Répertoire des personnes assurées

Évaluation des incidences sur la vie privée

Avril 2022

Institut canadien d'information sur la santé
Canadian Institute for Health Information

La production du présent document est rendue possible grâce à un apport financier de Santé Canada et des gouvernements provinciaux et territoriaux. Les opinions exprimées dans ce rapport ne représentent pas nécessairement celles de Santé Canada ou celles des gouvernements provinciaux et territoriaux.

Institut canadien d'information sur la santé
495, chemin Richmond, bureau 600
Ottawa (Ontario) K2A 4H6
Téléphone : 613-241-7860
Télécopieur : 613-241-8120
icis.ca
droitdauteur@icis.ca

Comment citer ce document :
Institut canadien d'information sur la santé. *Évaluation des incidences sur la vie privée du répertoire des personnes assurées, avril 2022*. Ottawa, ON : ICIS; 2022.

This publication is also available in English under the title *Insured Persons Repository Privacy Impact Assessment, April 2022*.

L'Institut canadien d'information sur la santé (ICIS) est fier de publier l'évaluation des incidences sur la vie privée suivante conformément à sa *Politique d'évaluation des incidences sur la vie privée* :

- *Évaluation des incidences sur la vie privée du répertoire des personnes assurées, avril 2022*

Approuvé par

Brent Diverty
Vice-président, Stratégies de données et Statistiques

Rhonda Wing
Directrice exécutive, chef de la protection des renseignements personnels et avocate générale, Bureau de la chef de la protection des renseignements personnels et des services juridiques

Ottawa, avril 2022

Table des matières

Le répertoire des personnes assurées (RPA) en bref

1. Le RPA a été créé pour
   - soutenir l'élaboration et l'évolution de la méthodologie de regroupement de la population de l'ICIS. Ce regroupement ajusté selon les risques de la population sert de mesure composite du fardeau de la maladie ou de l'utilisation future des services de santé par les membres d'une population, qu'ils soient utilisateurs du système de santé ou non. Une évaluation des incidences sur la vie privée de la méthodologie de regroupement de la population et des diverses sources de données sous-jacentes, dont les données du RPA, est également accessible au icis.ca;
   - favoriser la réalisation d'analyses axées sur les patients — utilisation des soins de santé ajustée en fonction de l'âge, du sexe et de la morbidité dans différentes populations — qu'il est difficile d'effectuer à l'heure actuelle à partir d'autres sources de données.
2. Le RPA recueille des renseignements personnels sur la santé de tous les clients et sur leur admissibilité à l'assurance maladie, qu'ils aient accédé ou non au système de santé.
3. En 2013, 3 provinces ont fourni un fichier d'extraction ad hoc de leurs données sur les personnes assurées afin de faciliter l'élaboration initiale de la méthodologie de regroupement de la population de l'ICIS.
4. Depuis 2021, la Nouvelle-Écosse, l'Ontario et la Saskatchewan soumettent des données au RPA de l'ICIS. L'Alberta a aussi fourni des données au RPA, mais leur utilisation est actuellement limitée à l'amélioration de la méthodologie de regroupement de la population de l'ICIS. L'ICIS poursuit son travail auprès des autres autorités compétentes afin d'obtenir une couverture nationale pour le RPA.

1 Introduction

L'Institut canadien d'information sur la santé (ICIS) recueille et analyse de l'information sur la santé et les soins de santé au Canada. Il a pour mandat de fournir une information comparable et exploitable qui favorise une amélioration rapide des soins de santé, de la performance des systèmes de santé et de la santé de la population dans l'ensemble du continuum de soins. L'ICIS obtient des données des hôpitaux et d'autres établissements de santé, des établissements de soins de longue durée, des autorités sanitaires régionales, des praticiens et des gouvernements. Ces données comprennent des renseignements sur les services de santé dispensés aux patients, sur les professionnels de la santé qui dispensent ces services et sur le coût des services de santé.

La présente évaluation des incidences sur la vie privée a pour but d'examiner les risques liés au respect de la vie privée, à la confidentialité et à la sécurité associés au répertoire des personnes assurées (RPA). Elle consiste en un examen des 10 principes énoncés dans le *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation, et de la façon dont ils s'appliquent au RPA. Elle analyse aussi l'application du *Cadre de gestion des risques liés au respect de la vie privée et à la sécurité* de l'ICIS.

Cette évaluation vise avant tout à respecter la *Politique d'évaluation des incidences sur la vie privée* de l'ICIS.

2 Contexte

2.1 Présentation du répertoire des personnes assurées

En 2013, l'ICIS commençait à élaborer sa méthodologie de regroupement de la population. L'objectif était d'élaborer une méthodologie et un logiciel de regroupement de la population à partir des données et de l'expertise de l'ICIS. D'ordre clinique, la méthodologie regroupe toute la population et repose sur un ensemble de groupes ou de cellules qui décrivent l'état clinique des personnes et la gravité de leurs problèmes de santé. Les groupes cliniques et les modèles prévisionnels connexes utilisent les données à l'échelle des patients provenant de sources de données multiples.

Une source de données cruciale pour l'élaboration de la méthodologie, mais qui n'existait pas en 2013, est le RPA. Les données du RPA sont les seules à inclure tous les membres de la population assurés, qu'ils aient ou non accédé au système de santé. Dans la conception d'un modèle prédictif, il est important de tenir compte de la population entière, même des personnes qui n'ont pas utilisé le système de santé, car elles ont toutes le potentiel de devenir des utilisateurs.

3 provinces (l'Ontario, l'Alberta et la Colombie-Britannique) ont initialement fourni à l'ICIS un fichier d'extraction ad hoc des données de leur propre RPA afin de l'aider à créer sa méthodologie de regroupement de la population. Afin d'élargir la couverture de son RPA et de faire évoluer sa méthodologie, l'ICIS a commencé à collaborer avec d'autres provinces pour établir une collecte régulière de données. En date de 2022, la Nouvelle-Écosse, l'Ontario et la Saskatchewan fournissent régulièrement des données au RPA de l'ICIS. L'Alberta soumet également des données, mais pour l'instant, celles-ci peuvent être utilisées uniquement pour améliorer la méthodologie de regroupement de la population.

2.2 Collecte de données

Les ministères provinciaux et territoriaux de la Santé maintiennent une liste des numéros d'assurance maladie incluant les caractéristiques de leurs titulaires et indiquant leur admissibilité à l'assurance maladie provinciale ou territoriale. Les données recueillies à cette fin première sont par la suite soumises à l'ICIS. Chaque enregistrement soumis au RPA est représentatif du fichier de données provincial ou territorial qui respecte, dans la mesure du possible, les exigences du fichier minimal demandé par l'ICIS. Il comprend les éléments suivants :

- Numéro d'assurance maladie
- Code postal du patient
- Date de naissance du patient
- Sexe du patient

2.3 RPA : gestion de l'accès, soumission des données et cheminement des données

Chaque fournisseur de données (c.-à-d. chaque ministère provincial ou territorial de la Santé) extrait de ses sources de données existantes un fichier de données provincial ou territorial qui respecte, dans la mesure du possible, les exigences du fichier minimal demandé par l'ICIS.

L'accès aux applications sécurisées de l'ICIS est soumis au processus de gestion de l'accès en fonction du type d'utilisateur de l'ICIS, qui est géré par le service Gestion de produits et Expérience client. Ce service gère l'autorisation et la révocation de l'accès aux applications sécurisées de l'ICIS conformément aux processus établis du système de gestion de l'accès (SGA).

Une fois authentifiés dans le SGA, les fournisseurs de données du RPA soumettent à l'ICIS des données au niveau de l'enregistrement par l'intermédiaire du Service de soumission électronique de données (eDSS) sécurisé de l'ICIS ou d'une autre connexion directe serveur à serveur.

Une fois les fichiers de données du RPA reçus par l'ICIS, la présence d'erreurs et d'incohérences est automatiquement vérifiée selon des spécifications propres à chaque province ou territoire, et le numéro d'assurance maladie provincial ou territorial de chaque enregistrement est chiffré. Une fois le chiffrement effectué, un nombre limité d'employés autorisés procède au traitement secondaire de chaque fichier provincial ou territorial de données du RPA avant que les fichiers soient transférés dans l'environnement analytique SAS de l'ICIS. Ce traitement secondaire peut inclure la correction d'erreurs en consultation avec les fournisseurs de données (ce qui leur évite de devoir soumettre de nouveau les données) et la suppression des éléments de données inutiles aux analyses périodiques réalisées dans l'environnement SAS.

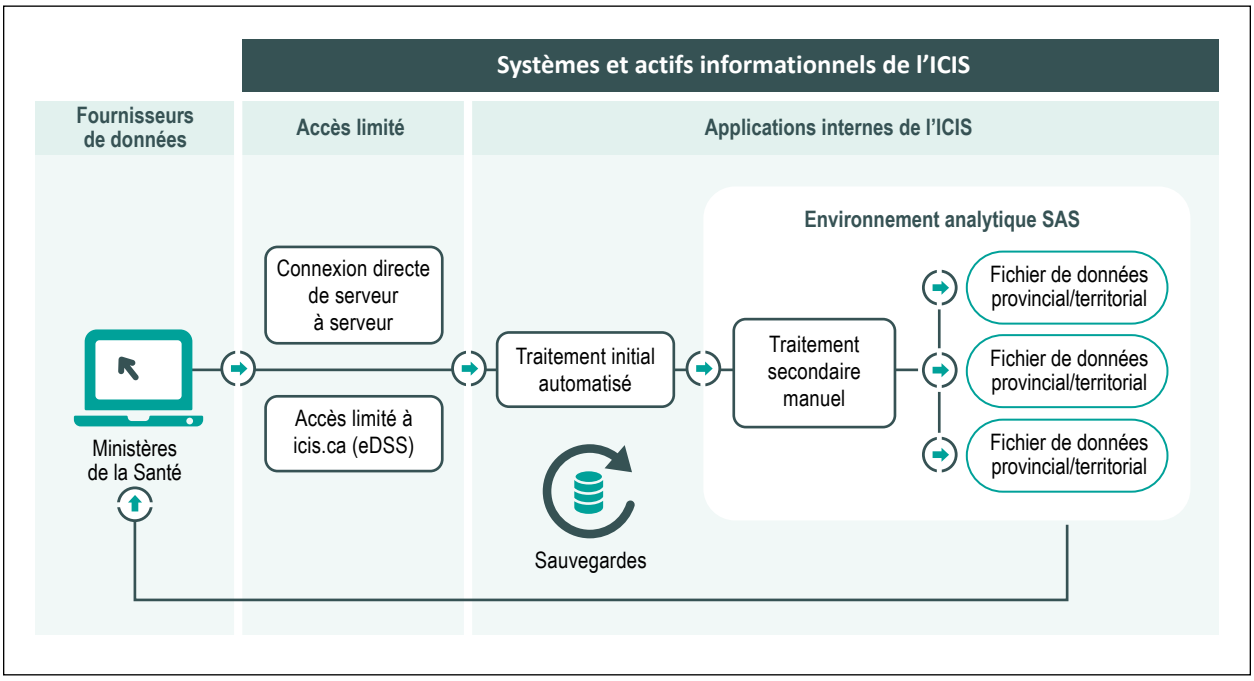
Une fois les données soumises, traitées et enregistrées dans le RPA, une copie du fichier de données du RPA est téléchargée dans l'environnement analytique SAS de l'ICIS et mise à la disposition du personnel autorisé pour les besoins de l'ICIS. Le personnel peut accéder aux données du RPA au moyen de l'environnement analytique SAS de l'ICIS, qui est géré par un processus centralisé d'accès aux données SAS conformément aux politiques en matière d'accès aux données de l'ICIS.

L'ICIS renvoie les données du RPA au fournisseur qui a d'abord soumis les données, à savoir le ministère de la Santé concerné.

Des copies des données et des applications de l'ICIS sont conservées dans des systèmes de sauvegarde.

Le cheminement des données pour le RPA est illustré dans son ensemble par la figure suivante.

Figure Aperçu du cheminement des données pour le répertoire des personnes assurées



3 Analyse du respect de la vie privée

3.1 Programme de gestion des risques liés au respect de la vie privée et à la sécurité

La gestion des risques en matière de respect de la vie privée et de sécurité est un processus officiel et reproductible qui vise la détection, l'évaluation, la prise en charge et la surveillance des risques dans le but de réduire au minimum la probabilité qu'ils se matérialisent ou leurs éventuelles incidences. En 2015, l'ICIS a approuvé son *Cadre de gestion des risques liés au respect de la vie privée et à la sécurité* et mis en œuvre la *Politique sur la gestion des risques liés au respect de la vie privée et à la sécurité* connexe. La chef de la protection des renseignements personnels et le chef de la sécurité de l'information de l'ICIS, en collaboration avec des membres de la direction, ont la responsabilité de détecter, évaluer, prendre en charge, surveiller et examiner les risques en matière de respect de la vie privée et de sécurité.

Les risques liés au respect de la vie privée et à la sécurité peuvent être détectés de diverses façons, notamment par des évaluations des incidences sur la vie privée. Une fois détectés, les risques sont inscrits au registre des risques liés au respect de la vie privée et à la sécurité, et reçoivent la cote **élevé**, **moyen** ou **faible** selon leur probabilité et leur incidence :

- **élevé :** la probabilité que le risque se manifeste est élevée, ou les mesures de contrôle et les stratégies ne sont pas fiables ou efficaces;
- **moyen :** la probabilité que le risque se manifeste est moyenne, ou les mesures de contrôle et les stratégies sont moyennement fiables ou efficaces;
- **faible :** la probabilité que le risque se manifeste est faible, ou les mesures de contrôle et les stratégies sont fiables et efficaces.

Le niveau de risque est calculé en fonction de la probabilité et de l'incidence du risque détecté. Le résultat de l'évaluation du niveau de risque (faible, moyen ou élevé) définit le degré de risque. Un niveau de risque élevé est signe d'une menace grave qu'il est impératif de prendre immédiatement en charge. Une fois un premier traitement du risque effectué, le risque résiduel (nouveau calcul de la probabilité et de l'incidence du risque par suite du traitement) est évalué et comparé à l'énoncé sur la tolérance des risques liés au respect de la vie privée et à la sécurité de l'ICIS, qui stipule que l'ICIS a une faible tolérance à de tels risques. Si le niveau de risque résiduel demeure plus élevé que faible, de nouvelles mesures de prise en charge doivent être appliquées jusqu'à ce que le risque soit faible, ou jusqu'à ce que le risque non pris en charge ou résiduel soit accepté par le Comité exécutif de l'ICIS au nom de l'organisme.

Aucun risque lié au respect de la vie privée et à la sécurité n'a été détecté à la suite de cette évaluation des incidences sur la vie privée.

3.2 Textes législatifs régissant les données du RPA

Généralités

L'ICIS se conforme à sa *Politique de respect de la vie privée, 2010* ainsi qu'à toute loi ou entente juridique sur la vie privée applicable.

Lois sur la protection de la vie privée

L'ICIS est un collecteur secondaire de données sur la santé, expressément à des fins de planification et de gestion du système de santé, ce qui comprend l'analyse statistique et la production de rapports. Il incombe aux fournisseurs de données de respecter les obligations légales prévues dans leur province ou territoire, selon le cas, au moment de la collecte des données.

Les provinces et territoires suivants disposent de lois sur la protection des renseignements personnels sur la santé : Terre-Neuve-et-Labrador, Île-du-Prince-Édouard, Nouvelle-Écosse, Nouveau-Brunswick, Ontario, Manitoba, Saskatchewan, Alberta, Yukon et Territoires du Nord-Ouest. Ces lois octroient aux établissements l'autorisation de divulguer des renseignements personnels sur la santé sans le consentement des patients pour les besoins des systèmes de santé et à condition que certaines exigences soient remplies. Par exemple, l'ICIS est reconnu comme une entité prescrite en vertu de la *Loi sur la protection des renseignements personnels sur la santé* de l'Ontario; les dépositaires de renseignements sur la santé de l'Ontario peuvent donc divulguer de tels renseignements à l'ICIS sans le consentement des patients en vertu de l'article 29, comme le prévoit l'alinéa 45(1) de la Loi.

Les établissements situés dans des provinces et territoires qui ne disposent pas de lois sur la protection des renseignements personnels sur la santé sont assujettis aux lois régissant le secteur public. Ces lois donnent aux établissements le droit de divulguer des renseignements personnels à des fins statistiques sans le consentement de la personne concernée.

Ententes

À l'ICIS, les données du RPA sont régies par la *Politique de respect de la vie privée, 2010*, la législation en vigueur dans les provinces et territoires et les ententes de partage de données conclues avec les provinces et territoires. Les ententes de partage des données établissent les critères relatifs au but, à l'utilisation, à la divulgation, à la conservation et à la destruction des renseignements personnels sur la santé fournis à l'ICIS, ainsi que toute divulgation subséquemment permise. Les ententes décrivent aussi l'autorité législative selon laquelle les renseignements personnels sur la santé sont divulgués à l'ICIS.

3.3 Premier principe : responsabilité à l'égard des renseignements personnels sur la santé

Il incombe au président-directeur général de l'ICIS de s'assurer de la conformité à la *Politique de respect de la vie privée, 2010* de l'ICIS. À cet égard, l'ICIS compte sur une chef de la protection des renseignements personnels et avocate générale, un comité sur le respect de la vie privée, la confidentialité et la sécurité, un comité de gouvernance et de respect de la vie privée issu du Conseil d'administration et un conseiller principal externe à la protection des renseignements personnels.

Organisation et gouvernance

Le tableau qui suit présente les principaux postes de direction à l'ICIS responsables de la gestion des risques liés au respect de la vie privée et à la sécurité pour les données du RPA.

Tableau Principaux postes et responsabilités

Poste ou groupe	Rôles et responsabilités
Vice-président, Stratégies de données et Statistiques	Responsable du fonctionnement général et de l'orientation stratégique du RPA
Directrice, Services d'information sur les produits pharmaceutiques et la main-d'œuvre de la santé	Responsable de la prise de décisions stratégiques et opérationnelles concernant le RPA
Gestionnaire, Information sur les médecins	Responsable de la gestion continue et de la mise en place du RPA, ainsi que de la prise de décisions opérationnelles quotidiennes relatives au RPA
Chef de la sécurité de l'information	Responsable de l'orientation stratégique et de la mise en œuvre générale du programme de sécurité de l'information de l'ICIS
Directrice exécutive, chef de la protection des renseignements personnels et avocate générale	Responsable de l'orientation stratégique et de la mise en œuvre générale du programme de respect de la vie privée de l'ICIS
Gestionnaire, Opérations d'affaires et d'infrastructure	Responsable du respect des exigences techniques relatives à la soumission électronique sur le Web et au traitement initial des données, y compris le chiffrement des numéros d'assurance maladie provinciaux ou territoriaux avant le transfert des fichiers de données du RPA à l'environnement analytique SAS de l'ICIS

3.4 Deuxième principe : établissement des objectifs de la collecte de renseignements personnels sur la santé

L'ICIS a pour mandat de fournir une information comparable et exploitable qui favorise une amélioration rapide des soins de santé, de la performance des systèmes de santé et de la santé de la population dans l'ensemble du continuum des soins. L'ICIS doit donc notamment veiller à

- soutenir l'élaboration et l'évolution de sa méthodologie de regroupement de la population;
- favoriser la réalisation d'analyses axées sur les patients — utilisation des soins de santé ajustée en fonction de l'âge, du sexe et de la morbidité dans différentes populations — qu'il est difficile d'effectuer à l'heure actuelle à partir d'autres sources de données.

Pour ce faire, l'ICIS recueille les types suivants de données du RPA aux fins indiquées.

Identificateurs personnels et renseignements démographiques

Ces éléments de données comprennent le numéro d'assurance maladie, la date de naissance, le code postal et le sexe. L'ICIS utilise ces informations pour brosser le portrait complet des soins fournis à la personne en regroupant les enregistrements décrivant les divers types de soins qui lui ont été fournis à divers moments par divers établissements. Afin de pouvoir réunir les enregistrements, l'ICIS doit savoir lesquels se rapportent à la personne. Par conséquent, tous les enregistrements doivent inclure des identificateurs, surtout le numéro d'assurance maladie de la personne. L'ICIS utilise l'âge dérivé de la date de naissance, l'information géographique dérivée du code postal et le sexe pour réaliser des analyses démographiques des services de santé fournis et de leurs résultats.

3.5 Troisième principe : consentement pour la collecte, l'utilisation ou la divulgation de renseignements personnels sur la santé

À titre de collecteur secondaire de données, l'ICIS n'a pas de contact direct avec les patients. L'ICIS s'attend à ce que les fournisseurs de données respectent les règles et leurs responsabilités en matière de collecte, d'utilisation et de divulgation de données, y compris en ce qui concerne le consentement et les avis, comme le prévoient les lois, les règlements et les politiques en vigueur dans les provinces et territoires.

3.6 Quatrième principe : restriction de la collecte de renseignements personnels sur la santé

L'ICIS veille à respecter le principe de la minimisation des données. En vertu des articles 1 et 2 de sa *Politique de respect de la vie privée, 2010*, l'ICIS ne recueille des fournisseurs de données que les renseignements raisonnablement nécessaires pour les besoins du système de santé, dont l'analyse statistique et la production de rapports, à des fins de gestion, d'évaluation ou de surveillance des systèmes de santé.

L'ICIS ne recueille que les renseignements personnels sur la santé nécessaires aux activités autorisées liées à l'analyse et à la qualité des données et poursuit l'élaboration du RPA en collaboration avec les ministères de la Santé du pays. La nature de l'information à recueillir restera déterminée pour chaque province et territoire et évoluera au fil du temps.

Comme indiqué à la section 2.3, les données du RPA ne seront pas recueillies en fonction de spécifications obligatoires de soumission des données publiées par l'ICIS, qui établissent généralement des contraintes strictes concernant la disposition du fichier et les variables pour la soumission des données. Il est donc possible qu'un fournisseur de données du RPA soumette par mégarde des données superflues. L'ICIS s'efforce d'atténuer ce risque de plusieurs manières.

Premièrement, l'ICIS a établi une liste des éléments de données requis (c.-à-d. le fichier minimal) et s'en sert dans ses négociations avec chaque fournisseur de données potentiel pour s'assurer que seules les données essentielles au RPA sont soumises. Deuxièmement, l'ICIS dispose de son propre processus de dépersonnalisation des données pour chiffrer les numéros d'assurance maladie. Si la structure du fichier ne correspond pas aux attentes (p. ex. si des renseignements supplémentaires sont inclus), le processus de dépersonnalisation échoue. Le cas échéant, l'équipe Opérations d'affaires et d'infrastructure informe la section de programme du problème de fichier, et celle-ci demande ensuite au fournisseur de vérifier les données soumises.

Troisièmement, le personnel de l'ICIS a mis en place d'autres procédures pour repérer manuellement les éléments de données superflus. Ce repérage a lieu durant la phase de traitement secondaire (voir la section 2.3) de chaque fichier de données du RPA, avant son transfert à l'environnement analytique SAS. Tout élément de données non exigé par l'ICIS est supprimé du fichier de soumission lors de cette phase de traitement secondaire, et l'ICIS demande à la province ou au territoire d'ajuster ses spécifications pour les soumissions futures. Les éléments de données requis pour les besoins du RPA, mais inutiles aux activités courantes de l'environnement analytique SAS de l'ICIS, ne sont accessibles que de façon exceptionnelle, sous réserve d'autorisation conforme aux procédures et à la *Politique de respect de la vie privée, 2010*, de l'ICIS.

3.7 Cinquième principe : restriction de l'utilisation, de la divulgation et de la conservation des renseignements personnels sur la santé

Restriction de l'utilisation

Clients

L'ICIS restreint l'utilisation des données du RPA aux objectifs autorisés décrits à la section 3.4. Cela comprend les analyses comparatives dans et entre chaque province et territoire, les analyses des tendances visant à évaluer et à surveiller l'incidence de tout changement en matière de politiques, de pratiques et de prestation de services, ainsi que la production de statistiques pour appuyer la planification, la gestion et l'amélioration de la qualité.

Personnel de l'ICIS

Le personnel de l'ICIS est autorisé à accéder aux données et à les utiliser uniquement en cas de nécessité, notamment pour la gestion du traitement et de la qualité des données, la production de statistiques et de fichiers de données, ainsi que la réalisation d'analyses. Tous les membres du personnel de l'ICIS doivent signer une entente de confidentialité au moment de leur embauche, et sont ensuite tenus de renouveler chaque année leur engagement à l'égard du respect de la vie privée.

L'accès du personnel à l'environnement analytique SAS est fourni au moyen du processus centralisé d'accès aux données SAS de l'ICIS, qui est géré par le Centre de services de l'ICIS. Cet environnement distinct et sécurisé sert au stockage des fichiers de données analytiques. Le personnel peut s'en servir pour effectuer des analyses et stocker les résultats.

Ce processus garantit que toutes les demandes d'accès, y compris aux données du RPA, sont vérifiables et autorisées, conformément à l'article 10 de la *Politique de respect de la vie privée, 2010* de l'ICIS. Le processus d'accès aux données SAS fait l'objet d'une vérification annuelle qui permet de confirmer que les employés accèdent aux données seulement en cas de nécessité. L'article 3.9 explique comment les différentes mesures procédurales et techniques sont mises en place en vue de prévenir l'accès non autorisé aux données du RPA et de sécuriser les données de toute autre manière.

Couplage des données

Les données du RPA sont couplées avec les données d'autres sources de l'ICIS. Comme le couplage des données peut accroître les risques d'identification de la personne, l'ICIS prend des mesures d'atténuation des risques.

Les articles 14 à 31 de la *Politique de respect de la vie privée, 2010* de l'ICIS régissent le couplage des enregistrements contenant des renseignements personnels sur la santé. En vertu de cette politique, l'ICIS permet le couplage des renseignements personnels sur la santé dans certaines circonstances. Il est généralement permis de coupler des données au sein d'une seule banque de données pour l'usage exclusif de l'ICIS. Le couplage de données à partir de multiples banques de données pour l'usage exclusif de l'ICIS et toutes les demandes de couplage de données formulées par des tiers sont soumis à un processus interne d'examen et d'approbation. Lors du couplage, l'ICIS utilise généralement des numéros d'assurance maladie chiffrés. Les données couplées demeurent assujetties aux dispositions en matière d'utilisation et de divulgation de la *Politique de respect de la vie privée, 2010*.

Les critères d'approbation du couplage de données sont énoncés comme suit aux articles 23 et 24 de la *Politique de respect de la vie privée, 2010* de l'ICIS :

Article 23 Les personnes dont les renseignements personnels sur la santé sont utilisés pour le couplage de données y consentent au préalable. OU

Article 24 Tous les critères suivants sont respectés :

a. l'objectif du couplage de données s'inscrit dans le mandat de l'ICIS;
b. les avantages pour le public sont considérablement plus importants que les risques de violation de la vie privée des personnes;
c. les résultats du couplage de données ne porteront pas préjudice aux personnes concernées;
d. le couplage de données s'inscrit dans un projet précis et ponctuel, et les données couplées seront par la suite détruites dans le respect des règles énoncées aux articles 28 et 29;
e. le couplage de données est effectué dans le cadre d'un programme de travail continu et approuvé de l'ICIS; les données sont conservées aussi longtemps que nécessaire pour la réalisation des fins déterminées, après quoi elles sont détruites dans le respect des règles énoncées aux articles 28 et 29;
f. le couplage de données permet de réaliser des économies évidentes par rapport à d'autres méthodes ou est l'unique méthode envisageable.

Norme de couplage de données sur les clients

En 2015, l'ICIS a adopté une norme de couplage de données sur les clients à l'échelle de l'organisme. Cette norme régit le couplage des enregistrements qui ont été créés depuis 2010-2011 et qui contiennent les éléments de données suivants : numéro d'assurance maladie chiffré et province ou territoire ayant émis le numéro d'assurance maladie. Les enregistrements qui ne satisfont pas à ces critères sont régis par un mécanisme de couplage défini au cas par cas.

Destruction des données couplées

L'article 28 de la *Politique de respect de la vie privée, 2010* de l'ICIS définit l'exigence selon laquelle l'ICIS doit détruire les renseignements personnels sur la santé et les données dépersonnalisées de façon sécuritaire, à l'aide de méthodes de destruction qui conviennent au format, au support ou au dispositif, de manière à ce qu'une reconstitution ne soit pas raisonnablement prévisible.

Pour certains projets ponctuels, l'article 29 de la *Politique de respect de la vie privée, 2010* de l'ICIS prévoit par ailleurs que la destruction sécuritaire des données couplées aura lieu dans l'année suivant la publication de l'analyse ou dans les 3 années suivant le couplage, selon la première éventualité, conformément à la *norme de destruction de l'information* de l'ICIS. S'il s'agit de données couplées dans le cadre d'un programme de travail continu, une destruction sécuritaire doit avoir lieu lorsque les données ne sont plus nécessaires pour la réalisation des fins déterminées, conformément à la *norme de destruction de l'information* de l'ICIS. Cette exigence s'applique au couplage de données tant pour l'usage exclusif de l'ICIS que pour les demandes formulées par des tiers.

Renvoi des données au fournisseur

Sur demande, l'ICIS peut fournir à un organisme une copie des données qu'il a soumises au RPA, sous forme de renvoi au fournisseur. L'article 34 de la *Politique de respect de la vie privée, 2010* stipule que l'ICIS, en plus de renvoyer les données aux organismes déclarants, peut également remettre les enregistrements au ministère concerné, pour des motifs de qualité des données ou à d'autres fins inscrites dans son mandat (p. ex. la gestion des services de santé et de la santé de la population, qui comprend la planification, l'évaluation et l'affectation des ressources). Le renvoi des données au fournisseur de données est considéré comme une utilisation et non comme une divulgation.

Restriction de la divulgation

Demandes de données formulées par des tiers

Les données du RPA ne sont pas accessibles dans le cadre du processus de demande de données par des tiers de l'ICIS.

Diffusion publique

L'ICIS ne diffuse pas publiquement de données agrégées tirées du RPA.

Restriction de la conservation

Le RPA fait partie des banques de données de l'ICIS. Conformément à son mandat et à ses fonctions de base, l'ICIS conserve les données de ce système aussi longtemps que nécessaire pour la réalisation des fins déterminées.

3.8 Sixième principe : exactitude des renseignements personnels sur la santé

L'ICIS dispose d'un programme complet sur la qualité des données. Tout problème connu de qualité des données doit être réglé par le fournisseur de données ou consigné dans la documentation sur les limites des données, que l'ICIS fournit à tous les utilisateurs.

À l'instar d'autres banques de données de l'ICIS, le RPA doit subir régulièrement une évaluation de la qualité des données fondée sur le *Cadre de la qualité de l'information* de l'ICIS. Ce processus comprend de nombreuses activités visant à évaluer les diverses dimensions de la qualité, dont l'exactitude des données du RPA.

3.9 Septième principe : mesures de protection des renseignements personnels sur la santé

Cadre de respect de la vie privée et de sécurité de l'ICIS

L'ICIS a élaboré un *Cadre de respect de la vie privée et de sécurité* visant à offrir une approche globale de la gestion du respect de la vie privée et de la sécurité. Ce cadre est fondé sur des pratiques exemplaires des secteurs public et privé ainsi que du secteur de la santé. Il est conçu de façon à coordonner les politiques de l'ICIS en matière de respect de la vie privée et de sécurité, et à offrir une vision intégrée des pratiques de gestion de

l'information adoptées par l'organisme. Les paragraphes qui suivent décrivent les aspects de la sécurité des systèmes de l'ICIS qui revêtent une importance particulière au regard des données du RPA.

Sécurité des systèmes

L'ICIS reconnaît que l'information peut être considérée comme sécurisée uniquement si elle est protégée pendant tout son cycle de vie, c'est-à-dire à chaque étape des processus de création, de collecte, d'accès, de conservation, de stockage, d'utilisation, de divulgation et de destruction. Par conséquent, l'ICIS dispose d'un ensemble complet de politiques qui définissent les contrôles nécessaires pour garantir la protection de l'information en format physique et électronique, y compris des mesures rigoureuses de chiffrement et d'élimination. Ces politiques ainsi que les normes, lignes directrices et procédures opérationnelles qui s'y rattachent sont conformes aux pratiques exemplaires en matière de respect de la vie privée, de sécurité de l'information et de gestion des enregistrements, afin de garantir la confidentialité, l'intégrité et la disponibilité des actifs informationnels de l'ICIS.

Les registres de contrôle et de vérification du système font partie intégrante du programme de sécurité de l'information de l'ICIS. Qui plus est, ces registres sont immuables. En général, l'ICIS utilise des données dépersonnalisées au niveau de l'enregistrement (où le numéro d'assurance maladie a été supprimé ou chiffré) pour réaliser ses analyses. Il arrive dans des circonstances exceptionnelles que le personnel doive avoir accès aux numéros d'assurance maladie d'origine. Les procédures et la *Politique de respect de la vie privée, 2010* de l'ICIS prévoient des contrôles stricts qui garantissent que l'accès est autorisé dans les circonstances et au niveau appropriés, et que le principe de minimisation des données est respecté en tout temps. L'ICIS consigne dans ses registres les activités suivantes ayant trait à l'accès aux données :

- l'accès aux numéros d'assurance maladie et aux noms des patients (rarement recueillis) dans les bases de données de production de l'ICIS;
- l'accès aux fichiers de données contenant des renseignements personnels sur la santé qui sont extraits des bases de données de production de l'ICIS et mis à la disposition des analystes internes dans des circonstances exceptionnelles;
- la modification des privilèges d'accès dans les bases de données de production.

Les employés de l'ICIS sont sensibilisés à l'importance de maintenir la confidentialité des renseignements personnels sur la santé et d'autres types d'information sensible au moyen d'un programme de formation obligatoire sur le respect de la vie privée et la sécurité, et par l'intermédiaire de communications continues concernant les politiques et procédures de l'ICIS à ce sujet. Avant chaque tentative de connexion à un système d'information de l'ICIS, les employés doivent confirmer qu'ils comprennent l'interdiction d'accéder à ce système informatique ou de l'utiliser sans autorisation expresse de l'ICIS ni au-delà de cette autorisation.

L'ICIS s'emploie à protéger son système de technologies de l'information, à sécuriser ses banques de données ainsi qu'à protéger les renseignements sur la santé en sa possession au moyen de mesures de sécurité administratives, physiques et techniques appropriées, selon la sensibilité de l'information. Les vérifications représentent une composante importante du programme global de sécurité de l'information de l'ICIS. Elles visent à assurer le respect des pratiques exemplaires et à mesurer la conformité avec l'ensemble des politiques, des procédures et des pratiques de sécurité de l'information mises en œuvre par l'ICIS. Les vérifications servent entre autres à évaluer la conformité, sur le plan technique, des systèmes de traitement de l'information aux pratiques exemplaires ainsi qu'aux normes de sécurité et aux normes architecturales connues. Ces vérifications servent également à évaluer la capacité de l'ICIS à protéger l'information et les systèmes de traitement de l'information contre les menaces et vulnérabilités, ainsi que la posture de sécurité globale de l'infrastructure technique de l'ICIS, notamment les réseaux, les serveurs, les coupe-feu, les logiciels et les applications.

Les évaluations de la vulnérabilité et les tests d'intrusion de son infrastructure et de certaines applications, effectués par des tiers sur une base régulière, constituent une composante importante du programme de vérification de l'ICIS. Toutes les recommandations issues de vérifications par des tiers sont consignées dans le registre des recommandations du plan d'action général de l'ICIS, et les mesures qui s'imposent sont prises.

3.10 Huitième principe : transparence de la gestion des renseignements personnels sur la santé

L'ICIS publie des informations concernant ses politiques de protection de la vie privée, ses pratiques en matière de traitement des données et ses programmes de gestion des renseignements personnels sur la santé. Plus précisément, le *Cadre de respect de la vie privée et de sécurité* et la *Politique de respect de la vie privée, 2010* de l'ICIS sont accessibles sur son site Web (icis.ca).

3.11 Neuvième principe : accès individuel et modification apportées aux renseignements personnels sur la santé

L'ICIS n'utilise pas les renseignements personnels sur la santé en sa possession pour prendre des décisions administratives ou relatives aux personnes concernées. Toute personne qui souhaite accéder à ses renseignements personnels sur la santé verra sa demande traitée conformément aux articles 60 à 63 de la *Politique de respect de la vie privée, 2010* de l'ICIS.

3.12 Dixième principe : plaintes concernant le traitement par l'ICIS des renseignements personnels sur la santé

Comme le précisent les articles 64 et 65 de la *Politique de respect de la vie privée, 2010* de l'ICIS, les plaintes, questions et préoccupations concernant le traitement des renseignements par l'ICIS sont examinées par la chef de la protection des renseignements personnels, qui peut acheminer une demande ou une plainte au commissaire au respect de la vie privée de la province ou du territoire de l'auteur de la demande ou de la plainte.

4 Conclusion

L'évaluation du RPA effectuée par l'ICIS n'a relevé aucun risque lié au respect de la vie privée et à la sécurité.

Cette évaluation sera mise à jour ou révisée conformément à la *Politique d'évaluation des incidences sur la vie privée* de l'ICIS.

Annexe

Texte de remplacement pour l’image

Collecte de données par l’ICIS : une fois authentifiés dans le cadre des processus d’autorisation et de révocation de l’accès du système de gestion de l’accès de l’ICIS, les fournisseurs de données du RPA soumettent des données au niveau de l’enregistrement à l’ICIS par le biais de son Service de soumission électronique de données (eDSS) sécurisé ou d’une autre connexion directe serveur à serveur.

Traitement interne des données après la collecte par l’ICIS : la présence d’erreurs et d’incohérences dans les fichiers de données du RPA est automatiquement vérifiée selon des spécifications propres à chaque province et territoire, et le numéro d’assurance maladie provincial ou territorial de chaque enregistrement est chiffré. Les employés autorisés procèdent au traitement secondaire de chaque fichier avant qu’il soit transféré dans l’environnement analytique SAS de l’ICIS. Ce traitement secondaire peut inclure la correction d’erreurs en consultation avec les fournisseurs de données (ce qui leur évite de devoir soumettre de nouveau les données) et la suppression des éléments de données inutiles pour l’environnement SAS.

Sauvegardes : des copies des données du RPA sont conservées dans des systèmes de sauvegarde.

Renvoi, divulgation et utilisation des données par l’ICIS : le personnel de l’ICIS accède aux données de l’environnement analytique SAS en cas de nécessité seulement, dans le but de renvoyer les données au fournisseur qui les a soumises. Les données du RPA ne sont pas accessibles dans le cadre du programme de demande de données par des tiers de l’ICIS, et l’ICIS ne diffuse pas publiquement de données agrégées du RPA.

aide@icis.ca

ICIS Ottawa
495, chemin Richmond
Bureau 600
Ottawa (Ont.)
K2A 4H6
613-241-7860

ICIS Toronto
4110, rue Yonge
Bureau 300
Toronto (Ont.)
M2P 2B7
416-481-2002

ICIS Victoria
880, rue Douglas
Bureau 600
Victoria (C.-B.)
V8W 2B7
250-220-4100

ICIS Montréal
1010, rue Sherbrooke Ouest
Bureau 602
Montréal (Qc)
H3A 2R7
514-842-2226

icis.ca

13861-0522