteur pour la conservation et le transfert en toute sécurité des RP et des renseignements codés. Plus précisément, les services d'intégration des données doivent adopter des mesures de protection administratives, techniques et physiques pour protéger les composants du système et les renseignements de leur environnement d'intégration contre toute tentative d'attaque, d'atteinte ou d'accès non autorisé.

EXIGENCES ABOLUES

Pour assurer la conservation et le transfert en toute sécurité des RP et des renseignements codés en vertu de la Partie, les services d'intégration des données doivent :

7. s'assurer que l'environnement du service d'intégration des données n'est accessible qu'aux membres qui doivent y avoir accès dans l'exercice de leurs fonctions en vertu de la Partie.
8. mettre en œuvre des mesures de sécurité physique raisonnables compte tenu des circonstances pour protéger les RP et les renseignements codés contre le vol, la perte, l'utilisation et la divulgation non autorisées.
9. mettre en œuvre des mesures de sécurité raisonnables compte tenu des circonstances pour protéger les RP et les renseignements codés conservés et/ou transférés sous forme électronique contre le vol, la perte, l'utilisation et la divulgation non autorisées.
10. s'assurer que les RP et les renseignements codés ne sont accessibles à distance et/ou conservés sur des appareils mobiles que dans des circonstances approuvées.
11. mener des évaluations des menaces et des risques et conserver et revoir les registres d'audit tant que les circonstances le permettent.
12. mettre en place et en œuvre un processus pour gérer les changements de l'environnement du service d'intégration des données.
13. veiller à ce que les RP et les renseignements codés soient sauvegardés de manière à pouvoir être récupérés intégralement, et que le service d'intégration des données dispose d'un plan efficace de continuité des activités et de reprise après sinistre.
14. répondre aux atteintes à la vie privée et à la sécurité en temps opportun et de manière appropriée.

DISPOSITIONS PERTINENTES DE LA PARTIE

Les exigences relatives à la conservation et au transfert en toute sécurité des RP sont décrites conformément aux dispositions suivantes de la Partie :

- Sécurité et conservation - art. 49(11)(a à c)
  - Exigences en matière de sécurité (2)
  - Avis de vol ou de perte communiqué à un particulier (3)
  - Avis au commissaire (4)

- Normes relatives aux données - art. 49.14(1)(a)(iv)

EXIGENCES PARTICULIÈRES

Exigences 7 : S'assurer que l'environnement du service d'intégration des données n'est accessible qu'aux membres qui doivent y avoir accès dans l'exercice de leurs fonctions en vertu de la Partie.	
7.1	Déterminer et définir : 1. les rôles professionnels qui doivent accéder à l'environnement du service d'intégration des données dans l'exercice de leurs fonctions; 2. les responsabilités de ces rôles commerciaux; a. les rôles professionnels doivent au moins être séparés afin de garantir que les fonctions opérationnelles sont séparées des fonctions de sécurité et d'audit, de sorte qu'aucun membre ne dispose d'un contrôle de bout en bout sur un processus; i. lorsque les tâches ne peuvent pas être réparties entre plusieurs membres distincts en raison du manque de ressources humaines disponibles (p. ex., dans les petits services d'intégration des données), d'autres contrôles appropriés, comme la surveillance des activités et la supervision de la direction, doivent être renforcés pour obtenir le même; 3. les besoins d'accès de chaque rôle commercial à l'environnement du service d'intégration des données (y compris des parties de ce dernier); 4. le(s) rôle(s) professionnel(s) attribué(s) à chaque membre; 5. le niveau minimum de privilèges requis pour accéder à l'environnement du service d'intégration des données; 6. les exigences et les conditions qui doivent être satisfaites pour permettre l'accès à l'environnement du service d'intégration des données, notamment toutes les exigences de la Partie, les normes relatives aux données, les pratiques et procédures, les autres dispositions applicables de la *Loi sur l'AIPVP* et de ses règlements, ainsi que les ententes et les reconnaissances faits en vertu de ceux-ci; 7. les conditions et les restrictions imposées à chaque rôle commercial, telles que les limitations de lecture, de création, de mise à jour ou de suppression, et les circonstances dans lesquelles les conditions et les restrictions seront imposées; 8. les circonstances dans lesquelles l'accès sera approuvé, suspendu, révoqué ou autrement interrompu; 9. les fins pour lesquelles les membres sont autorisés et non autorisés à utiliser l'environnement du service d'intégration des données qui, au minimum, ne doit permettre que l'utilisation de l'environnement du service d'intégration des données pour les affaires du service d'intégration des données en vertu de la Partie et d'autres fins approuvées.

7.2	Veillez à ce que les membres n'accèdent à l'environnement du service d'intégration des données que dans les conditions suivantes : 1. L'accès est à des fins et dans des circonstances définies et toutes les conditions, exigences et restrictions ont été satisfaites; 2. Le but déterminé pour l'accès aux RP et/ou aux renseignements codés ne peut être atteint sans les RP et/ou les renseignements codés; 3. L'accès aux RP et/ou aux renseignements codés ne dépassera pas ce qui est raisonnablement nécessaire pour atteindre l'objectif déterminé; 4. Des mesures raisonnables compte tenu des circonstances ont été prises pour s'assurer que l'accès à l'environnement du service d'intégration des données est autorisé, notamment : a. l'attribution d'un seul membre à un nom d'utilisateur ou compte d'accès (c.-à-d. pas de partage de comptes entre les membres); b. établir des exigences en matière de force, de protection, d'utilisation, de confidentialité et de modification des mots de passe/phrases de passe; c. établir une procédure de traitement des échecs répétés de tentatives d'accès, notamment le nombre d'échecs qui entraînera un refus d'accès; d. établir un processus de traitement des sessions inactives, notamment la durée de l'inactivité qui nécessitera une réauthentification; e. établir des exigences pour l'utilisation de l'authentification multifactorielle; f. réexaminer et améliorer périodiquement la séparation des tâches entre les rôles professionnels, notamment en ce qui concerne la sécurité, l'administration des bases de données, l'anonymisation, l'établissement de liens et la collecte, l'utilisation et la divulgation des RP et/ou des renseignements codés; g. la révocation immédiate de l'accès lorsque l'emploi d'un membre, sa relation contractuelle ou autre avec le service d'intégration des données a pris fin, ou lorsqu'un examen détermine que les droits d'accès du membre à l'environnement d'intégration des données ou à une partie de celui-ci ne sont plus nécessaires.
7.3	**7.3.1** Créer et tenir à jour un registre des membres qui ont reçu l'autorisation d'accéder à l'environnement du service d'intégration des données. **7.3.2** Le registre doit au moins déterminer ce qui suit : 1. le nom de chaque membre; 2. le rôle professionnel attribué au membre; 3. le nom du membre qui a approuvé l'accès; 4. la date à laquelle l'accès a été accordé; 5. la date de résiliation ou la date de la prochaine révision de l'accès. **7.3.3** Il faut revoir le registre chaque année en interne.

	Remarque : Il peut s'agir d'un registre autonome ou d'une combinaison du registre des membres ayant un accès physique au service d'intégration des données, conformément à l'exigence 8.3, et du registre des membres autorisés à accéder à distance aux RP et aux renseignements codés ou à conserver des RP et des renseignements codés sur des dispositifs mobiles, conformément à l'exigence 10.3.
7.4	**7.4.1** Exiger des membres du service d'intégration des données qu'ils signent une entente de confidentialité au début de leur emploi, de leur contrat ou de toute autre relation avec le service d'intégration des données, puis tous les ans. **7.4.2** Les membres doivent respecter les termes de l'entente de confidentialité.
7.5	S'assurer que les accords de confidentialité signés par les membres contiennent des dispositions appropriées, notamment ce qui suit, au minium : 1. Le statut du service d'intégration des données en vertu de la *Loi sur l'AIPVP* et les devoirs et responsabilités découlant de ce statut, notamment les définitions de RP, de renseignements codés et d'anonymisation; 2. Les personnes qui exécutent l'entente de confidentialité sont membres du service d'intégration des données et décrire les responsabilités associées à ce statut; 3. L'obligation pour les membres de se conformer à la Partie, à ses règlements, aux normes relatives aux données, aux pratiques et aux procédures élaborées et mises en œuvre par le service d'intégration des données, aux autres dispositions applicables de la *Loi sur l'AIPVP* et de ses règlements, ainsi qu'aux accords et aux reconnaissances conclus en vertu de ceux-ci; 4. Une reconnaissance que les membres ont lu, compris et accepté de respecter les termes de l'entente de confidentialité; 5. Les fins pour lesquelles les membres sont autorisés à collecter, utiliser et divulguer des RP, des renseignements codés et/ou des renseignements anonymisés, ainsi que les limitations, conditions et restrictions éventuelles; 6. L'interdiction pour les membres de collecter, d'utiliser et de divulguer des RP, des renseignements codés et/ou des renseignements anonymisés, sauf dans les cas prévus par l'entente de confidentialité ou, en cas de divulgation, dans les cas prévus par la loi; 7. L'interdiction pour les membres de collecter, d'utiliser ou de divulguer des RP et/ou des renseignements codés si d'autres renseignements permettent d'atteindre l'objectif recherché, et l'interdiction de collecter, d'utiliser ou de divulguer plus de RP et/ou de renseignements codés que ce qui est raisonnablement nécessaire pour atteindre l'objectif recherché; 8. L'obligation des membres de retourner en toute sécurité tous les biens du service d'intégration des données, y compris les RP, les renseignements codés et les renseignements anonymisés, ainsi que tous les mécanismes d'accès physique (comme les cartes d'identification, les cartes d'accès et les

	clés), au plus tard à la date de cessation de l'emploi, du contrat ou de toute autre relation avec le service d'intégration des données ou lorsqu'un examen détermine que les biens ou les mécanismes d'accès physique ne sont plus nécessaires aux responsabilités du membre pour le service d'intégration des données; 9. L'obligation pour les membres d'informer le service d'intégration des données à la première occasion raisonnable d'une atteinte réelle ou présumée à la vie privée ou à la sécurité; 10. Le respect de l'entente de confidentialité fera l'objet d'un contrôle interne et indiquer la manière dont ce contrôle sera effectué; 11. Les sanctions appropriées pour les atteintes à la vie privée et à la sécurité commises par le membre, notamment le licenciement potentiel; 12. L'obligation des membres de faciliter l'exercice d'un droit d'accès en vertu de l'article 10 de la *Loi sur l'AIPVP* et les droits d'accès et de correction en vertu de l'article 47 de la *Loi sur l'AIPVP*; 13. L'interdiction pour les membres d'utiliser des renseignements anonymisés, seuls ou avec d'autres renseignements, pour identifier une personne.
7.6	N'autoriser les membres à accéder à l'environnement du service d'intégration des données qu'après avoir signé l'entente de confidentialité requis au début de leur emploi, de leur relation contractuelle ou autre avec le service d'intégration des données.
7.7	**7.7.1** Élaborer et tenir un registre des ententes de confidentialité exécutés au sein du service d'intégration des données. **7.7.2** Le registre doit au moins comprendre : 1. le nom de chaque membre; 2. les dates de début et de fin de leur emploi, de leur relation contractuelle ou autre avec le service d'intégration des données; 3. les dates auxquelles les ententes de confidentialité ont été exécutés.
7.8	**7.8.1** Le service d'intégration des données qui conclut un accord avec une personne, une entité ou un organisme qui fournit des services liés à la collecte, à l'établissement de liens, à l'utilisation, à la divulgation, à l'anonymisation, à la conservation, au transfert, à l'élimination ou à la destruction de RP, de renseignements codés ou de renseignements anonymisés, et qui n'est pas membre du service d'intégration des données, doit s'assurer qu'il signe un accord écrit avec cette personne, cette entité ou cet organisme. **7.8.2** L'accord écrit doit au moins contenir les restrictions déterminées dans la présente exigence :

	1. La personne, l'entité ou l'organisation ne doit pas utiliser les RP, les renseignements codés ou les renseignements anonymisés auxquels elle a accès dans le cadre de la prestation des services au service d'intégration des données, sauf aux fins de la prestation des services et uniquement dans la mesure nécessaire à cette fin; 2. La personne, l'entité ou l'organisation ne doit pas divulguer les RP, les renseignements codés ou les renseignements anonymisés auxquels elle a accès dans le cadre de la prestation des services au service d'intégration des données; 3. La personne, l'entité ou l'organisation doit se conformer à toutes les exigences de la Partie, aux normes relatives aux données, aux pratiques et procédures, aux autres dispositions applicables de la *Loi sur l'AIPVP* ou de ses règlements, ou aux accords ou reconnaissances conclus en vertu de ceux-ci, comme cela s'appliquerait à un membre du service d'intégration des données; 4. La personne, l'entité ou l'organisation ne doit pas permettre à ses employés ou à toute personne agissant en son nom d'accéder aux RP, aux renseignements codés ou aux renseignements anonymisés, à moins que l'employé ou la personne agissant en son nom n'accepte par écrit de se conformer aux restrictions qui s'appliquent à la personne, l'entité ou l'organisation qui fournit des services en vertu de la présente exigence.

Exigences 8 : Mettre en œuvre des mesures de sécurité physique raisonnables compte tenu des circonstances pour protéger les RP et les renseignements codés contre le vol, la perte, l'utilisation et la divulgation non autorisées.	
8.1	Déterminer et définir les mesures de sécurité physique raisonnables qui doivent être mises en œuvre pour protéger les RP et les renseignements codés contre le vol, la perte, l'utilisation et la divulgation non autorisées, notamment : 1. les serrures, les alarmes et l'accès restreint ou surveillé aux locaux du service d'intégration des données et aux endroits dans les locaux où sont conservés des RP et/ou des renseignements codés; 2. un processus de contrôle de l'accès des visiteurs au service d'intégration des données, qui doit comprendre des mesures pour déterminer, filtrer et superviser les visiteurs; 3. les mesures de sécurité pour les espaces de travail, les appareils et les supports de données utilisés lors du travail à distance, ainsi que les procédures connexes à suivre; 4. les mesures de sécurité physique applicables à la conservation et au transfert en toute sécurité des RP, des renseignements codés et des renseignements anonymisés sur des supports de données non électroniques (le cas échéant); 5. les méthodes précises qui doivent être utilisées pour conserver et transférer les RP, les renseignements codés et les renseignements anonymisés sur des supports de données non électroniques (le cas échéant);

	6. les conditions, exigences et restrictions applicables aux méthodes précises, y compris toutes les exigences dans : a. la Partie; b. les normes relatives aux données; c. les pratiques et procédures; d. les autres dispositions applicables de la *Loi sur l'AIPVP* et de ses règlements; e. les accords et les reconnaissances faites en vertu de ceux-ci.
8.2	Veiller à ce que : 1. seuls les membres et les visiteurs autorisés ont accès aux locaux physiques du service d'intégration des données et aux endroits à l'intérieur des locaux où sont conservés des RP, des renseignements codés et/ou des renseignements anonymisés, et toutes les conditions, exigences et restrictions ont été respectées; 2. toutes les faiblesses ou vulnérabilités déterminées dans les mesures de sécurité physique du service d'intégration des données sont résolues en temps opportun en fonction de leur niveau de gravité; 3. l'accès physique aux locaux du service d'intégration des données et aux endroits à l'intérieur des locaux où sont conservés des RP, des renseignements codés et/ou des renseignements anonymisés est immédiatement révoqué lorsque l'emploi d'un membre, sa relation contractuelle ou autre avec le service d'intégration des données a pris fin, ou lorsqu'un examen détermine que les droits d'accès du membre aux locaux ou à une partie de ceux-ci ne sont plus nécessaires; 4. les membres retournent en toute sécurité tous les biens du service d'intégration des données, y compris les RP et les renseignements codés, ainsi que tous les mécanismes d'accès physique (comme les cartes d'identification, les cartes d'accès et les clés), au plus tard à la date de cessation de l'emploi, du contrat ou de toute autre relation avec le service d'intégration des données ou lorsqu'un examen détermine que les biens ou les mécanismes d'accès physique ne sont plus nécessaires aux responsabilités du membre pour le service d'intégration des données; 5. la conservation et le transfert de RP, de renseignements codés et/ou de renseignements anonymisés sur des supports de données non électroniques (le cas échéant) sont autorisés à des fins et dans des circonstances définies, et toutes les conditions, exigences et restrictions ont été respectées.
8.3	**8.3.1** Établir et tenir à jour un registre des membres ayant un accès physique au service d'intégration des données. **8.3.2** Le registre doit au moins comprendre ce qui suit : 1. le(s) nom(s) du(des) membre(s); 2. le nom du ou des membres qui ont approuvé l'accès; 3. la date à laquelle l'accès a été accordé;

	4. la date de fin de l'accès, le cas échéant. **Remarque :** Il peut s'agir d'un registre autonome ou d'un registre combiné au registre des membres autorisés à accéder à l'environnement du service d'intégration des données conformément à l'exigence 7.3, et/ou au registre des membres autorisés à accéder à distance aux RP et aux renseignements codés ou à conserver des RP et des renseignements codés sur des dispositifs mobiles conformément à l'exigence 10.3.

Exigences 9 : Mettre en œuvre des mesures de sécurité raisonnables dans les circonstances pour protéger les RP et les renseignements codés conservés et/ou transférés sous forme électronique contre le vol, la perte, l'utilisation et la divulgation non autorisées.	
9.1	Déterminer et définir les mesures de sécurité raisonnables qui doivent être mises en œuvre pour protéger les RP et les renseignements codés contre le vol, la perte, l'utilisation et la divulgation non autorisées. Elles doivent au moins doit inclure ce qui suit : 1. Placer tous les composants du système qui font partie de l'environnement d'intégration des données dans une zone de réseau interne, séparée du reste du réseau; **Remarque :** On peut séparer les réseaux en combinant des technologies comme les réseaux locaux virtuels (VLAN), les pare-feux, les listes de contrôle d'accès, etc., qui doivent être déterminées expressément pour les opérations, les applications et l'infrastructure d'un service d'intégration des données. 2. Des pare-feux pour garantir que seul le trafic réseau autorisé est celui qui entre et sort de l'environnement du service d'intégration des données et le gérer; 3. Des mécanismes permettant de déterminer où et quand les RP et les renseignements codés risquent de faire l'objet de menaces et de vulnérabilités, et comment les renseignements seraient affectés par ces menaces et vulnérabilités; 4. Des pratiques et des contrôles de gestion des vulnérabilités pour déterminer, évaluer, corriger et atténuer efficacement toute faiblesse de sécurité dans l'environnement du service d'intégration des données; a. Les tests de pénétration doivent être effectués au moins une fois par an et après toute modification importante de l'environnement du service d'intégration des données; b. L'analyse de la vulnérabilité doit être effectuée au moins une fois par trimestre et après toute modification importante de l'environnement du service d'intégration des données; 5. Des contrôles pour surveiller et détecter efficacement toute tentative d'accès non autorisé à l'environnement du service d'intégration des données, y compris un processus de déploiement de contrôles anti-maliciel;

	6. Des connexions authentifiées, une cryptographie forte et des protocoles sécurisés pour transférer les renseignements; 7. Les méthodes précises qui doivent être utilisées pour conserver et transférer en toute sécurité les RP et les renseignements codés, ainsi que les conditions, les restrictions et les exigences applicables aux méthodes particulières, notamment toutes les exigences dans : a. la Partie; b. les normes relatives aux données; c. les pratiques et procédures; d. les autres dispositions applicables de la *Loi sur l'AIPVP* et de ses règlements; e. les accords et les reconnaissances faites en vertu de ceux-ci.
9.2	Veiller à ce que : 1. la conservation et le transfert des RP et/ou des renseignements codés sont autorisés à des fins et dans des circonstances définies, et toutes les conditions, exigences et restrictions ont été respectées; 2. toutes les faiblesses ou vulnérabilités déterminées dans les mesures de sécurité du service d'intégration des données sont résolues en temps opportun en fonction de leur niveau de risque.

Exigences 10 : S'assurer que les RP et les renseignements codés ne sont accessibles qu'à distance et/ou conservés sur des appareils mobiles que dans des circonstances approuvées.	
10.1	Déterminer et définir : 1. les exigences ou les conditions qui doivent être satisfaites pour permettre l'accès aux RP et aux renseignements codés à distance et/ou sur des appareils mobiles, y compris toutes les exigences de la Partie, les normes relatives aux données, les pratiques et procédures, les autres dispositions applicables de la *Loi sur l'AIPVP* et de ses règlements, ainsi que les accords et les reconnaissances faits en vertu de ceux-ci; 2. toute restriction pouvant s'appliquer à l'accès à distance et/ou à la conservation des RP et des renseignements codés sur les appareils mobiles; 3. les méthodes d'accès à distance et/ou de conservation en toute sécurité sur les appareils mobiles et les procédures connexes qui doivent être suivies; 4. les types de dispositifs qui peuvent être utilisés pour l'accès et/ou la conservation; 5. les fins auxquelles il est possible d'accéder à distance aux RP et aux renseignements codés et/ou de les conserver sur un dispositif mobile.
10.2	S'assurer que les membres accèdent à distance aux RP et/ou aux renseignements codés, et/ou conservent les RP et/ou les renseignements codés, sur un appareil mobile uniquement dans les conditions suivantes :

	1. À des fins et dans des circonstances définies, et toutes les conditions, exigences et restrictions ont été respectées; 2. L'accès à distance et/ou la conservation sur un appareil mobile de RP et/ou de renseignements codés ne sont fournis qu'aux membres qui ont besoin de l'accès à distance et/ou de la conservation sur un appareil mobile pour exercer des fonctions autorisées; 3. Les RP et les renseignements codés sont uniquement accessibles à distance et/ou conservés sur des dispositifs autorisés (p. ex., fournis et gérés par l'entreprise); 4. La finalité déterminée pour l'accès aux RP et/ou aux renseignements codés, et/ou leur conservation, ne peut raisonnablement être atteinte sans l'accès aux RP et/ou aux renseignements codés, et/ou leur conservation; 5. L'accès ou la conservation de RP et/ou de renseignements codés ne dépassera pas ce qui est raisonnablement nécessaire pour atteindre l'objectif déterminé; 6. En cas d'accès à distance à des RP et/ou des renseignements codés, il est interdit aux membres de copier, de déplacer ou de sauvegarder des RP et/ou des renseignements codés sur des supports de données à distance. 7. En cas de conservation de RP et/ou de renseignements codés sur un appareil mobile, les RP et/ou les renseignements codés conservés doivent être fortement cryptés à l'aide d'un mot de passe difficile à trouver, et l'appareil doit avoir un verrouillage automatique et un économiseur d'écran (le cas échéant) activé après une période d'inactivité; 8. Des mesures raisonnables, compte tenu des circonstances, ont été prises pour s'assurer que tous les accès à distance aux RP et/ou aux renseignements codés, et/ou leur conservation sur des appareils mobiles, sont autorisés, notamment : a. la révocation immédiate des droits d'accès à distance lorsque l'emploi d'un membre, sa relation contractuelle ou autre avec le service d'intégration des données a pris fin, ou lorsqu'un examen détermine que les droits d'accès à distance du membre à l'environnement du service d'intégration des données ou à une partie de celui-ci ne sont plus nécessaires.
10.3	**10.3.1** Élaborer et tenir un registre de tous les membres du service d'intégration des données autorisés à accéder à distance aux RP et aux renseignements codés et/ou à conserver les RP et les renseignements codés sur des appareils mobiles. **10.3.2** Le registre doit au moins comprendre ce qui suit : 1. le nom et les coordonnées du membre; 2. si le membre est autorisé à accéder à distance, et/ou à conserver sur un dispositif mobile, des RP et/ou des renseignements codés; 3. Le nom du membre qui a approuvé l'accès à distance et/ou la conservation sur le dispositif mobile;

	4. une description des applications du programme et des renseignements que l'utilisateur est autorisé à consulter à distance et/ou à conserver sur un appareil mobile; 5. l'objectif pour lequel l'accès et/ou la conservation ont été approuvés; 6. la date de l'approbation. **Remarque :** Il peut s'agir d'un registre autonome ou d'un registre combiné avec le registre des membres autorisés à accéder à l'environnement du service d'intégration des données, conformément à l'exigence 7.3, et/ou le registre des membres ayant un accès physique au service d'intégration des données, conformément à l'exigence 8.3.

Exigences 11 : Mener des évaluations des menaces et des risques et conserver et revoir les registres d'audit tant que les circonstances le permettent.	
11.1	Déterminer et définir les circonstances ou les événements pour lesquels une évaluation des menaces et des risques (EMR) est nécessaire; 1. Une EMR doit au moins être effectuée avant que le service d'intégration des données ne devienne opérationnel et lors de tout changement important de l'environnement du service d'intégration des données; 2. Au moins une fois par an, l'EMR ou les EMR les plus récentes doivent être révisées et mises à jour, le cas échéant, pour tenir compte de tout changement applicable au paysage des menaces, des tendances émergentes et des nouvelles technologies.
11.2	**11.2.1** Déterminer et définir le contenu obligatoire d'une EMR. **11.2.2** Une EMR doit au moins inclure : 1. une description de tous les éléments de renseignement du champ d'application; 2. l'identification des risques, notamment le potentiel de perte, d'endommagement ou de destruction d'un actif à la suite de l'exploitation d'une vulnérabilité par une menace; 3. les mesures de protection recommandées, notamment les améliorations ou les modifications apportées aux mesures de protection administratives, techniques et physiques du service d'intégration des données pour éliminer ou réduire les menaces et les vulnérabilités déterminées, en fonction de la gravité du risque.
11.3	S'assurer que les recommandations résultant des EMR sont classées par ordre de priorité et traitées afin d'éliminer ou de réduire les menaces et les vulnérabilités déterminées en temps opportun en fonction de la gravité du risque.
11.4	**11.4.1** Élaborer et tenir un registre des EMR. **11.4.2** Le registre doit au moins comprendre ce qui suit :

	1. la ou les dates auxquelles l'EMR a été achevée ou mise à jour, ou devrait être achevée ou mise à jour; 2. le nom du (des) membre(s) chargé(s) de remplir ou de mettre à jour l'EMR ou de veiller à ce qu'il soit rempli ou mise à jour; 3. les recommandations découlant de l'EMR; 4. le(s) nom(s) du (des) membre(s) chargé(s) de traiter chaque recommandation; 5. la date à laquelle chaque recommandation a été, ou devrait être, traitée; 6. comment chaque recommandation a été, ou devrait être, traitée.
11.5	**11.5.1** Déterminer et définir les renseignements qui doivent être enregistrés pour saisir et permettre la détection et le suivi des atteintes à la vie privée et à la sécurité. **11.5.2** Le service d'intégration des données doit au moins élaborer et tenir un registre qui comprend : 1. les identifiants des utilisateurs ou les comptes d'accès des membres; 2. la date et l'heure de chaque accès à l'environnement du service d'intégration des données; 3. l'identité du ou des dispositifs; 4. les tentatives réussies et ratées d'accès à l'environnement du service d'intégration des données, y compris tous les cas où des RP et/ou des renseignements codés sont consultés, manipulés ou traités d'une autre manière; 5. les fichiers consultés, y compris une référence aux RP et/ou aux renseignements codés consultés, manipulés ou traités d'une autre manière afin de déterminer quels RP et/ou quels renseignements codés de la personne ont été consultés, manipulés ou traités d'une autre manière, le cas échéant; 6. une description du type de renseignements consultés, manipulés ou traités d'une autre manière; 7. le nom du membre qui a consulté, manipulé ou traité d'une autre manière les renseignements; 8. les modifications des configurations du système; 9. l'utilisation des utilitaires du système; 10. les notifications des systèmes de contrôle de sécurité. **Remarque :** Les renseignements conservés dans le registre en vertu de cette exigence doivent être protégés de manière adéquate afin d'éviter le risque de fuite inappropriée de renseignements sensibles.

Exigences 12 : Mettre en place et en œuvre un processus pour gérer les changements de l'environnement du service d'intégration des données.	
12.1	**12.1.1** Déterminer et définir un processus sécurisé pour gérer les changements fournis et demandés par les fournisseurs dans l'environnement du service d'intégration des données.

	12.1.2 Le processus de gestion des modifications de l'environnement du service d'intégration des données doit au moins comprendre un processus pour : 1. examiner et suivre régulièrement les modifications fournies par le fournisseur et mettre en place des routines (p. ex., les correctifs de sécurité); 2. demander des changements; 3. déterminer si le changement doit être mis en œuvre ou non et les critères à prendre en compte pour prendre cette décision; 4. déterminer la priorité du changement, le moment où le changement doit être mis en œuvre et les critères à prendre en compte pour prendre ces décisions; 5. mettre les changements à l'essai.
12.2	Pour chaque changement, élaborer et maintenir une documentation qui inclut, au minimum : 1. une description du changement; 2. la date à laquelle le changement a été mis en place (p. ex., dans le cas de correctifs de sécurité) ou a été demandé; 3. le(s) nom(s) du (des) membre(s) qui demande(nt) le changement; 4. la justification de ce changement; 5. la priorité et l'incidence du changement; 6. le système d'information, la technologie, l'équipement, la ressource, l'application ou le programme auxquels le changement se rapporte; 7. les approbations requises pour le changement; 8. si le changement a été approuvé ou refusé, la raison de l'approbation ou du refus et le nom du ou des membres qui ont approuvé ou refusé le changement; 9. la date, le cas échéant, à laquelle le changement a été testé, le(s) membre(s) responsable(s) des tests et le succès ou l'échec des tests; 10. le nom du ou des membres responsables de la mise en œuvre du changement; 11. le délai de mise en œuvre du changement; 12. la date à laquelle la modification a été mise en œuvre, si elle a été approuvée.

Exigences 13 : S'assurer que les RP et les renseignements codés sont sauvegardés de manière à pouvoir être récupérés intégralement, et que le service d'intégration des données dispose d'un plan efficace de continuité des activités et de reprise après sinistre.	
13.1	Déterminer et définir : 1. la nature et les types de supports de données de secours conservés par le service d'intégration des données; 2. la fréquence à laquelle les renseignements sont sauvegardés; 3. les circonstances dans lesquelles les renseignements sauvegardés doivent être mis à disposition; 4. les processus, y compris les procédures connexes à suivre, pour les méthodes de sauvegarde et de récupération, ainsi que leur mise à l'essai.

13.2	**13.2.1** Déterminer et définir un plan de continuité des activités et de reprise après sinistre en cas d'interruptions des activités à court et à long terme et de menaces pour les capacités d'exploitation du service d'intégration des données, y compris les interruptions et menaces naturelles, humaines, environnementales et techniques. **13.2.2** Le plan de continuité des activités et de reprise après sinistre doit au moins inclure un processus pour : 1. la notification interne de l'interruption ou de la menace, ainsi que les personnes, entités ou organisations externes qui doivent être informées des interruptions d'activité à court et à long terme et des menaces pesant sur les capacités de fonctionnement du service d'intégration des données, y compris une liste actualisée des personnes à contacter pour la notification; 2. l'évaluation de la gravité de l'interruption ou de la menace; 3. la détermination des circonstances dans lesquelles le plan de continuité des activités et de reprise après sinistre sera activé et le processus d'activation; 4. une évaluation initiale de l'interruption ou de la menace; 5. une évaluation détaillée des dommages et évaluer l'effort prévu pour reprendre, récupérer et restaurer les éléments d'infrastructure, les systèmes d'information et les services; 6. la détermination de la priorité pour la reprise et le rétablissement de chaque application critique et de chaque fonction commerciale; 7. la détermination de toutes les applications et fonctions commerciales critiques, du matériel et des logiciels, des licences de logiciels, des supports de récupération, des équipements, des schémas de réseau du système, des configurations du matériel, des paramètres de configuration des logiciels, des paramètres de configuration des systèmes de base de données et des paramètres de réseau pour les pare-feux, les routeurs, les serveurs de noms de domaine, les serveurs de courrier électronique, etc. 8. tester, maintenir, évaluer et modifier le plan de continuité des activités et de reprise après sinistre.
13.3	**13.3.1** Veiller à ce que les méthodes de sauvegarde et de récupération, ainsi que le plan de continuité des activités et de reprise après sinistre, soient testés au moins une fois par an. **13.3.2** Documenter et traiter les tests effectués et toutes les conclusions et recommandations découlant de ces tests en temps opportun.

Exigences 14 : Répondre aux atteintes à la vie privée et à la sécurité en temps opportun et de manière appropriée.	
14.1	Déterminer, signaler en interne, contenir, notifier, enquêter sur les atteintes réelles ou présumées à la vie privée et à la sécurité de manière rapide et opportune et y remédier. Mettre en œuvre des procédures d'escalade si nécessaire.

14.2	Déterminer et définir : 1. les procédures à suivre pour déterminer, signaler, contenir, notifier, enquêter sur les atteintes réelles ou présumées à la vie privée ou à la sécurité, y compris les critères d'escalade au sein du service d'intégration des données, et y remédier; 2. les procédures à suivre lorsqu'une atteinte réelle ou présumée est à la fois une atteinte à la vie privée et à la sécurité; 3. les procédures à suivre pour déterminer si une atteinte réelle à la vie privée ou à la sécurité a eu lieu; 4. un processus permettant de déterminer quand la notification aux personnes concernées et au CIPVP est nécessaire; 5. la manière dont la notification doit être effectuée (p. ex., verbalement ou par écrit) et les renseignements à communiquer aux personnes concernées et au CIPVP; a. Les renseignements à communiquer doivent au moins comprendre : i. l'étendue de l'atteinte; ii. la nature des renseignements en cause; iii. les mesures mises en œuvre pour contenir l'atteinte; iv. une enquête supplémentaire et les mesures qui seront prises; 6. un processus permettant de donner suite aux recommandations résultant des enquêtes sur les atteintes à la vie privée ou à la sécurité afin d'éliminer ou de réduire le risque de telles atteintes à l'avenir.
14.3	Veiller à ce que : 1. les membres signalent toute atteinte réelle ou présumée à la vie privée et à la sécurité à la première occasion raisonnable; 2. toutes les mesures raisonnables sont prises, lorsqu'elle enquête sur une atteinte à la vie privée ou à la sécurité, pour éliminer et réduire le risque d'atteintes futures à la vie privée et à la sécurité et que, ce faisant, le service d'intégration des données tient compte de tous les facteurs pertinents, notamment des besoins suivants : a. Revoir et modifier les mesures de protection administratives, techniques et physiques pertinentes afin de renforcer la conformité; b. Examiner, élaborer et mettre en œuvre de nouvelles pratiques et procédures; c. Assurer une formation actualisée pour les membres; d. Tester et évaluer les mesures correctives afin de déterminer si elles ont été mises en œuvre correctement, et si les pratiques et procédures doivent être modifiées; 3. Le service d'intégration des données évalue si l'avis aux personnes, au CIPVP et aux autres parties concernées a été efficace (p. ex., a-t-il été fait en temps opportun, le ton et le contenu de l'avis étaient-ils appropriés, et les personnes concernées ont-elles reçu un soutien suffisant?)

14.4	**14.4.1** Créer et tenir un registre des atteintes à la vie privée et à la sécurité. **14.4.2** Le registre doit au moins comprendre ce qui suit : 1. La nature et l'étendue de l'atteinte (p. ex., combien de personnes sont touchées, le type de RP en cause, l'étendue du confinement, etc. ;) 2. Les mesures prises pour gérer l'atteinte (p. ex., le confinement et l'enquête, les recommandations faites); 3. Le nom du ou des membres responsables de la gestion de l'atteinte et de la prise en compte de chaque recommandation formulée; 4. Les plants pour informer les personnes concernées par l'atteinte, le CIPVP et d'autres parties, au besoin; 5. Le calendrier de la gestion continue de l'atteinte; 6. Les dates pertinentes (p. ex, date de l'atteinte (si elle est connue), date à laquelle l'atteinte a été déterminée ou soupçonnée, date de la notification aux parties concernées, date à laquelle les recommandations ont été traitées, etc.)

Conseils :

Les normes en technologie de l'information du gouvernement de l'Ontario (NTI-GO) sont les publications officielles relatives aux normes, aux lignes directrices, aux rapports techniques et aux pratiques préférées du gouvernement de l'Ontario. Si un service d'intégration des données est soumis au NTI-GO, il doit collaborer avec son groupe I et TI respectif et les professionnels de la cybersécurité pour élaborer les pratiques et procédures pertinentes.

Le CIPVP publie également des documents d'orientation visant à promouvoir la conformité aux lois ontariennes sur l'accès à l'information et la protection de la vie privée. Ces publications fournissent des conseils détaillés sur plusieurs exigences décrites dans cette norme et peuvent être utilisées par les services d'intégration des données pour un soutien supplémentaire.

ÉLIMINATION ET DESTRUCTION EN TOUTE SÉCURITÉ

La présente norme décrit les exigences que doivent respecter les services d'intégration des données pour assurer l'élimination ou la destruction en toute sécurité des RP, des renseignements codés et des supports de données connexes. Une fois éliminés ou détruits en toute sécurité, les RP et les renseignements codés sont définitivement supprimés du support de données correspondant, de sorte qu'ils ne puissent être reconstitués ou récupérés dans des circonstances raisonnablement prévisibles.

EXIGENCES ABOLUES

Pour assurer l'élimination ou la destruction en toute sécurité des RP et des renseignements codés en vertu de la Partie, les services d'intégration des données doivent :

15. Éliminer ou détruire rapidement et en toute sécurité les RP, les renseignements codés et les supports de données contenant ces renseignements.
16. Conserver et transférer les RP, les renseignements codés et les supports de données contenant les renseignements en toute sécurité en attendant leur élimination ou leur destruction.
17. Vérifier que les RP, les renseignements codés et les supports de données contenant les renseignements ont été éliminés ou détruits en toute sécurité.

DISPOSITIONS PERTINENTES DE LA PARTIE

Les exigences relatives à l'élimination et à la destruction en toute sécurité des RP sont décrites conformément aux dispositions suivantes de la Partie :

- Établissement de liens et anonymisation - alinéa 49.6(1)4.
- Sécurité et conservation - sous-alinéas 49.11(1)(a)(c) et (d)
  - Exigences en matière de sécurité – (2)

EXIGENCES PARTICULIÈRES

Exigences 15 : Éliminer ou détruire rapidement et en toute sécurité les RP, les renseignements codés et les supports de données contenant ces renseignements.	
15.1	Déterminer et définir la ou les méthodes sécurisées d'élimination et de destruction des RP, des renseignements codés et des supports de données connexes qui seront utilisés par le service d'intégration des données. Pour arriver à cette conclusion, les services d'intégration des données doivent tenir compte du type de renseignement et des supports de données (p. ex., supports électroniques et papier).

15.2	**15.2.1** Déterminer et définir les conditions dans lesquelles les RP, les renseignements codés et les supports de données contenant ces renseignements doivent être éliminés ou détruits en toute sécurité. **15.2.2** Les conditions doivent au moins inclure : 1. Le moment où les supports seront réutilisés; 2. Le moment où les supports expireront; 3. Le moment où les supports ne seront plus sous la garde ou le contrôle du service d'intégration des données.

Exigences 16 : Conserver et transférer les RP, les renseignements codés et les supports de données contenant les renseignements en toute sécurité en attendant leur élimination ou leur destruction.	
16.1	Déterminer et définir : 1. un espace physique et un ou plusieurs conteneurs clairement identifiés et verrouillés pour la conservation en toute sécurité des RP, des renseignements codés et des supports de données connexes jusqu'à leur élimination ou leur destruction en toute sécurité; 2. la procédure à suivre pour transférer en toute sécurité les RP, les renseignements codés et les supports de données connexes à l'extérieur du service d'intégration des données en vue de leur élimination ou de leur destruction (le cas échéant).
16.2	Veiller à ce que : 1. les RP, les renseignements codés et les supports de données connexes ne sont éliminés ou détruits en toute sécurité que dans des circonstances autorisées, et lorsque toutes les conditions, exigences ou restrictions ont été satisfaites, y compris toutes les exigences relatives : a. à la Partie; b. aux normes relatives aux données; c. aux pratiques et procédures; d. aux autres dispositions applicables de la *Loi sur l'AIPVP* et de ses règlements; e. aux accords et aux reconnaissances faits en vertu de ceux-ci; 2. les RP, les renseignements codés et les supports de données connexes destinés à être éliminés ou détruits en toute sécurité sont physiquement séparés des autres renseignements; 3. les RP, les renseignements codés et les supports de données connexes destinés à être éliminés ou détruits en toute sécurité sont conservés dans un ou plusieurs conteneurs clairement identifiés et verrouillés en attendant leur élimination ou leur destruction en toute sécurité;

	4. en ce qui concerne chaque transfert de supports de données en dehors du service d'intégration des données en vue de leur élimination ou de leur destruction en toute sécurité, le service d'intégration des données : a. documente la date, l'heure et le mode de transfert; b. tient un registre des confirmations écrites attestant de la réception des supports de données; c. tient un inventaire détaillé des supports de données liés à chaque transfert.

Exigences 17 : Vérifier que les RP, les renseignements codés et les supports de données contenant les renseignements ont été éliminés ou détruits en toute sécurité.	
17.1	**17.1.1** Déterminer et définir le contenu requis des certificats d'élimination ou de destruction en toute sécurité. **17.1.2** Les certificats d'élimination ou de destruction en toute sécurité doivent au moins inclure : 1. le service d'intégration des données d'où provient les supports de données; 2. le fabricant, le modèle ou le numéro de série (s'il s'agit de supports électroniques); 3. le type de support (papier ou électronique); 4. la méthode d'élimination ou de destruction utilisée; 5. le(s) nom(s) du/des membre(s) demandant l'élimination ou la destruction en toute sécurité; 6. le nom, la fonction, l'adresse, les coordonnées et la signature de la personne responsable de l'élimination ou de la destruction et la date de l'élimination ou de la destruction.
17.2	Déterminer et définir : 1. le délai dans lequel les certificats d'élimination ou de destruction en toute sécurité doivent être obtenus; 2. la période pendant laquelle, et le lieu où, les certificats d'élimination ou de destruction en toute sécurité seront conservés.
17.3	S'assurer de ce qui suit : 1. Un certificat d'élimination ou de destruction en toute sécurité est obtenu pour chaque support de données éliminé ou détruit en toute sécurité, confirmant l'élimination ou la destruction en toute sécurité des RP, des renseignements codés et des supports de données associés; 2. Le service d'intégration des données élabore et tient à jour un registre qui comprend au moins : a. les dates auxquelles les RP, les renseignements codés et les supports de données connexes sont transférés pour être éliminés ou détruits en toute sécurité;

	b. les dates de réception des certificats d'élimination ou de destruction en toute sécurité; 3. La ou les méthodes d'élimination ou de destruction en toute sécurité déterminées sont revues périodiquement par le service d'intégration des données pour s'assurer de leur efficacité.

Conseils :

Le Règlement 459 de l'Ontario : Disposition des renseignements personnels en vertu de la *Loi sur l'AIPVP* décrit les exigences visant à protéger la sécurité et la confidentialité des RP qui doivent être détruites. Si un service d'intégration des données est assujetti au règlement, il doit collaborer avec ses professionnels de la gestion des documents et des renseignements et de la protection de la vie privée pour élaborer les pratiques et procédures pertinentes.

Le CIPVP publie également des documents d'orientation visant à promouvoir la conformité aux lois ontariennes sur l'accès à l'information et la protection de la vie privée. Ces publications fournissent des conseils détaillés sur plusieurs exigences décrites dans cette norme et peuvent être utilisées par les services d'intégration des données pour un soutien supplémentaire.

PÉRIODE DE CONSERVATION

La présente norme décrit les exigences que doivent respecter les services d'intégration des données pour conserver les RP et les renseignements codés pendant des périodes déterminées. Une période de conservation est la durée globale pendant laquelle les renseignements doivent être conservés avant de pouvoir et, dans certains cas, de devoir être supprimés. En vertu de la Partie, les services d'intégration des données doivent conserver les RP pendant une période déterminée par les normes relatives aux données.

EXIGENCES ABOLUES

Pour s'assurer que les RP et les renseignements codés visés par la Partie sont conservés pendant les périodes précisées conformément à la Partie, les services d'intégration des données doivent :

18. mettre en œuvre des exigences de conservation pour les RP et les renseignements codés.

DISPOSITIONS PERTINENTES DE LA PARTIE

Les exigences relatives à la conservation des RP sont décrites conformément aux dispositions suivantes de la Partie :

- Établissement de liens et anonymisation - alinéa 49.6(1)4.
- Idem - par.49.6(2)
- Sécurité et conservation - alinéa 49.11(1)(c)
- Normes relatives aux données - sous-alinéa 14(1)(a)(iv)

EXIGENCES PARTICULIÈRES

Exigences 18 : Mettre en œuvre des exigences de conservation pour les RP et les renseignements codés.	
18.1	**18.1.1** Déterminer et définir un processus permettant de déterminer la durée de conservation des RP et des renseignements codés. 1. Le processus doit au moins tenir compte des facteurs suivants : a. les besoins commerciaux ou opérationnels; b. les exigences légales et réglementaires; c. les attentes de la communauté et du public; d. les intérêts de la vie privée des particuliers. **18.1.2** Déterminer et définir une période de conservation pour chaque catégorie de RP.

	1. Les RP du dossier créé par le service d'intégration des données contenant la quantité minimale de RP nécessaire à l'établissement de liens en vertu de l'exigence 20.3 doivent être au moins conservées assez longtemps pour permettre aux personnes d'exercer leurs droits d'accès et de correction en vertu de l'article 47 de la *Loi sur l'AIPVP*. **18.1.3** Déterminer et définir une période de conservation des renseignements codés. 1. les renseignements codés doivent être conservés pendant au moins un an après l'achèvement de l'anonymisation et la remise des renseignements anonymisés à la personne, l'entité ou l'organisation qui en fait la demande. **Remarque :** L'objectif de la période minimale de conservation des renseignements codés est de faciliter l'exercice des droits d'accès et de correction des personnes en vertu de l'article 47 de la *Loi sur l'AIPVP.* Pour que les services d'intégration des données puissent déterminer la personne à laquelle se rapportent les renseignements codés, ils doivent conserver les identificateurs minimaux qui se rapportent au sous-ensemble particulier des données codées. Ces identifiants minimaux sont conservés dans le dossier déterminé par l'exigence 20.3.
18.2	**18.2.1** Conserver les RP originaux non codés pendant une période maximale de 180 jours civils après leur transformation en renseignements codés afin de permettre un établissement de liens précise, conformément à l'exigence 20. **18.2.2** Si la collecte d'une série de RP est nécessaire pour le codage afin de permettre un établissement de liens précis, conserver les RP originaux non codés pendant une période maximale de 180 jours civils après la transformation des derniers RP de la série en renseignements codés. Le délai entre la première et la dernière collecte d'une série de RP ne doit pas dépasser un an. **18.2.3** Les périodes maximales de conservation peuvent être prolongées lorsque : 1. nécessaire en raison de circonstances exceptionnelles ou imprévues; 2. la prolongation est d'une durée définie qui est le minimum nécessaire pour que les RP originaux non codés soient transformés en renseignements codés afin de permettre un établissement de liens précis; 3. un avis détaillant la raison et la durée de la prolongation demandée est fourni par écrit à l'archiviste de l'Ontario et au CIPVP au moins 30 jours civils avant l'expiration de la période de conservation initiale; 4. le CIPVP approuve la prolongation par écrit. **Remarque :** Pour davantage de clarté, ces durées maximales de conservation ne s'appliquent pas au document créé par le service d'intégration des données contenant la quantité minimale de RP nécessaire à l'établissement de liens en vertu de l'exigence 20.3.

18.3	S’assurer que les RP et les renseignements codés sont supprimés à la plus antérieure des dates suivantes : 1. L’expiration de la ou des périodes de conservation maximales déterminées et définies par le service d’intégration des données conformément à l’exigence 18.1; 2. L’expiration de la ou des périodes de conservation maximales établies en vertu de l’exigence 18.2, selon le cas; 3. Sa conservation n’est plus nécessaire pour atteindre la finalité pour laquelle ils ont été collectés ou créés, après l’expiration des périodes de conservation minimales établies en vertu de l’exigence 18.1. **Remarque :** Après la suppression de RP ou de renseignements codés en vertu de cette exigence, les services d’intégration des données ne sont pas autorisés à reconstituer les renseignements supprimés ou à y avoir de nouveau accès.
18.4	Plus précisément, les périodes de conservation des exigences 18.1 à 18.3 : 1. sont des exemptions à la période de conservation énoncées au sous-alinéa 49.6(1)4 de la Partie; 2. précisent la période de conservation aux fins de l’alinéa 49.11(1)(c) de la Partie. **Remarque :** Cette exigence précise que les délais de conservation contenus dans cette norme remplacent les délais de conservation minimum et maximum précisés dans les dispositions de la Partie citées ci-dessus. Après la suppression des renseignements conformément aux exigences de conservation de la présente norme, les RP, les renseignements codés et les supports de données contenant les renseignements doivent être éliminés ou détruits en toute sécurité conformément aux exigences 15, 16 et 17.
18.5	**18.5.1** Établir et tenir un registre des RP et des renseignements codés qui ont été supprimés conformément à la période de conservation définie. **18.5.2** Le registre doit au moins comprendre ce qui suit : 1. Une description des RP ou des renseignements codés; 2. Une description de la période de conservation applicable; 3. La date de collecte des RP et la date de transformation des RP en renseignements codés (le cas échéant); 4. La date à laquelle les RP ou les renseignements codés ont été supprimés et le nom du ou des membres qui ont supprimé les RP ou les renseignements codés. **Remarque :** Il peut s’agir d’un registre autonome ou d’un registre combiné à l’inventaire des RP et des renseignements codés au sein du service d’intégration des données, conformément à l’exigence 5.4.

Conseils :

Pour les services d'intégration des données applicables, ils doivent s'assurer que la conservation et l'élimination des documents sont gérées conformément à la *Loi de 2006 sur les Archives publiques et la conservation des documents*. Le service d'intégration des données devrait collaborer avec ses professionnels de la gestion des documents et des renseignements et de la protection de la vie privée pour élaborer un calendrier des documents contenant des RP et d'autres documents créés, reçus et conservés par le service d'intégration des données aux fins des exigences de la présente norme et selon ces exigences.

Un calendrier des documents décrit les documents gérés par le service d'intégration des données, détermine les périodes de conservation autorisées, détermine les documents ayant une valeur durable et précise la disposition finale des documents à la fin de leur période de conservation - soit pour être détruits, transférés aux Archives de l'Ontario ou, lorsque cela est nécessaire et possible, pour continuer à être conservés par le service d'intégration des données au nom des Archives. Conformément à la *Loi de 2006 sur les Archives publiques et la conservation des documents*, un calendrier des documents doit être approuvé par l'Archiviste de l'Ontario. Toutefois, un calendrier de conservation de documents en vertu de la *Loi de 2006 sur les Archives publiques et la conservation des documents* ne doit pas exiger que les documents soient conservés au-delà des périodes de conservation maximales applicables énoncées dans les présentes normes relatives aux données. Reportez-vous aux exigences du calendrier des enregistrements pour des directives plus détaillées.

ANONYMISATION ET ÉTABLISSEMENT DE LIENS

La présente norme décrit les exigences auxquelles doivent se conformer les services d'intégration des données pour mettre en œuvre un processus d'anonymisation et d'établissement de liens précis et protecteur de la vie privée afin de garantir que les RP recueillis en vertu de la Partie peuvent être transformés et utilisée à des fins d'analyse, comme le permet la Partie. Elle exige également que le processus d'anonymisation, en particulier la transformation des RP en renseignements codés, soit entrepris dès que cela est raisonnablement possible dans les circonstances.

EXIGENCES ABOLUES

Pour s'assurer que les RP recueillis en vertu de la Partie sont déterminés et liés d'une manière précise et qui protège la vie privée, les services d'intégration des données doivent :

19. Séparer les tâches liées au codage et à l'établissement de liens.
20. Dès que cela est raisonnablement possible dans les circonstances, transformer les RP collectés par le service d'intégration des données en renseignements codés.
21. Établir des liens entre les renseignements codés et d'autres renseignements codés, si nécessaire pour l'analyse.
22. Déterminer les renseignements codés avant l'analyse.

DISPOSITIONS PERTINENTES DE LA PARTIE

Les exigences en matière d'anonymisation et d'établissement de liens sont décrites conformément aux dispositions suivantes de la Partie :

- Sens de « anonymisation » - par. 49.1(2)
- Règles générales : renseignements personnels - par. 49.3(1)
  - Quantité de renseignements - (2)
- Établissement de liens et anonymisation - alinéa 49.6(1)(1 à 3)
  - Idem (2)
- Restrictions en matière d'utilisation des renseignements personnels - par. 49.7(1)
- Restrictions en matière d'utilisation des renseignements anonymisés - art. 49.8

EXIGENCES PARTICULIÈRES

Exigences 19 : Séparer les tâches liées au codage et à l'établissement de liens.	
19.1	Déterminer et définir des rôles distincts pour les processus de codage et d'établissement de liens au sein du service d'intégration des données.

	Remarque : La séparation des rôles et des tâches en matière de codage et d'établissement de lien a pour but de faciliter la protection de la vie privée en empêchant qu'un seul membre, à un moment donné, ait un accès trop concentré aux RP. Elle est également conforme à l'exigence de minimisation des données prévue au paragraphe 49.3(2) de la Partie.
19.2	Assurer la séparation de ces rôles dans les processus de codage et d'établissement de liens en utilisant des mesures de protection administratives, techniques et physiques raisonnables dans les circonstances. **Remarque :** Lorsqu'il est impossible de séparer les tâches entre plusieurs membres en raison du manque de ressources humaines disponibles (p. ex., comme c'est le cas dans les petits services d'intégration des données), d'autres mesures de protection appropriées, comme la surveillance des activités, les pistes de vérification et la supervision de la direction, doivent être renforcées pour obtenir le même effet.

Exigences 20 : Dès que cela est raisonnablement possible dans les circonstances, transformer les RP collectés par le service d'intégration des données en renseignements codés.	
20.1	Déterminer et définir les identificateurs directs et indirects communs minimaux nécessaires pour permettre l'établissement de liens.
20.2	Veiller à ce que les identifiants directs soient retirés des RP et remplacés par un code interne sécurisé unique à la personne. **Remarque :** Le résultat de ce processus est la création de renseignements codés. C'est le début du processus d'anonymisation pour permettre la création de liens conformément au paragraphe 49.6(1) de la Partie. En outre, avant l'analyse, la méthode d'anonymisation prévue par l'exigence 22 doit être appliquée aux renseignements codés.
20.3	Établir et maintenir une correspondance précise et à jour entre chaque code interne attribué et les identifiants directs et indirects communs minimaux. **Remarque :** Les identificateurs directs retirés des RP en vertu de l'exigence 20.2 peuvent être conservés par le service d'intégration des données afin d'être utilisés pour l'attribution de codes internes et l'établissement de liens, le cas échéant. Ces identifiants doivent être séparés des renseignements codés (p. ex., dans une base de données d'identifiants utilisée pour la mise en correspondance entre chaque code interne attribué et les identifiants communs minimaux). Cette correspondance entre les codes internes attribués et les identificateurs communs minimaux facilitera également la tâche des services d'intégration des données qui répondent aux personnes exerçant leurs droits d'accès et de correction en vertu de l'article 47 de la *Loi sur l'AIPVP*.

	La transformation des RP dans cette exigence entraîne : la création de renseignements codés; le mappage entre les identificateurs mentionnés ci-dessus; et aucun autre RP.

Exigences 21 : Établir un lien entre les renseignements codés à d'autres renseignements codés, si nécessaire pour l'analyse.	
21.1	Déterminer et définir : 1. les méthodes qui doivent être utilisées pour établir un lien avec les renseignements codés; 2. les risques liés à l'exactitude de ces liens; 3. comment ces risques pour l'exactitude seront atténués.
21.2	**21.2.1** Veiller à ce que : 1. les renseignements codés ne soient liés que dans des circonstances autorisées et lorsque toutes les conditions, exigences et restrictions ont été satisfaites, y compris toutes les exigences de la Partie, des normes relatives aux données, des pratiques et procédures, des autres dispositions applicables de la *Loi sur l'AIPVP* et de ses règlements, et des accords et reconnaissances conclus en vertu de ceux-ci; 2. l'exactitude des établissements de liens de renseignements codés en utilisant des méthodes et des procédures d'essai raisonnables dans les circonstances. **21.2.2** Examiner périodiquement en interne les établissements de liens pour s'assurer qu'ils sont exacts.

Exigences 22 : Déterminer les renseignements codés avant l'analyse.	
22.1	**22.1.1** Déterminer et définir les critères à appliquer pour calculer le risque de désanonymisation qui doivent au moins porter sur : 1. le type de validation des données; 2. les identifiants qui doivent être supprimés, cachés ou transformés d'une autre manière; 3. les types d'attaques de désanonymisation à envisager; 4. les types de renseignements de base dont disposent les destinataires des données. **22.1.2** Déterminer et définir une méthodologie d'anonymisation basée sur le risque. **22.1.3** La méthodologie doit au moins faire appel à des techniques, des garanties, des mesures et des procédures appropriées et comprendre les étapes suivantes :

	1. Classer les variables; 2. Déterminer un seuil acceptable de risque de désanonymisation; 3. Mesurer les risques liés aux données et au contexte; 4. Calculer le risque global de désanonymisation; 5. S'assurer que le risque global est inférieur ou égal au seuil de risque de désanonymisation.
22.2	S'assurer que la méthodologie d'anonymisation est appliquée aux renseignements codés avant l'analyse pour veiller aux fins suivantes : 1. Il n'est pas raisonnablement prévisible, dans ces circonstances, qu'une personne puisse être déterminée; 2. Le risque de désanonymisation est très faible. **Remarque :** Les deux points ci-dessus décrivent le même résultat, mais sous des angles différents. La première suit la définition statutaire de ce qui doit être réalisé par l'anonymisation, tandis que la seconde fournit un compte rendu technique qui se prête mieux à la quantification.
22.3	**22.3.1** Élaborer et tenir à jour la documentation relative à l'application de la méthode d'anonymisation à tout renseignement codé. **22.3.2** La documentation doit au moins inclure : 1. le(s) destinataire(s) des données et le type de diffusion; 2. une description des renseignements codés qui ont été anonymisés, y compris les éléments de données ou les champs particuliers; 3. les mesures prises pour désanonymiser les renseignements; 4. les analyses utilisées pour déterminer, mesurer et calculer la quantité et les types de techniques d'anonymisation, de sauvegardes, de paramètres et de procédures qui ont été appliqués.

AVIS PUBLIC ET RAPPORT ANNUEL

Cette norme décrit les exigences minimales que doivent respecter les services d'intégration des données pour assurer l'ouverture et la transparence de leurs pratiques en matière de renseignements. En vertu de cette Partie, les services d'intégration des données doivent mettre à la disposition du public des renseignements sur la façon dont ils recueillent, utilisent et divulguent les RP. En particulier, les services d'intégration des données doivent créer et publier la documentation relative à l'avis de collecte, aux rapports d'utilisation, aux rapports annuels et aux plaintes et demandes de renseignements sur la vie privée.

EXIGENCES ABOLUES

Pour s'assurer que les exigences relatives à l'avis de collecte, au rapport d'utilisation, au rapport annuel et aux plaintes et demandes de renseignements sur la protection de la vie privée en vertu de la Partie sont respectées, les services d'intégration des données doivent :

23. Publier un avis de collecte qui concerne les RP à collecter en vertu de la Partie.
24. Publier une liste complète des avis de collecte publiés par le service d'intégration des données.
25. Publier un rapport sur l'utilisation des RP pour établir des liens et anonymiser les données, et réaliser un audit.
26. Publier un rapport annuel portant sur la collecte, l'utilisation, l'anonymisation, l'établissement de liens et la divulgation des RP recueillies en vertu de la Partie.
27. Répondre aux plaintes et aux demandes de renseignements du public en matière de protection de la vie privée et les traiter en temps opportun.

AVIS DE COLLECTE

DISPOSITIONS PERTINENTES DE LA PARTIE

Les exigences relatives à l'avis de collecte sont décrites conformément aux dispositions suivantes de la Partie :

- Avis de collecte - art. 49.10

EXIGENCES PARTICULIÈRES POUR L'AVIS DE COLLECTE

Exigences 23 : Publier un avis de collecte qui concerne les RP à collecter en vertu de la Partie.	
23.1	Publier un avis comprenant les renseignements énoncés dans les exigences 23.2 à 23.8 avant chaque nouvelle collecte de RP.

	Remarque : On parle de nouvelle collecte lorsque les RP sont collectés auprès d'une source pour la première fois. On parle de collecte continue lorsque les mêmes éléments de données des RP sont recueillis auprès de la même source sur une base définie (p. ex., les mêmes éléments de données de RP sont recueillis chaque mois pendant deux ans). Si une collecte de RP fait partie d'une collecte continue des mêmes RP auprès de la même source, un avis de collecte distinct n'est pas nécessaire chaque fois que les mêmes éléments de données de RP sont recueillis. Par exemple, si les RP doivent être recueillis tous les mois pendant deux ans, l'avis de collecte publié avant le premier mois de collecte doit définir la fréquence et la durée de la collecte. Un nouvel avis de collecte n'est pas nécessaire lorsqu'une collecte en cours se poursuit dans les mois suivants.
23.2	Citer l'autorité légale qui permet la collecte en se référant à l'article ou aux articles précis de la Partie qui autorise la collecte et aux autres lois pertinentes. Par exemple : Les renseignements personnels sont recueillis indirectement pour faciliter l'évaluation des programmes et services financés par le ministère de (X) conformément à l'article 49.2 de la *Loi sur l'AIPVP* et sous réserve des conditions énoncées à l'article 49.4 de la *Loi sur l'AIPVP*.
23.3	Décrire les types de RP à recueillir. La description doit inclure des détails sur la portée des RP collectés, notamment le secteur, la plage de dates et les caractéristiques démographiques/populaires. Par exemple : Dossiers de transport, y compris les collisions de véhicules à moteur et les réclamations pour blessures et décès, entre mars 2019 et mars 2020 des conducteurs titulaires d'un permis en Ontario. La collecte aura lieu tous les trimestres au cours de la période d'un an définie.
23.4	Indiquer la ou les sources et les ensembles de données à partir desquels les RP doivent être recueillis. Par exemple, en développant l'exemple de l'exigence 23.3 : • Collisions de véhicules à moteur sur les routes provinciales (ministère des Transports) • Collisions mortelles et avec blessés par type d'impact initial (ministère des Transports) • Collisions entre véhicules à moteur sur les routes provinciales (Municipalités - Centres de déclaration des collisions) • Demandes d'indemnisation pour dommages corporels dans le cadre de l'assurance automobile (Autorité ontarienne de réglementation des services financiers)

	• Demandes d'indemnisation en cas de décès dans le cadre de l'assurance automobile (Autorité ontarienne de réglementation des services financiers)
23.5	Décrire le(s) but(s) pour lesquels les RP doivent être recueillis et utilisés, notamment la nature générale des liens qui peuvent être établis. Le but de la collecte doit être conforme aux objectifs autorisés énoncés à l'article 49.2 de la *Loi sur l'AIPVP*. L'utilisation des RP doit inclure leur anonymisation et peut inclure l'établissement de liens entre les RP, ainsi que la réalisation d'audits, le cas échéant, comme indiqué au paragraphe 49.7(1). Par exemple : Le service d'intégration des données recueille des RP dans le but de planifier la prestation des programmes et des services. Les RP recueillis seront anonymisés et reliés entre elles afin de mieux comprendre les exigences en matière de sécurité des usagers de la route et d'assurance des véhicules sous juridiction provinciale. Les variables des collisions de véhicules à moteur, les décès et les demandes d'indemnisation seront liés.
23.6	Déterminer les fins pour lesquelles les RP peuvent être divulgués et toutes les fins connues (au moment de la collecte) pour lesquelles les RP seront divulgués. Par exemple : Les RP seront divulgués aux membres du service d'intégration des données du ministère de (X) qui ont besoin d'accéder aux renseignements dans l'exercice de leurs fonctions en rapport avec la Partie. Le RP sera également divulgué au service interministériel d'intégration des données du ministère de (Y). Le service d'intégration des données du ministère de (X) peut également divulguer les RP qu'il recueille : • à un autre service interministériel d'intégration des données et/ou à un service extraministériel d'intégration des données; • comme l'exige la loi; • à une institution ou à un organisme d'application de la loi au Canada dans le cadre d'une enquête; • aux fins d'une procédure devant une cour ou un tribunal; • au commissaire à l'information et à la protection de la vie privée de l'Ontario; • à des fins de recherche.
23.7	Indiquer le titre, l'adresse électronique, l'adresse postale et le numéro de téléphone d'un ou de plusieurs membres du service d'intégration des données qui peuvent répondre à toute question sur la collecte, l'utilisation et la divulgation des RP en vertu de la Partie.
23.8	Inclure un courriel, une adresse postale et un numéro de téléphone pour le CIPVP, avec une description des fonctions du CIPVP en vertu de l'article 49.12.

23.9	**23.9.1** Publier l'avis en anglais et en français sur un site Web du gouvernement de l'Ontario ou, dans le cas d'un service extraministériel d'intégration des données, sur le site Web de la personne ou de l'entité. **23.9.2** Veiller à ce que l'avis de collecte soit rédigé dans un langage clair et facile à comprendre.
23.10	Pour les collectes permanentes de RP, mettre à jour l'avis de collecte publié, dès que cela est raisonnablement possible, afin de vous assurer qu'il continue à décrire la collecte avec précision.

Exigences 24 : Publier une liste complète des avis de collecte publiés par le service d'intégration des données.	
24.1	**24.1.1** Établir et tenir à jour une liste des avis de collecte publiés par le service d'intégration des données. **24.1.2** La liste doit au moins inclure : 1. la date de la première publication de chaque avis de collecte; 2. une description des projets entrepris par le service d'intégration des données à l'aide des renseignements mentionnés dans chaque avis de collecte (p. ex., l'amélioration des résultats en matière de santé grâce au rattachement à un fournisseur de soins primaires); 3. les sources de RP référencées dans chaque avis de collecte; 4. la date de la dernière mise à jour de chaque avis de collecte; 5. un lien vers chaque avis de collecte.
24.2	**24.2.1** Publier la liste en anglais et en français sur un site Web du gouvernement de l'Ontario ou, dans le cas d'un service extraministériel d'intégration des données, sur le site Web de la personne ou de l'entité. **24.2.2** Veiller à ce que la liste emploie un langage clair et facile à comprendre.

RAPPORT SUR L'UTILISATION

DISPOSITIONS PERTINENTES DE LA PARTIE

Les exigences relatives aux rapports sur l'utilisation sont décrites conformément aux dispositions suivantes de la Partie :

- Restrictions en matière d'utilisation des renseignements personnels - par. 49.7(1)
  - Service extraministériel d'intégration des données (1.1)
  - Rapport sur l'utilisation (2)

- Normes relatives aux données - sous-alinéa 49.14(1)(a)(iii)

EXIGENCES PARTICULIÈRES EN MATIÈRE D'ÉTABLISSEMENT DE RAPPORTS D'UTILISATION

Exigences 25 : Publier un rapport sur l'utilisation des RP pour établir des liens et anonymiser les données, et réaliser un audit.	
25.1	Le rapport doit au moins comprendre : 1. la liste des RP et des renseignements codés du service d'intégration des données élaborée et tenue à jour conformément à l'exigence 25.3; 2. les descriptions des audits entrepris en vertu de l'alinéa 49.7(1)(b). **Remarque :** Les services d'intégration des données peuvent combiner ce rapport d'utilisation avec le rapport annuel décrit à l'exigence 26 (ci-dessous).
25.2	**25.3.1** Publier le rapport sur les utilisations des RP au moins une fois par an en anglais et en français sur un site Web du gouvernement de l'Ontario ou, dans le cas d'un service extraministériel d'intégration des données, sur le site Web de la personne ou de l'entité. **25.3.2** Veiller à ce que le rapport emploie un langage clair et facile à comprendre.
25.3	**26.7.1** Développer et tenir une liste des ensembles de données (conservés par le service d'intégration des données de : 1. les identificateurs conservés pour être utilisés dans l'attribution d'identificateurs internes et la création de liens conformément à l'exigence 20.3; 2. renseignements codés. **26.7.2** La liste doit au moins inclure : 1. le nom de l'ensemble de données; 2. une description de l'ensemble de données; 3. la plage de dates de l'ensemble de données; 4. les éléments de données ou les champs particuliers contenus dans l'ensemble de données; 5. la source(s) de renseignements dans l'ensemble de données; 6. les projets entrepris par le service d'intégration des données à l'aide de l'ensemble de données. **Remarque :** Les ensembles de données des RP originaux non codés recueillis par le service d'intégration des données n'ont pas besoin d'être inclus dans cette liste puisqu'ils seront reflétés dans les avis de collecte, mais les renseignements codés dérivés de ces ensembles de données doivent être inclus.

RAPPORT ANNUEL

DISPOSITIONS PERTINENTES DE LA PARTIE

Les exigences relatives au rapport annuel sont décrites conformément aux dispositions suivantes de la Partie :

- Rapport annuel - par. 49.13(1)
  - Idem (1.1)
  - Contenu du rapport

EXIGENCES PARTICULIÈRES POUR LE RAPPORT ANNUEL

Exigences 26 : Publier un rapport annuel portant sur la collecte, l'utilisation, l'anonymisation, l'établissement de liens et la divulgation des RP recueillies en vertu de la Partie.	
26.1	S'assurer qu'un rapport annuel est publié au plus tard le 1er avril de l'année suivant la période de couverture du rapport et qu'il comprend les renseignements énoncés dans les exigences 26.2 à 26.6. Le rapport annuel doit couvrir la période du 1er janvier au 31 décembre.
26.2	Décrire les types de RP qui ont été recueillis, utilisés et divulgués.
26.3	Décrire la ou les finalités pour lesquelles les RP ont été recueillis, utilisés et divulgués, en incluant des détails contextuels supplémentaires, si possible.
26.4	Décrire la nature des liens de renseignements codés qui ont été établis, y compris en faisant référence à la liste élaborée et tenue à jour conformément à l'exigence 25.3.
26.5	Inclure un résumé de la façon dont les renseignements anonymisés ont été utilisés et divulgués, notamment en ce qui concerne les projets entrepris par le service d'intégration des données figurant dans la liste élaborée et tenue à jour conformément à l'exigence 25.3.
26.6	Décrire comment les pratiques et procédures du service d'intégration des données répondent aux exigences de la Partie et permettent la collecte, l'utilisation, l'anonymisation, l'établissement de liens, la divulgation, la conservation, le transfert et l'élimination ou la destruction des RP dans le respect de la vie privée et en toute sécurité.
26.7	**26.7.1** Publier le rapport annuel en anglais et en français sur un site Web du gouvernement de l'Ontario ou, dans le cas d'un service extraministériel d'intégration des données, sur le site Web de la personne ou de l'entité.

	26.7.2 Veiller à ce que le rapport annuel emploie un langage clair et facile à comprendre.

PLAINTES ET DEMANDES DE RENSEIGNEMENTS SUR LA VIE PRIVÉE

DISPOSITIONS PERTINENTES DE LA PARTIE

Les exigences relatives aux plaintes et aux demandes de renseignements sur la vie privée sont décrites conformément aux dispositions suivantes de la Partie III.1 de la *Loi sur l'AIPVP* :

- Sécurité et conservation – par. 49.11(1)
  - Exigences en matière de sécurité (2)
  - Avis au commissaire (4)

EXIGENCES PARTICULIÈRES POUR LES PLAINTES ET LES DEMANDES DE PLAINTE SUR LA VIE PRIVÉE

Exigences 27 : Répondre aux plaintes et aux demandes de renseignements du public en matière de protection de la vie privée et les traiter en temps opportun.	
27.1	**27.1.1** Déterminer et définir comment un membre du public peut déposer une plainte ou une demande de renseignements sur la protection de la vie privée en rapport avec les activités du service d'intégration des données. **27.1.2** Le processus doit au moins inclure : 1. la manière dont une plainte ou une demande de renseignements peut être formulée (p. ex., par courriel, courrier, téléphone, etc. ;) 2. les renseignements demandés à la personne qui a déposé la plainte ou la demande de renseignements; 3. le titre et les coordonnées de la personne à qui une plainte ou une demande de renseignements peut être adressée.
27.2	**27.2.1** Déterminer et définir les procédures et les délais à respecter pour recevoir, documenter, suivre, enquêter, remédier sur les plaintes et les demandes de renseignements sur la vie privée émanant du public et y répondre. **27.2.2** Les procédures doivent au moins inclure : 1. les renseignements à fournir aux personnes qui exercent leur droit d'accès en vertu de l'article 10 de la *Loi sur l'AIPVP* et/ou aux personnes qui exercent leurs droits d'accès et de rectification en vertu de l'article 47 de la *Loi sur l'AIPVP*, notamment les renseignements sur le lieu et le destinataire des demandes;

	2. que lorsqu'une plainte ou une demande de renseignements porte sur une atteinte réelle ou présumée à la vie privée ou à la sécurité, elle sera également traitée conformément au protocole de gestion des atteintes à la vie privée du service d'intégration des données, conformément à l'exigence 14; 3. que les personnes qui déposent une plainte ou une demande de renseignements doivent recevoir une réponse à leur plainte ou demande de renseignements les informant des mesures qui seront ou ont été prises, le cas échéant, pour résoudre la plainte ou la demande de renseignements (ceci peut avoir lieu à différentes étapes du processus); 4. que les personnes qui déposent une plainte ou une demande de renseignements doivent être informées qu'elles peuvent déposer une plainte auprès du CIPVP et recevoir les renseignements nécessaires pour communiquer avec le CIPVP, ainsi qu'une description des fonctions du CIPVP en vertu de l'article 49.12 de la Partie; 5. le processus permettant de déterminer quand la notification doit être fournie au CIPVP, en fonction de la portée de la plainte ou de l'enquête et d'autres facteurs pertinents. **27.2.3** La publication des détails du processus en anglais et en français sur un site Web du gouvernement de l'Ontario ou, dans le cas d'un service extraministériel d'intégration des données, sur le site Web de la personne ou de l'entité. **27.2.4** Employer un langage clair et facile à comprendre dans les détails du processus.
27.3	**27.3.1** Établir et tenir un registre des plaintes relatives à la protection de la vie privée reçues par le service d'intégration des données. **27.3.2** Le registre doit au moins comprendre ce qui suit : 1. la date de réception de la plainte; 2. la nature de la plainte; 3. la ou les mesures prises pour résoudre la plainte et la date à laquelle le plaignant a été informé de la ou des mesures prises; 4. le délai dans lequel la plainte a été traitée; 5. le résultat de la plainte ou de l'enquête (notamment toute recommandation formulée à la suite d'une enquête, le délai dans lequel ces recommandations doivent être traitées, le nom du ou des membres chargés de les traiter et les dates auxquelles les recommandations ont été traitées).

PUBLICATION D’AUTRES DOCUMENTS

Pour favoriser la transparence et la reddition de comptes, les services d’intégration des données doivent mettre à la disposition du public d’autres documents relatifs aux politiques, aux procédures et aux opérations du service d’intégration des données. Il peut s’agir d’une référence à des publications de renseignements ouvertes, de documents relatifs aux examens de la CIPVP et de questions fréquemment posées.

GLOSSAIRE DES TERMES

Terme	Définition
Anonymisation	« anonymisation » au sens de la Partie.
Atteinte à la sécurité	Une situation dans laquelle : • il existe une atteinte réelle ou potentielle à la confidentialité, à l'intégrité ou à la disponibilité de l'environnement d'intégration des données du service d'intégration des données, ou l'environnement d'intégration des données est autrement exposé à un risque accru; • une infraction à la Partie, aux normes relatives aux données, aux pratiques et procédures, aux autres dispositions applicables de la *Loi sur l'AIPVP* ou de ses règlements, ou aux accords ou reconnaissances faits en vertu de ceux-ci concernant : - conservation, transfert, élimination ou destruction en toute sécurité; - anonymisation et établissement de liens.
Atteinte à la vie privée	Tout vol ou toute perte de renseignements personnels ou codés ou toute collecte, utilisation ou divulgation de renseignements personnels ou codés qui n'est pas autorisée en vertu de la Partie, des normes relatives aux données, des pratiques et procédures, des autres dispositions applicables de la Loi sur l'*AIPVP* ou de ses règlements, et des accords et reconnaissances faits en vertu de ceux-ci.
Élimination en toute sécurité ou destruction	Le retrait permanent d'un renseignement contenu dans un support de données de telle sorte que sa reconstruction ou sa récupération n'est pas raisonnablement prévisible en la circonstance.
Environnement d'intégration des données	Tous les composants de système et les ressources d'information associés de l'environnement technologique d'un service d'intégration des données, notamment : • le matériel, les logiciels, les applications, les systèmes de sécurité, les appareils de réseau et les serveurs; • RP, renseignements codés, renseignements anonymisés, registres et données d'authentification.

Établissement de liens	Une méthode permettant de rassembler des renseignements provenant de différentes sources sur une même personne.
Identifiant direct	Variables qui fournissent un lien explicite avec une personne concernée et qui peuvent identifier directement une personne. Par exemple, le nom, l'adresse, l'adresse électronique, le numéro de téléphone, le numéro de télécopieur, le numéro de carte de crédit, le numéro de plaque d'immatriculation, le numéro d'identification du véhicule, le numéro d'assurance sociale, le numéro de la carte de santé, le numéro du dossier médical, l'identifiant du dispositif, les identifiants biométriques, le numéro d'adresse du protocole internet (IP) et le localisateur universel de ressources du Web (URL).
Identifiant indirect	Variables qui peuvent ne pas identifier directement une personne, mais qui peuvent néanmoins être utilisées pour une désanonymisation indirecte. Ces identifiants peuvent être utilisés, seuls ou avec d'autres renseignements disponibles, pour identifier une personne. Par exemple, le sexe, la date de naissance ou l'âge, les dates d'événements (p. ex., décès, admission, procédure, sortie, visite), les lieux (p. ex., codes postaux, noms de bâtiments, régions), l'origine ethnique, le pays de naissance, les langues parlées, le statut d'autochtone, le statut de minorité visible, la profession, l'état civil, le niveau d'éducation, le nombre total d'années de scolarité, les antécédents criminels, le revenu total et la confession religieuse.
Loi sur l'AIPVP	La *Loi de 1990 sur l'accès à l'information et la protection de la vie privée*
La Partie	Partie III. (Intégration des données) de la *Loi sur l'AIPVP*
Membre	Un « membre » d'un service d'intégration des données au sens de la Partie.
Plaintes relatives à la protection de la vie privée	Préoccupations ou plaintes relatives à la conformité d'un service d'intégration des données : • La Partie; • Les normes relatives aux données; • Les pratiques et procédures; • Les autres dispositions applicables de la *Loi sur* l'*AIPVP* ou de ses règlements; Les accords ou les reconnaissances faits en vertu de ceux-ci.

Renseignements codés	Renseignements personnels dont les identifiants directs ont été supprimés et remplacés par un code interne.
Renseignements personnels (RP)	Les « renseignements personnels » au sens de la *Loi sur l'AIPVP.*
Service d'intégration des données	Un « service ministériel d'intégration des données », un « service interministériel d'intégration des données » ou un « service extraministériel d'intégration des données » au sens prévu par la Partie III.
Supports de données	Le support physique sous-jacent sur lequel les renseignements sont sauvegardés, généralement classé sous deux formes : non électronique et électronique. Les imprimés sur papier et les notes manuscrites sont des exemples de supports de données non électroniques. Les supports de données électroniques comprennent par exemple les disques durs des ordinateurs, les disques durs des photocopieuses et des imprimantes, les disques solides amovibles, y compris la mémoire, les disques et les clés USB, les téléphones mobiles et les bandes magnétiques.
Supprimer	La suppression de toute référence électronique au renseignement ou, dans le cas de supports de données non électroniques, l'accès physique au renseignement.