Base de données sur les soins de santé primaires

Évaluation des incidences sur la vie privée

Mars 2023

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.

À moins d'indication contraire, les données utilisées proviennent des provinces et territoires du Canada.

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. *Base de données sur les soins de santé primaires : évaluation des incidences sur la vie privée, mars 2023*. Ottawa, ON : ICIS; 2023.

This publication is also available in English under the title *Primary Health Care Database Privacy Impact Assessment, March 2023*.

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* :

- *Base de données sur les soins de santé primaires : évaluation des incidences sur la vie privée, mars 2023*

Approuvée par

Brent Diverty
Vice-président, Stratégies de données et Statistiques

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

Ottawa, mars 2023

Table des matières

La Base de données sur les soins de santé primaires en bref 5

1 Introduction 6

2 Contexte 7

2.1 Présentation de la Base de données sur les soins de santé primaires 7

2.2 Collecte de données 8

2.3 Gestion de l'accès et cheminement des données de la Base de données sur les soins de santé primaires 8

3 Analyse du respect de la vie privée 10

3.1 Gestion des risques liés à la vie privée et à la sécurité 10

3.2 Textes législatifs régissant les données de la Base de données sur les soins de santé primaires 11

3.3 Premier principe : responsabilité à l'égard des renseignements personnels sur la santé 12

3.4 Deuxième principe : établissement des objectifs de la collecte de renseignements personnels sur la santé 13

3.5 Troisième principe : consentement pour la collecte, l'utilisation ou la divulgation de renseignements personnels sur la santé 14

3.6 Quatrième principe : restriction de la collecte de renseignements personnels sur la santé 15

3.7 Cinquième principe : restriction de l'utilisation, de la divulgation et de la conservation des renseignements personnels sur la santé 15

3.8 Sixième principe : exactitude des renseignements personnels sur la santé 20

3.9 Septième principe : mesures de protection des renseignements personnels sur la santé 21

3.10 Huitième principe : transparence de la gestion des renseignements personnels sur la santé 23

3.11 Neuvième principe : accès individuel aux renseignements personnels sur la santé et modification de ceux-ci 23

3.12 Dixième principe : plaintes concernant le traitement par l'ICIS des renseignements personnels sur la santé 23

4 Conclusion 23

La Base de données sur les soins de santé primaires en bref

1. Les soins de santé primaires sont, pour la plupart des patients, une porte d'entrée aux systèmes de santé et ils servent de pivot central pour la coordination entre les divers dispensateurs de soins. Ils placent le patient au cœur des soins et mettent l'accent sur l'intégralité et l'interrelation de la santé et du bien-être sur le plan physique, mental et social.
2. Les soins de santé primaires englobent les services de soins primaires ainsi qu'un vaste éventail de services touchant les déterminants sociaux de la santé, comme la scolarité, le revenu, le logement et l'environnement.
3. L'Institut canadien d'information sur la santé (ICIS) recueille des données sur la prestation des services de soins de santé primaires et sur les caractéristiques sociodémographiques des patients aux fins de la Base de données sur les soins de santé primaires.
4. L'ICIS utilise cette base de données pour produire de l'information qui peut servir à orienter la gestion des services de soins de santé primaires, à surveiller la santé de la population, à examiner les taux de dépistage et de vaccination et à cerner les lacunes en matière d'accès aux soins de santé primaires.
5. Depuis 2018, l'ICIS et l'Alliance pour des communautés en santé — un réseau ontarien d'organismes de soins primaires et de centres de santé communautaires — collaborent pour démontrer les avantages de l'utilisation des données sur les soins de santé primaires tirées des dossiers médicaux électroniques.
6. En date de 2022, l'ICIS avait obtenu de l'Alliance des données sur près de 17 millions de visites effectuées par plus de 1 million de patients dans 73 centres de santé communautaires ontariens.
7. Aux fins de son mandat, l'ICIS procède à une collecte de données similaires dans les provinces et territoires où le cadre législatif autorise la divulgation de données sur les soins de santé primaires à l'ICIS.
8. L'ICIS recueille les renseignements suivants aux fins de la Base de données sur les soins de santé primaires : numéro d'assurance maladie, caractéristiques démographiques, renseignements sur la santé et données administratives comme l'identificateur de l'organisme de soins de santé primaires et du dispensateur de services de santé.
9. L'ICIS utilise ces données dans un format dépersonnalisé pour créer de l'information qui appuie les activités du programme sur les soins de santé primaires.

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. Son mandat consiste à 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 à la Base de données sur les soins de santé primaires. Première évaluation des incidences sur la vie privée de l'ICIS à l'égard des soins de santé primaires, 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 à la Base de données sur les soins de santé primaires. 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 de la Base de données sur les soins de santé primaires

Soins de santé primaires

Les soins de santé primaires sont, pour la plupart des patients, une porte d'entrée aux systèmes de santé et ils servent de pivot central pour la coordination entre les divers dispensateurs de soins. Ils placent le patient au cœur des soins et mettent l'accent sur l'intégralité et l'interrelation de la santé et du bien-être sur le plan physique, mental et social. Les soins de santé primaires englobent les services de soins primaires ainsi qu'un vaste éventail de services touchant les déterminants sociaux de la santé, comme la scolarité, le revenu, le logement et l'environnement.

Base de données sur les soins de santé primaires

L'ICIS recueille des données sur la prestation des services de soins de santé primaires et sur les caractéristiques sociodémographiques des patients aux fins de la Base de données sur les soins de santé primaires. Il utilise cette base de données pour produire de l'information qui peut servir à orienter la gestion des services de soins de santé primaires, à surveiller la santé de la population, à examiner les taux de dépistage et de vaccination et à cerner les lacunes en matière d'accès aux soins de santé primaires.

Depuis 2018, l'ICIS et l'Alliance pour des communautés en santé — un réseau ontarien d'organismes de soins primaires et de centres de santé communautaires — collaborent pour démontrer les avantages de l'utilisation des données sur les soins de santé primaires tirées des dossiers médicaux électroniques. En date de 2022, l'ICIS avait obtenu de l'Alliance des données sur près de 17 millions de visites effectuées par plus de 1 million de patients dans 73 centres de santé communautaires ontariens. L'ICIS recueille des données similaires dans les provinces et territoires où le cadre législatif autorise la divulgation de données sur les soins de santé primaires à l'ICIS.

2.2 Collecte de données

L'ICIS recueille les renseignements suivants aux fins de la Base de données sur les soins de santé primaires : numéro d'assurance maladie, caractéristiques démographiques, renseignements sur la santé et données administratives comme l'identificateur de l'organisme de soins de santé primaires et du dispensateur de services de santé. L'ICIS utilise ces données pour appuyer les activités ci-dessus liées au programme sur les soins de santé primaires.

De plus amples renseignements sur les données que recueille l'ICIS aux fins de la Base de données sur les soins de santé primaires sont accessibles sur le site Web de l'ICIS.

2.3 Gestion de l'accès et cheminement des données de la Base de données sur les soins de santé primaires

L'accès aux applications sécurisées de l'ICIS est régi par la Division de la gestion de produits et de l'expérience client de l'ICIS. Cette division 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).

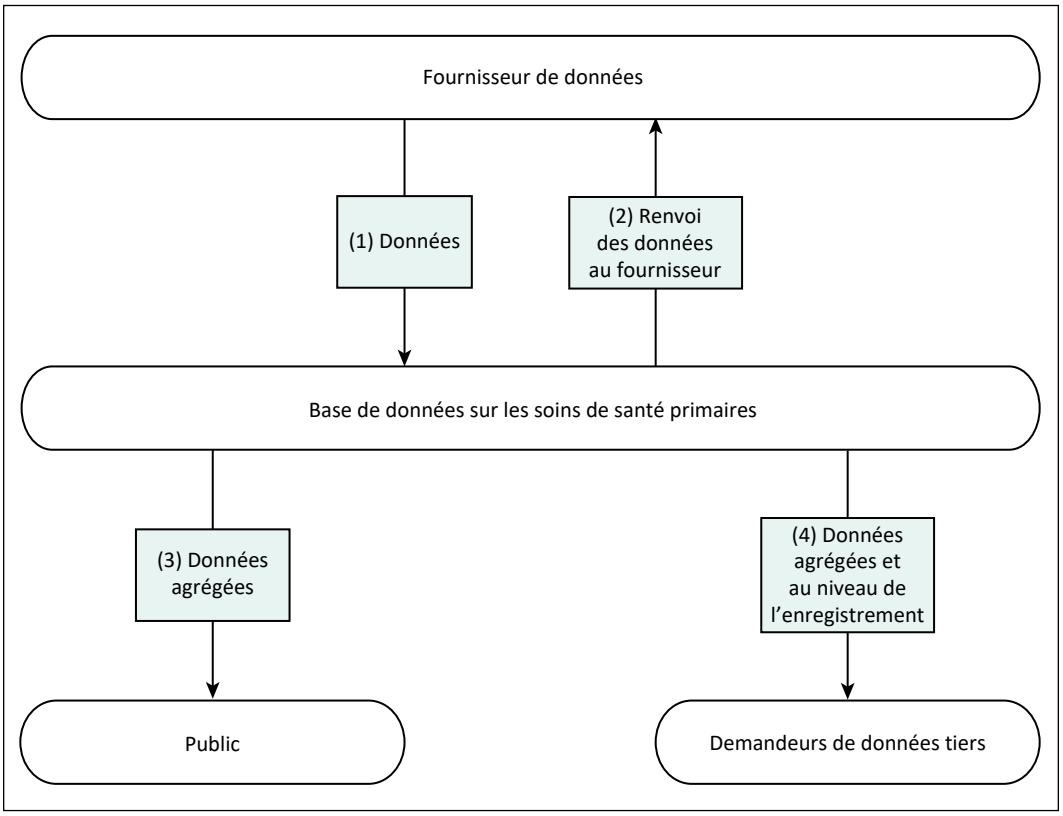
Une fois authentifiés dans le SGA de l'ICIS, les fournisseurs de données sur les soins de santé primaires soumettent à l'ICIS des données au niveau de l'enregistrement saisies électroniquement au moyen d'un logiciel spécialisé. Ils utilisent pour ce faire le Service de soumission électronique de données (eDSS) sécurisé de l'ICIS ou une application serveur à serveur.

Le cheminement des données de la Base de données sur les soins de santé primaires va comme suit :

1. Les fournisseurs de données, notamment les organismes qui offrent des services de soins de santé primaires (p. ex. les cliniques de soins de santé primaires, les centres de santé communautaires) soumettent des données à la Base de données sur les soins de santé primaires.
2. Sur demande, une copie des enregistrements (une fois qu'ils ont été traités aux fins de la Base de données sur les soins de santé primaires) est transmise au fournisseur de données.
3. L'ICIS divulgue des données agrégées au public.
4. L'ICIS divulgue des renseignements personnels sur la santé, des données dépersonnalisées au niveau de l'enregistrement et des données agrégées aux tiers qui en font la demande, conformément à sa politique sur le respect de la vie privée et aux ententes qu'il a conclues avec ses fournisseurs de données.

La figure ci-dessous illustre le cheminement des données de la Base de données sur les soins de santé primaires.

Figure Cheminement des données de la Base de données sur les soins de santé primaires



3 Analyse du respect de la vie privée

3.1 Gestion des risques liés à la vie privée et à la sécurité

La gestion des risques liés au respect de la vie privée et à la 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 leur éventuelle incidence. L'ICIS a mis en œuvre le *Cadre de gestion des risques liés au respect de la vie privée et à la sécurité* et 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 avocate générale 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, d'évaluer, de prendre en charge, de surveiller et d'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. La cote de niveau du 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 le risque initial pris en charge, le risque résiduel (nouveau calcul de la probabilité et de l'incidence du risque par suite du traitement) est évalué en fonction de l'énoncé sur la tolérance à l'égard des risques liés au respect de la vie privée et à la sécurité de l'ICIS, qui indique 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 mises en œuvre jusqu'à l'obtention d'un niveau 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.

Comme il est indiqué à la section 3.4, l'ICIS a par ailleurs entrepris un processus d'évaluation des risques liés au respect de la vie privée et à la sécurité à l'égard des champs de texte libre et de texte semi-structuré.

3.2 Textes législatifs régissant les données de la Base de données sur les soins de santé primaires

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 des systèmes de santé, ce qui comprend l'analyse statistique et la production de rapports. Il incombe aux fournisseurs de données de respecter les obligations légales de leur autorité compétente, selon le cas, au moment de la collecte des données.

À l'heure actuelle, les particuliers et les organismes qui fournissent des services de soins de santé primaires en cabinet privé à Terre-Neuve-et-Labrador, en Nouvelle-Écosse, au Nouveau-Brunswick et en Ontario sont autorisés à divulguer des renseignements personnels sur la santé à l'ICIS sans le consentement des personnes concernées en vertu des lois en matière de protection des renseignements personnels sur la santé en vigueur dans ces provinces. Par exemple, comme l'ICIS est reconnu en tant qu'entité prescrite en vertu de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS) de l'Ontario, les dépositaires de l'information sur la santé de l'Ontario — y compris ceux en cabinets privés — ont le droit de divulguer des renseignements personnels sur la santé à l'ICIS sans le consentement des personnes concernées.

Ententes

À l'ICIS, les données de la Base de données sur les soins de santé primaires 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 fournisseurs de données. 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 ainsi qu'un comité de gouvernance et de respect de la vie privée issu du Conseil d'administration.

Organisation et gouvernance

Le tableau ci-dessous 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 de la Base de données sur les soins de santé primaires :

Tableau Principaux postes et responsabilités

Poste et groupe	Rôles et responsabilités
Vice-président, Stratégies de données et Statistiques	Responsable de l'orientation stratégique générale de la Base de données sur les soins de santé primaires
Directeur, Dépenses et Soins primaires	Responsable du fonctionnement général de la Base de données sur les soins de santé primaires et des décisions administratives stratégiques connexes
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
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

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. Pour ce faire, l'ICIS recueille les types suivants de données sur les soins de santé primaires aux fins indiquées :

Identificateur personnel du patient

Il s'agit ici du numéro d'assurance maladie de la personne. L'ICIS utilise ces informations pour brosser le portrait complet du continuum des soins en regroupant les enregistrements décrivant les divers types de soins qui ont été fournis à la personne à divers moments par divers dispensateurs de soins et établissements.

Caractéristiques démographiques du patient

Il peut s'agir, par exemple, de la date de naissance, du code postal, du sexe, du genre, de la langue, du niveau d'études ou des identificateurs de groupe racial, ethnique ou autochtone. L'ICIS utilise l'âge calculé à partir de la date de naissance, l'information géographique dérivée du code postal ainsi que le sexe, le genre, la langue et les identificateurs de groupe racial, ethnique ou autochtone pour réaliser des analyses démographiques des services de santé fournis et de leurs résultats.

Caractéristiques de santé du patient

Il peut s'agir, par exemple, de diagnostics et de traitements, de comorbidités connexes, de mesures cliniques et de vaccins. L'ICIS se sert de cette information pour analyser la prévalence des maladies et les interventions réalisées au sein d'une population donnée, évaluer les types de problèmes de santé qui exigent un traitement ou une réadaptation, mesurer la qualité des soins fournis à la personne et calculer les coûts associés au traitement.

Données administratives

Il peut s'agir, par exemple, de la date de la visite dans un centre de soins primaires, de la date de début d'un traitement ou de la date d'orientation vers un service. À l'aide de ces informations, l'ICIS évalue le temps d'attente pour les soins, la coordination et la continuité des soins, de même que les ressources consommées pour leur prestation.

Identificateurs de l'organisme

Il s'agit du nom ou du code de l'organisme qui a fourni les soins ou de l'organisme vers lequel la personne a été orientée pour obtenir des soins. L'ICIS utilise cette information pour analyser les soins fournis par divers dispensateurs ou types de dispensateurs.

Identificateurs du dispensateur de services de santé

Il peut par exemple s'agir du numéro attribué à chaque dispensateur de services (p. ex. professionnel de la santé) qui a participé aux soins du patient. Cette information permet à l'ICIS de déterminer les types de ressources humaines ayant contribué aux soins.

Champs de texte libre et de texte semi-structuré

Les champs de texte libre désignent des champs généraux dans lesquels peuvent être saisies des données de toutes sortes, sous forme de texte ou de chiffres, par exemple des commentaires cliniques ou des précisions comme dans le cas des champs de type « Autre, veuillez préciser _____ ». Les champs de texte semi-structuré proposent un choix d'options qui peuvent être modifiées par l'utilisateur. Par exemple, un champ de texte semi-structuré faisant état de la langue d'expression pourrait contenir les valeurs prédéfinies « Français », « Anglais » et « Inconnue », tout en offrant la possibilité d'en ajouter de nouvelles, comme « Espagnol », « Mandarin » et « Arabe ».

À l'heure actuelle, la Base de données sur les soins de santé primaires utilise des champs de texte semi-structuré pour recueillir des données notamment sur la raison de la visite, le problème de santé pris en charge et les médicaments prescrits. Ces champs permettent à l'utilisateur de modifier les valeurs prédéfinies ou d'en ajouter de nouvelles si aucune des valeurs proposées ne répond à ses besoins. Bien que peu probable, il est possible qu'un utilisateur saisisse des renseignements personnels (p. ex. le nom du patient) dans un champ de texte semi-structuré. Pour atténuer ce risque, l'ICIS effectue des vérifications manuelles et automatisées des champs de texte semi-structuré pour relever et retirer tout renseignement personnel sur la santé.

Les risques liés au respect de la vie privée associés aux champs de texte libre et de texte semi-structuré sont actuellement évalués dans le cadre du programme de gestion des risques liés au respect de la vie privée et à la sécurité de l'ICIS, dont il est question à la section 3.1.

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 assument 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 souscrit au 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 des systèmes 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.

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 de la Base de données sur les soins de santé primaires aux objectifs autorisés décrits à la section 3.4. Cela comprend les analyses comparatives au sein des provinces et territoires et entre ceux-ci, 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 sécurisé de l'ICIS est géré au moyen du processus centralisé d'accès aux données de l'ICIS. Cet environnement distinct et sécurisé sert au stockage des fichiers de données analytiques, y compris des fichiers pour usage général, où le personnel doit effectuer ses analyses et en stocker les résultats.

Les fichiers de données pour usage général sont des fichiers prétraités conçus expressément pour les besoins des analystes internes. Le prétraitement consiste à supprimer le numéro d'assurance maladie original (et à le remplacer par un numéro d'assurance maladie chiffré), la date de naissance complète et le code postal complet, et à les remplacer par un ensemble de variables dérivées standards. Les fichiers de données pour usage général liés aux soins de santé primaires sont produits une fois par année aux fins d'intégration des nouvelles données.

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

Couplage des données

Les données de la Base de données sur les soins de santé primaires sont couplées à celles d'autres sources de données 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 même 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) (peut remplacer le critère d.) 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

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 sécuritaire 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 sécuritaire 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 retourner les enregistrements de la Base de données sur les soins de santé primaires au fournisseur de données.

Demandes de données formulées par des tiers

Des tiers peuvent demander qu'on leur fournisse des données au niveau de l'enregistrement ou des données agrégées sur mesure provenant de la Base de données sur les soins de santé primaires.

L'ICIS administre le programme de demandes de données par des tiers, qui établit les mesures de contrôle appropriées de respect de la vie privée et de la sécurité que l'organisme demandeur doit respecter. En outre, comme le stipulent les articles 37 à 57 de sa *Politique de respect de la vie privée, 2010*, l'ICIS divulgue des renseignements sur la santé conformément à son mandat et à ses fonctions de base, et s'efforce de divulguer les données dans le plus grand anonymat possible tout en répondant aux exigences de recherche ou d'analyse du demandeur. Cela signifie que les données sont agrégées dans la mesure du possible. Si les données agrégées ne sont pas suffisamment détaillées pour les besoins définis, l'ICIS peut décider, au cas par cas, de divulguer au destinataire des données dépersonnalisées au niveau de l'enregistrement ou des renseignements personnels sur la santé (dans des circonstances particulières, p. ex. avec le consentement de la personne). Le destinataire doit avoir signé au préalable une entente de protection des données ou un autre instrument juridiquement contraignant avec l'ICIS. Seuls les éléments de données nécessaires aux fins prévues seront divulgués.

Pour les demandeurs de données tiers, l'ICIS utilise un environnement d'accès sécurisé (EAS) comme moyen d'accès privilégié aux données au niveau de l'enregistrement (lequel est distinct de l'environnement analytique sécurisé à l'intention du personnel de l'ICIS précédemment décrit). L'EAS est un environnement chiffré et sécurisé hébergé dans le centre des données de l'ICIS. Conformément aux politiques et procédures en

vigueur à l'ICIS, les chercheurs autorisés — qui sont liés par de rigoureuses conditions d'utilisation — ont accès à des données extraites, préparées et vérifiées par des membres du personnel de l'ICIS pour un projet de recherche approuvé. Les données au niveau de l'enregistrement ne peuvent pas être copiées ni extraites de l'EAS; seuls des résultats agrégés peuvent être extraits de l'EAS. De plus amples renseignements sur l'EAS sont disponibles sur le site Web de l'ICIS (à la page Faire une demande de données et dans le document *Évaluation des incidences sur la vie privée de l'environnement d'accès sécurisé*).

L'ICIS adopte une approche de gestion axée sur le cycle de vie dans les cas où il accorde aux chercheurs et autres utilisateurs autorisés l'accès à des données au niveau de l'enregistrement en extrayant les données pertinentes dans des fichiers transmis aux utilisateurs. Le Secrétariat à la vie privée et aux services juridiques a élaboré et gère un processus de surveillance continue de la conformité qui fait partie intégrante de ce cycle de vie. Dans le cadre de ce processus, tous les fichiers de données qui sont divulgués à des demandeurs tiers font l'objet d'un suivi et d'une surveillance de façon à garantir leur destruction sécuritaire à la fin de leur cycle de vie. Avant d'avoir accès aux données, les demandeurs tiers doivent signer une entente de protection des données et accepter de se conformer aux conditions et restrictions de l'ICIS concernant la collecte, le but, l'utilisation, la sécurité, la divulgation et le renvoi ou la destruction des données.

Les demandeurs de données sont tenus de remplir et soumettre un formulaire de demande. Ils sont également tenus de signer une entente en vertu de laquelle ils s'engagent à utiliser les données uniquement aux fins précisées. Toutes les ententes de protection des données conclues avec des tiers stipulent que les organismes destinataires doivent veiller à la stricte confidentialité des données au niveau de l'enregistrement et qu'ils ne doivent pas divulguer ces données à des personnes en dehors de l'organisme. L'ICIS impose en outre des obligations à ces tiers destinataires, notamment

- des exigences de destruction sécuritaire;
- le droit de l'ICIS de procéder à des vérifications;
- l'interdiction de publier des cellules comprenant moins de 5 observations;
- une solide technologie de cryptage satisfaisant aux normes de l'ICIS ou les surpassant si des appareils informatiques mobiles sont utilisés.

Outre le processus de surveillance continue de la conformité — qui consiste à s'assurer que les fichiers de données divulgués à des tiers destinataires font l'objet d'un suivi et d'une surveillance jusqu'à leur destruction sécuritaire à la fin de leur cycle de vie —, le Secrétariat à la vie privée et aux services juridiques communique chaque année avec les tiers destinataires de données pour vérifier qu'ils respectent toujours les obligations énoncées dans le formulaire de demande de données et l'entente de protection des données de l'ICIS qu'ils ont signée.

Comme il est indiqué à la section 3.4 de la présente évaluation des incidences sur la vie privée, l'ICIS recueille des données sur l'identificateur autochtone aux fins de la Base de données sur les soins de santé primaires. La divulgation de cet identificateur est soumise à la politique sur la diffusion et la divulgation de données identificatoires sur les Autochtones de l'ICIS, en vertu de laquelle toute demande de données identifiant des Autochtones doit être accompagnée d'une preuve de l'approbation des autorités autochtones compétentes. Pour en savoir plus, consultez le document *Tracer la voie vers la gouvernance respectueuse des données de l'ICIS sur les Premières Nations, les Inuits et les Métis*.

Diffusion publique

Dans le cadre de son mandat, l'ICIS publie uniquement des données agrégées en s'assurant de réduire au minimum le risque d'identification et de divulgation par recoupements. En général, il faut au moins 5 observations par cellule conformément à l'article 33 de la *Politique de respect de la vie privée, 2010* de l'ICIS. L'ICIS s'attend à ce que des statistiques agrégées et des analyses sur les soins de santé primaires soient publiées dans les documents et sur le site Web de l'ICIS au moyen d'outils comme Votre système de santé : En détail et les Statistiques éclair.

Restriction de la conservation

La Base de données sur les soins de santé primaires fait partie des banques de données de l'ICIS. Conformément à son mandat et à ses fonctions de base, l'ICIS peut conserver 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 exhaustif 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, la Base de données sur les soins de santé primaires doit régulièrement faire l'objet d'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 de la Base de données sur les soins de santé primaires.

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 de la Base de données sur les soins de santé primaires.

Sécurité des systèmes

L'ICIS reconnaît que l'information ne peut être considérée comme sécurisée que 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 de toute une série 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 des systèmes font partie intégrante du programme de sécurité de l'information de l'ICIS. Ces registres sont par ailleurs 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 évaluer 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. Elles servent également à évaluer la capacité de l'ICIS à protéger l'information et ses 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 toutes les mesures qui s'imposent sont prises.

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

L'ICIS publie de l'information concernant ses politiques sur le respect de la vie privée, ses pratiques relatives aux 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 à l'adresse icis.ca.

3.11 Neuvième principe : accès individuel aux renseignements personnels sur la santé et modification de ceux-ci

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 et avocate générale, qui peut acheminer une demande ou une plainte au commissaire à l'information et à la protection de la vie privée de la province ou du territoire de l'auteur de la demande ou de la plainte.

4 Conclusion

L'évaluation de la Base de données sur les soins de santé primaires effectuée par l'ICIS n'a relevé aucun risque lié au respect de la vie privée et à la sécurité.

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

30761-0423