Système d'information intégré interRAI

Évaluation des incidences sur la vie privée

Août 2021

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. *Système d'information intégré interRAI : évaluation des incidences sur la vie privée, août 2021*. Ottawa, ON : ICIS; 2021.

This publication is also available in English under the title *Integrated interRAI Reporting System Privacy Impact Assessment, August 2021*.

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* :

- *Système d’information intégré interRAI, août 2021*

Approuvé par

Brent Diverty
Vice-président, Stratégies de données et Statistiques

Rhonda Wing
Chef de la protection des renseignements personnels et avocate générale

Ottawa, août 2021

Table des matières

Le Système d'information intégré interRAI en bref

1. Le Système d'information intégré interRAI (SIIR) est une base de données pancanadienne de l'Institut canadien d'information sur la santé (ICIS) qui contient des données normalisées sur les services à domicile et les soins de longue durée (SLD) en établissement financés par le système public, y compris des données cliniques, démographiques, administratives et sur l'utilisation des ressources.
2. Le SIIR recueille de nouvelles versions des fichiers de données sur les services à domicile et les soins de longue durée qui étaient auparavant recueillis par le Système d'information sur les services à domicile (SISD) et le Système d'information sur les soins de longue durée (SISLD) de l'ICIS.
3. Le SIIR utilise une nouvelle méthode de collecte de données par message en temps quasi réel et un nouveau processus de validation fondé sur une application infonuagique.
4. Le SISD et le SISLD, respectivement mis en service en 2005 et en 2003, ont été créés en consultation avec des intervenants de partout au pays. Ces bases de données ne contiennent que les éléments de données jugés nécessaires à la réalisation de leurs objectifs. Le SIIR se limite aussi aux éléments de données considérés par les intervenants comme importants pour la production de rapports.
5. Le SIIR a commencé à recueillir des données en 2019; les données sur les services à domicile et les soins de longue durée en établissement sont longitudinales et fournissent de l'information historique sur chaque client.
6. Les données saisies dans le SIIR sont utilisées pour dégager de l'information exacte, actuelle et comparable sur les populations de clients qui reçoivent des services à domicile et de résidents qui reçoivent des soins de longue durée, sur les services dispensés et sur les résultats pour les clients et les résidents.
7. Les administrateurs des services de santé, les responsables de l'élaboration des politiques, les autorités gouvernementales, les chercheurs et d'autres intervenants se servent des données recueillies pour améliorer la qualité des services et gérer l'accès aux services ainsi que les ressources requises pour dispenser ces services.
8. L'information produite à partir des données soumises au SIIR est accessible aux organismes qui soumettent les données, aux ministères de la Santé, aux autorités sanitaires régionales et à d'autres organismes autorisés sous forme de rapports électroniques en ligne. Elle sera également diffusée publiquement dans les Statistiques éclair, l'outil Votre système de santé et d'autres produits d'information de l'ICIS.

Remarque : La présente évaluation des incidences sur la vie privée ne porte pas sur les risques liés au respect de la vie privée, à la confidentialité et à la sécurité associés au SISD et au SISLD. Cette information se trouve sur le site Web de l’ICIS, dans les documents intitulés *Évaluation des incidences sur la vie privée du Système d’information sur les services à domicile* et *Évaluation des incidences sur la vie privée du Système d’information sur les soins de longue durée*.

Définitions

Aux fins de la présente évaluation des incidences sur la vie privée, les termes ci-dessous ont la signification suivante :

La **base de données du Système d’information intégré interRAI (SIIR)** désigne toutes les données agrégées et au niveau de l’enregistrement recueillies pour le SIIR de l’ICIS et enregistrées dans ce système, ce qui inclut, de manière non exclusive, les données des instruments d’évaluation clinique suivants et des données administratives connexes de l’ICIS :

- Services à domicile (SD) interRAI;
- Soins de longue durée en établissement (SLD) interRAI.

Le **fournisseur de données** désigne un organisme, un dispensateur de soins ou toute autre personne qui communique des renseignements sur la santé à l’ICIS. Il peut s’agir notamment de ministères de la Santé, d’autorités sanitaires régionales ou d’organismes similaires, d’hôpitaux et d’autres établissements de soins de santé.

Le **client** désigne une personne recevant des soins de santé dans le cadre d’un programme de services à domicile ou dans un établissement de soins de longue durée. Dans le secteur des soins de longue durée, les clients sont souvent appelés des « résidents ».

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 (SLD), 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 objet d'examiner les risques de violation de la vie privée, de la confidentialité et de la sécurité associés au Système d'information intégré interRAI (SIIR). 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 SIIR. 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 surtout à respecter la Politique d'évaluation des incidences sur la vie privée de l'ICIS.

2 Renseignements contextuels

L'ICIS recueille des données sur les services à domicile depuis 2005 (voir l'*Évaluation des incidences sur la vie privée du Système d'information sur les services à domicile [SISD]*) et des données sur les soins de longue durée depuis 2003 (voir l'*Évaluation des incidences sur la vie privée du Système d'information sur les soins de longue durée [SISLD]*). Le SISD et le SISLD recueillent tous deux de l'information sur la santé des clients, leur état fonctionnel et cognitif, de l'information démographique et administrative, et de l'information sur les ressources utilisées pour dispenser les soins et services, grâce à des évaluations interRAI normalisées et à des données administratives approuvées par l'ICIS et ses intervenants de partout au Canada.

Le SIIR a été créé pour remplacer le SISD et le SISLD et recueillir des données sur les services à domicile et les soins de longue durée à l'aide des versions actualisées des instruments interRAI. Ces nouvelles versions appliquent les mêmes normes de données dans tous les secteurs. Le SIIR tire parti de ces normes communes grâce à son intégration et à ses processus de saisie des données modernisés, qui comprennent des protocoles de communication standards comme la norme internationale de Health Level Seven (HL7). Le SIIR exploite aussi la norme Fast Healthcare Interoperability Resources (FHIR), qui permet l'échange électronique d'information sur les soins de santé et utilise des interfaces de programmation d'applications (API) infonuagiques pour la soumission des données.

2.1 Présentation du SIIR

Le SIIR est une base de données longitudinale qui recueille l'information sur les évaluations des clients saisies par les fournisseurs de données à divers points lors des épisodes administratifs auprès des organismes qui dispensent des services à domicile ou des soins de longue durée. La norme de données est fondée sur 2 instruments intégrés : l'instrument d'évaluation pour services à domicile (SD) interRAI et l'instrument d'évaluation pour soins de longue durée en établissement (SLD) interRAI.

Le SIIR est conçu pour saisir de l'information sur les services à domicile financés par les gouvernements provinciaux et territoriaux, ce qui comprend les services publics dispensés par des organismes privés pour le compte d'un gouvernement. Il contient des données sur les services à domicile de courte durée (p. ex. pour les clients souffrant d'une affection aiguë de durée limitée) et de longue durée (p. ex. pour les clients qui nécessitent un soutien prolongé pour pouvoir demeurer dans la collectivité).

De même, le SIIR recueille de l'information sur les clients ou résidents qui vivent dans des établissements de soins de longue durée financés ou subventionnés par le système public (souvent aussi appelés « centres de soins infirmiers » ou « soins en hébergement »). Les organismes qui soumettent des données sur les soins de longue durée au SIIR peuvent être détenus et exploités par des intérêts privés ou par le gouvernement.

Les données saisies dans le SIIR sont utilisées pour dégager de l'information exacte, actuelle et comparable sur les populations de clients qui reçoivent des services à domicile et de résidents qui reçoivent des soins de longue durée, sur les services dispensés et sur les résultats pour les clients et les résidents. Les administrateurs des services de santé, les responsables de l'élaboration des politiques, les autorités gouvernementales, les chercheurs et d'autres intervenants se servent des données recueillies pour améliorer la qualité des services et gérer l'accès aux services ainsi que les ressources requises pour dispenser ces services.

Le SIIR intègre dans un même système de déclaration des données cliniques, démographiques, administratives et sur l'utilisation des ressources. Ces données portent sur les soins offerts aux clients des services à domicile et aux résidents des établissements de soins de longue durée financés par le système public. La base de données

- utilise le langage commun et normalisé du système d'évaluation;
- inclut des éléments détaillés propres à des populations précises de clients des services de soins;
- permet de repérer les multiples enregistrements longitudinaux liés à une personne en particulier;

- utilise les normes de données maîtres de l'ICIS (modèle de données de référence de l'ICIS [MDRI], CIM-10-CA, Base de données sur les produits pharmaceutiques du Système national d'information sur l'utilisation des médicaments prescrits [SNIUMP] et index organisationnel[i]).

Les banques de données actuelles qui recueillent les données sur les services à domicile et les soins de longue durée (SISD et SISLD) coexisteront avec le SIIR jusqu'à ce que les provinces et territoires effectuent la transition vers les instruments appropriés (SD interRAI et SLD interRAI). Notez que les établissements ne soumettront pas simultanément leurs données au SIIR, au SISD et au SISLD.

Au moment de la rédaction de cette évaluation des incidences sur la vie privée, aucune donnée des évaluations SD interRAI n'était encore soumise au SIIR. La soumission de ces données au SIIR devrait commencer à la fin de 2021.

2.2 Collecte des données

Le SIIR prend actuellement en charge 2 secteurs — les services à domicile et les soins de longue durée (aussi appelés soins continus en Ontario) — ainsi que 2 instruments — SD interRAI et SLD interRAI, dont voici la description :

- Le **système d'évaluation SD interRAI** sert à éclairer et à guider la planification de l'ensemble des soins et des services dans les établissements en milieu communautaire. Il met l'accent sur les capacités fonctionnelles et la qualité de vie de la personne en évaluant ses besoins, ses forces et ses préférences, et favorise l'orientation vers les services appropriés au besoin. Quand l'instrument est utilisé à de multiples reprises, il permet d'évaluer la réponse de la personne aux soins ou aux services en fonction des résultats obtenus. Le système d'évaluation SD interRAI sert à évaluer les personnes ayant besoin de soins chroniques, ainsi que celles ayant besoin de soins post-aigus (p. ex. après une hospitalisation ou dans une situation d'alternance entre l'hôpital et le domicile)[1].
- **Le système d'évaluation SLD interRAI** permet une évaluation complète et normalisée des besoins, des forces et des préférences des personnes recevant des soins de longue durée à l'hôpital ou en établissement de soins de longue durée[2].

SD interRAI, qui contient environ 306 éléments de données, et SLD interRAI, qui en contient environ 314, sont des instruments d'évaluation exhaustifs qui couvrent plusieurs domaines. Les 2 instruments ont environ 242 éléments de données en commun; ces éléments fondamentaux sont considérés comme importants dans tous les milieux de soins[3] et diffèrent en fonction de la population évaluée et du milieu où l'évaluation est effectuée.

i. L'index organisationnel est une base de données qui offre une vue d'ensemble des données organisationnelles de l'ICIS en liant les données soumises aux diverses banques de données de l'ICIS à chaque organisme. L'index organisationnel fait aussi le suivi des changements constants dans les organismes et leurs relations hiérarchiques.

Les données des 2 instruments interRAI actuellement pris en charge par le SIIR sont classées en 3 sections distinctes :

- **Données sur les clients (démographiques)** (p. ex. numéro de dossier, numéro d'assurance maladie, date de naissance, sexe, langue)
- **Données sur les épisodes (administratifs)** (p. ex. date d'admission, date de sortie, sources de paiement actuelles, types de programme)
- **Données d'évaluation clinique** (p. ex. traitements, diagnostics, fonctions cognitives, fonctions physiques)

Voici la liste des identificateurs recueillis par le SIIR :

Identificateurs personnels (des clients)

- Numéro d'assurance maladie
- Numéro de dossier
- Date de naissance
- Code postal du lieu de résidence habituel

Identificateurs autochtones

- Identité autochtone
- Sources de paiement actuelles

Identificateurs de l'établissement ou de l'organisme de santé

- Numéro de l'établissement/Code d'organisme
- Identificateur de l'installation

Fonctions du système

Les données sont soumises au SIIR au moyen de logiciels créés par les fournisseurs de données ou achetés auprès de fournisseurs externes. Ces logiciels peuvent intégrer ou non les fonctions suivantes du SIIR :

Ajouter/créer (des données sur les clients, les épisodes administratifs et les évaluations) : pour créer et soumettre de nouvelles données sur les clients, les épisodes administratifs et les évaluations jamais soumises auparavant

Corriger : pour corriger des données erronées (p. ex. une date de naissance ou un diagnostic inexact) déjà soumises et acceptées

Mettre à jour : pour modifier des données administratives déjà soumises et acceptées afin de disposer de données plus récentes (p. ex. numéro d'assurance maladie, type de lit, type de programme, sources de paiement actuelles)

Valider : pour envoyer au SIIR des données afin de les soumettre aux règles de validation de l'ICIS dans le but de détecter les éventuels problèmes à corriger (Contrairement à la fonction Créer, la fonction Valider n'enregistre pas les données à l'ICIS, mais ne fait que vérifier le respect des règles de validation.)

Supprimer : pour supprimer du SIIR des évaluations déjà soumises et acceptées

Transférer : pour transférer un client vers un autre établissement ou organisme afin que l'évaluation puisse s'y poursuivre (Cette fonction ne transfère toutefois pas les données du client d'un établissement ou organisme vers un autre dans le SIIR.)

Rechercher : pour trouver un sous-ensemble de données soumises par l'établissement ou l'organisme même au SIIR, le plus souvent à des fins de rapprochement. Le nombre de paramètres de recherche et de résultats est limité. La fonction de recherche a les mêmes fonctions que le Rapport de vérification de la qualité actuellement disponible dans le SISD, le SISLD et d'autres bases de données de l'ICIS. Voici des exemples de recherches possibles :

À propos du client

- Identificateur de l'ICIS relatif au client
- Numéro de l'établissement/Code d'organisme
- Numéro de dossier

À propos de l'épisode administratif

- Identificateur de l'épisode administratif de l'ICIS
- Date de début du séjour/Date d'ouverture du dossier
- Date de retour
- Dernier jour du séjour

À propos de l'évaluation

- Identificateur de l'évaluation de l'ICIS
- Type/Identificateur d'instrument
- Raison de l'évaluation
- Date de référence de l'évaluation

2.3 Gestion de l'accès et soumission et cheminement des données pour le SIIR

Le SIIR est une base de données longitudinale qui gère l'information sur les évaluations des clients saisies par les fournisseurs de données à divers points durant les épisodes administratifs auprès des organismes de santé qui dispensent des services à domicile ou des soins de longue durée.

Gestion de l'accès à la base de données du SIIR

L'accès aux applications sécurisées de l'ICIS est administré par le service Gestion de produits et Expérience client de l'ICIS. Celui-ci 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).

L'accès au SIIR exige que le système du fournisseur de données envoie des données à l'ICIS afin d'être inscrit auprès de l'organisme. Le fournisseur de données autorisé ou son fournisseur de logiciel autorisé peut se charger du processus. Le processus d'inscription pour l'accès est décrit ci-dessous :

Inscription des systèmes

Les fournisseurs de données ou leur fournisseur de logiciel autorisé doivent signer l'Entente sur les spécifications et les normes d'information sur la santé de l'ICIS[ii] (y compris l'Annexe A sur les modalités applicables aux produits), qui régit l'accès aux produits[iii], leur utilisation, ainsi que les droits, restrictions et obligations du client à l'égard de l'environnement et des produits (voir aussi la section 3.2). Les fournisseurs de données ou leur fournisseur de logiciel autorisé doivent aussi remplir le formulaire relatif aux soumissions d'essai par les fournisseurs pour identifier les personnes qui effectueront l'inscription des systèmes.

Pour inscrire un système auprès de l'ICIS, un représentant du fournisseur de données ou de son fournisseur de logiciel autorisé doit créer un profil auprès de l'ICIS. L'ICIS utilise les renseignements inclus dans le profil et dans le formulaire relatif aux soumissions d'essai par les fournisseurs pour accorder aux représentants l'accès nécessaire pour inscrire le système de l'organisme concerné. Une fois authentifiées par le système de gestion de l'accès (SGA) de l'ICIS, les données destinées au SIIR sont directement acheminées du système du fournisseur de données ou de l'application de son fournisseur de logiciel autorisé vers le SIIR de l'ICIS.

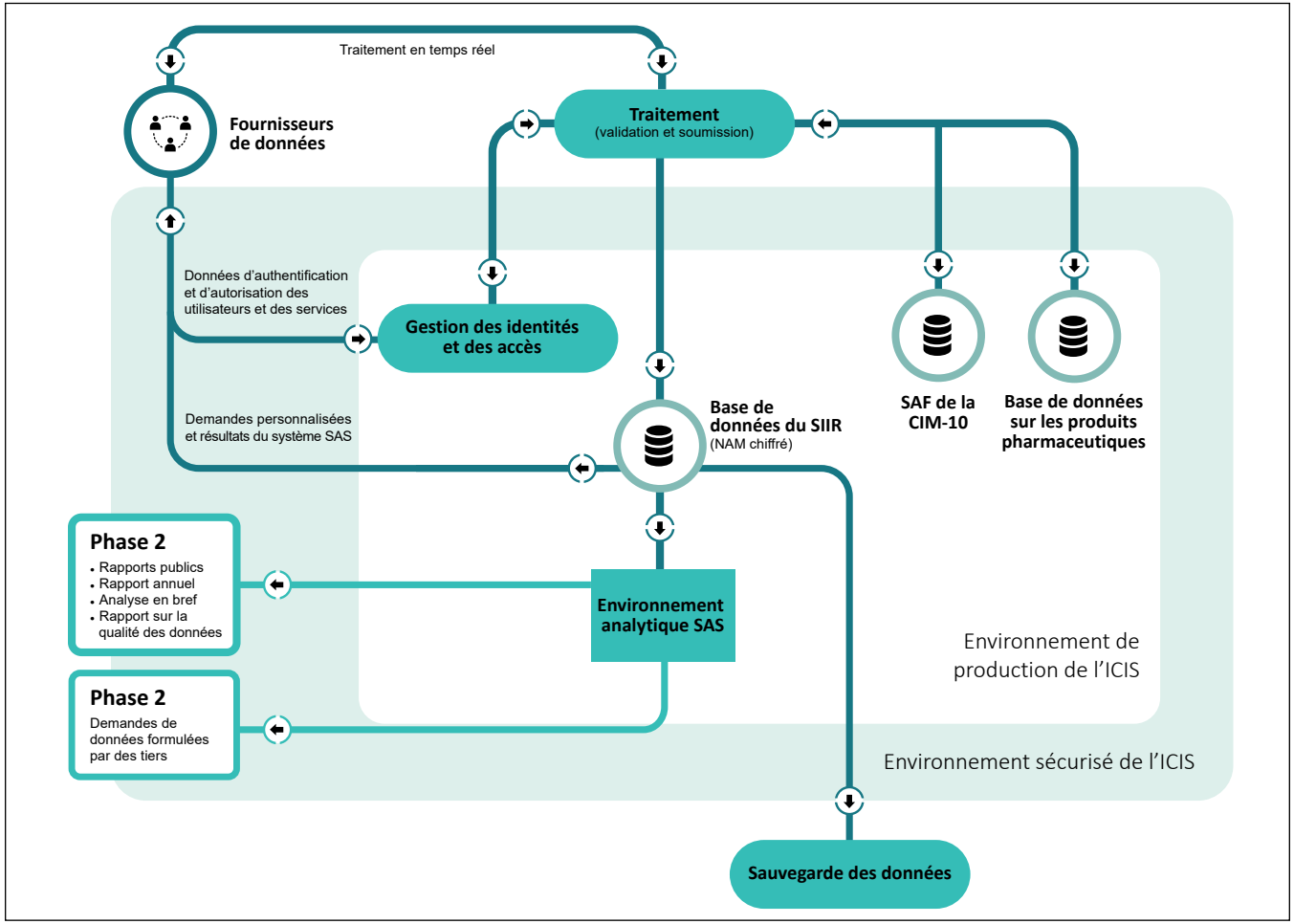
Cheminement des données

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

ii. L'Entente sur les spécifications et les normes d'information sur la santé de l'ICIS comprend une Annexe B, qui contient des formulaires pour cesser l'utilisation des produits.

iii. Le mot « produits » désigne les produits, les spécifications, les documents, les logiciels et les autres ressources et services connexes de l'ICIS — notamment pour le soutien et les mises à jour — sélectionnés par le client en vertu de l'entente, ce qui comprend également les méthodes, techniques, algorithmes, informations et données divulgués dans les produits.

Figure Aperçu du cheminement des données pour le SIIR



Remarques

NAM : numéro d'assurance maladie

SAF de la CIM-10 : Source analytique fiable de la *Classification statistique internationale des maladies et des problèmes de santé connexes, dixième version*

Au cours de la prestation normale des services, des utilisateurs recueillent des données au point de service. Ceux-ci ont été formés pour utiliser les instruments interRAI et se réfèrent aux manuels d'utilisation décrivant les normes liées à chaque instrument interRAI. Ils entrent les données nécessaires directement dans le système d'information de leur organisme, qui est conçu pour être utilisé avec le SIIR, et gèrent (créent, récupèrent, mettent à jour, corrigent, suppriment et recherchent) les enregistrements soumis au SIIR. Pour ce faire, ils font des appels d'API, qui sont enregistrés à des fins de vérification.

Lors de leur soumission au SIIR, toutes les données sont automatiquement validées dans l'environnement sécurisé de l'ICIS. Les erreurs et incohérences sont détectées en fonction des spécifications de soumission FHIR[iv] du SIIR. Lors des transactions de traitement des données, les codes de diagnostic et d'intervention de la CIM-10-CA sont validés au moyen des appels d'API aux copies des répertoires de la CIM dans la source analytique fiable de la CIM-10, et les entrées dans le formulaire des médicaments sont validées à l'aide des appels d'API à l'information du formulaire du SNIUMP (numéros d'identification des médicaments) dans la Base de données sur les produits pharmaceutiques. Les données sont répliquées dans l'environnement sécurisé de l'ICIS. Le rejet d'enregistrements est signalé en temps quasi réel. Les détails des échecs de validation sont envoyés aux systèmes d'information des fournisseurs de données afin que les utilisateurs puissent corriger les données et les soumettre de nouveau. Les échecs, ainsi que les données initialement soumises, sont enregistrés dans l'environnement sécurisé de l'ICIS et servent au soutien opérationnel.

Les enregistrements retenus après la validation sont enregistrés dans la base de données de production du SIIR jusqu'à ce qu'un analyste de l'ICIS intègre une copie de l'ensemble de données à la portion SIIR de l'environnement analytique SAS de l'ICIS. Les données considérées comme sensibles (c.-à-d. les champs qui contiennent, ou peuvent contenir, des renseignements personnels sur la santé) sont enregistrées séparément dans cet environnement. Il est donc possible d'autoriser l'accès seulement au personnel de l'ICIS qui en a besoin pour des raisons opérationnelles ou analytiques approuvées. L'accès du personnel aux données du SIIR de tous types est géré par le processus centralisé d'accès aux données SAS conformément aux politiques en matière d'accès aux données de l'ICIS.

Sur demande, l'ICIS renvoie les données du SIIR au fournisseur de données qui les a d'abord fournies, ainsi qu'au ministère de la Santé concerné. Les organismes qui soumettent des données de l'instrument d'évaluation SLD interRAI à l'ICIS, ainsi que leur ministère de la Santé ou des Services sociaux, les autorités sanitaires régionales et d'autres organismes approuvés, sont aussi autorisés à accéder aux rapports générés par l'ICIS à partir de ces données. Ces rapports privés fournissent des données agrégées sur les populations de

iv. FHIR est une norme décrivant les formats de données et les éléments de données (appelés « ressources »). C'est également une API permettant d'échanger des dossiers de santé électroniques. La norme a été créée par HL7, un organisme spécialisé dans les normes pour les soins de santé[4].

résidents et les résultats (p. ex. les indicateurs de qualité des soins) et sont accessibles dans l'environnement de production de rapports électroniques du SISLD (qui inclut maintenant des données du SISLD et du SIIR) — un outil Web sécurisé d'exploitation de données qui permet aux utilisateurs autorisés de voir et de manipuler les données de manière interactive.

Lors de la phase 2, l'ICIS divulguera aussi des données agrégées et au niveau de l'enregistrement aux tiers autorisés qui en feront la demande et des données agrégées au grand public, en vertu des ententes provinciales ou territoriales de partage des données et conformément à ses politiques en matière de protection de la vie privée et de sécurité de l'information.

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

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 pouvant être reproduit. Elle 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 incidence possible. 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, 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, par exemple 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 niveau de risque évalué (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 mises en œuvre jusqu'à l'obtention d'un niveau de risque 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.

Dans le cadre de cette évaluation des incidences sur la vie privée, 7 risques pour la vie privée et la sécurité ont été détectés lors de l'inscription et de l'authentification des systèmes. Ces risques ont été inscrits au registre des risques liés au respect de la vie privée et à la sécurité de l'ICIS. Ils ont été évalués et réduits jusqu'à ce que les risques résiduels soient faibles, conformément à la méthodologie de gestion des risques liés au respect de la vie privée et à la sécurité.

3.2 Textes de référence régissant les données du SIIR

Généralités

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

Lois sur la protection de la vie privée

L'ICIS est un collecteur secondaire de données sur la santé, particulièrement 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 de leur province ou de leur 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. Celles-ci 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 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. Celles-ci 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 SIIR sont régies par la *Politique de respect de la vie privée, 2010*, la législation en vigueur dans les autorités compétentes 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 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.

Entente de partage des données

Un contrat de licence signé avec interRAI en 1996 accorde à l'ICIS le droit exclusif d'utiliser les formulaires d'évaluation d'interRAI au Canada aux fins de production de rapports statistiques à l'échelle nationale. Le contrat de licence engage également l'ICIS à fournir à interRAI, sur une base annuelle, une copie dépersonnalisée des données recueillies au moyen des formulaires d'évaluation interRAI et soumises au SIIR. interRAI utilise ces données pour perfectionner ses instruments et les applications connexes, de même que pour préparer des analyses et des rapports concernant la pratique clinique, la santé de la population et le système de santé.

Entente sur les spécifications et les normes d'information sur la santé[v] (incluant l'Annexe A sur les modalités applicables aux produits) pour accéder à l'environnement et aux produits de l'ICIS et les utiliser

Les fournisseurs de données ou leur fournisseur de logiciel autorisé doivent signer l'Entente sur les spécifications et les normes d'information sur la santé, qui régit l'accès aux spécifications, normes et autres documents de l'ICIS et leur utilisation pour créer un logiciel de soumission au SIIR.

Entente de services de rapports électroniques de l'ICIS

Les fournisseurs de données autorisés qui soumettent des données sur les soins de longue durée au SISLD et au SIIR doivent signer l'Entente de services de rapports électroniques de l'ICIS pour accéder au service de production de rapports électroniques du SISLD. Cette entente stipule les obligations en matière d'accès aux données, ainsi qu'en matière de sécurité, d'utilisation et de divulgation des données. Elle est signée par un cadre supérieur de l'organisme afin que les utilisateurs soient conscients de leurs responsabilités organisationnelles. Le respect des modalités de l'entente est obligatoire.

v. L'Entente sur les spécifications et les normes d'information sur la santé de l'ICIS comprend une Annexe B contenant des formulaires pour cesser l'utilisation des produits, qui doivent être remplis conformément à l'article 9.2 de l'entente.

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 suivant présente les principaux postes de direction responsables de la gestion des risques en matière de respect de la vie privée et de sécurité pour les données du SIIR.

Tableau Principaux postes et responsabilités

Poste ou groupe	Rôles et responsabilités
Vice-président, Stratégies de données et Statistiques	Responsable de l'orientation stratégique générale du SIIR
Directeur, Soins spécialisés	Responsable des décisions opérationnelles et administratives stratégiques relatives au SIIR
Gestionnaire, Gestion des données, Soins spécialisés	Responsable de la maintenance et du fonctionnement généraux du SIIR
Gestionnaire, Développement de produits	Responsable de l'élaboration et de la mise en œuvre générales du projet du SIIR sur le plan technique
Gestionnaire, Applications de gestion de l'information sur la santé, STI	Responsable de la disponibilité des ressources et solutions techniques nécessaires à l'exploitation et à l'amélioration des données du SIIR
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	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 recueille les données du SIIR aux fins énoncées à la section 2.2 ci-dessus.

L'objectif de recueillir des données sur les services à domicile et les soins de longue durée en établissement est d'aider les dispensateurs de services de santé et décideurs de ces secteurs à

- gérer l'accès aux services;
- détecter les écarts entre les besoins des clients et les services dispensés;
- évaluer les clients ou résidents, planifier et gérer leurs soins et surveiller les résultats;
- surveiller les résultats des initiatives d'amélioration de la qualité des soins;
- comparer les résultats des services fournis par divers organismes;
- contribuer à définir les exigences de formation en fonction des besoins de l'ensemble des clients;
- améliorer la coordination des soins entre les hôpitaux qui donnent congé à des personnes vulnérables et les organismes ou établissements responsables de dispenser des services à ces personnes;
- gérer les ressources requises pour dispenser les services.

Vous trouverez ci-dessous la liste des identificateurs recueillis par le SIIR et leurs définitions. (Consultez la section 2.3 et la section 3.7 pour savoir comment l'ICIS gère les renseignements personnels sur la santé.)

Identificateurs personnels (des clients)

- **Numéro d’assurance maladie :** Le numéro d’assurance maladie attribué à la personne par le gouvernement provincial ou territorial.
- **Numéro de dossier :** Cet élément de données constitue un identificateur principal de la personne dans le SIIR. Il lie les évaluations de la personne au fil de ses épisodes administratifs dans un même organisme. Le numéro de dossier peut être le numéro de dossier de la personne ou tout autre identificateur unique qui respecte les critères de l’ICIS. Il ne peut pas s’agir du numéro d’assurance maladie attribué par le gouvernement provincial ou territorial, et il ne peut pas contenir le nom, complet ou partiel, la date de naissance ou le sexe de la personne. Il ne doit pas changer au fil du temps, y compris lors d’admissions, de retours et de sorties multiples à l’échelle d’un même établissement ou organisme. Il est comparé aux autres identificateurs personnels (p. ex. le numéro d’assurance maladie et la date de naissance) figurant sur chaque enregistrement afin d’assurer l’intégrité longitudinale de la base de données.
- **Date de naissance :** L’année, le mois et le jour où la personne est née.
- **Code postal du lieu de résidence habituel :** Le code postal à 6 caractères alphanumériques attribué par Postes Canada à la résidence permanente où la personne vit ou vivait avant son admission.

Identificateurs autochtones : Ces renseignements peuvent identifier une personne comme Autochtone (pour en savoir plus, consultez la page Premières Nations, Inuits et Métis)

- **Identité autochtone :** Auto-identification de la personne comme membre d’une collectivité autochtone. Ne requiert pas de preuve (c.-à-d. une carte de statut).
- **Sources de paiement actuelles :** Les organismes ou programmes gouvernementaux responsables du paiement des services rendus par l’organisme qui prend soin de la personne. La personne peut recevoir des services payés par plusieurs organismes ou programmes publics ou privés.

Identificateurs de l’établissement ou de l’organisme de santé

- **Numéro d’établissement/Code d’organisme :** Déterminé au moment de la mise en œuvre du SIIR selon les besoins provinciaux ou territoriaux en matière de soumission et de production de rapports. Il identifie de manière unique l’organisme (p. ex. établissement, agence, hôpital, zone, région ou autorité provinciale ou territoriale) responsable de recueillir l’information sur le client et les épisodes administratifs. Cet organisme peut également effectuer les évaluations interRAI.
- **Identificateur de l’installation :** Déterminé au moment de la mise en œuvre du SIIR selon les besoins provinciaux ou territoriaux en matière de soumission et de production de rapports. Il identifie de manière unique l’organisme (p. ex. établissement, hôpital, bureau de services à domicile, site) responsable d’effectuer les évaluations interRAI.

Champs de saisie libre

Les instruments pris en charge par le SIIR contiennent des champs de saisie libre qui permettent de consigner des renseignements cliniques pertinents (voir la liste ci-dessous). Il peut arriver que les utilisateurs y indiquent des renseignements personnels sur la santé ou d’autres données sensibles. Ces champs ne figurent pas tous dans chaque instrument. Des vérifications de validation ont été intégrées dans le SIIR pour empêcher la saisie d’un numéro de dossier, d’un numéro d’assurance maladie ou d’une date de naissance dans un de ces champs. Les données inscrites dans ces champs sont quand même isolées dans l’environnement analytique de l’ICIS, séparées des autres données, et l’accès n’est accordé qu’avec autorisation, en cas de nécessité absolue.

- **Objectifs relatifs aux soins — objectif prioritaire :** Ce champ saisit l’objectif prioritaire des soins prodigués à la personne.
- **Objectifs relatifs aux soins exprimés par la personne :** Ce champ saisit les motifs qui ont amené la personne à demander des soins ou des services. Cet élément permet à la personne d’exprimer ses propres attentes afin que le dispensateur de soins comprenne mieux ses besoins et ses espoirs en vue de lui offrir des soins personnalisés. Comme les objectifs de la personne en matière de soins peuvent changer au fil du temps, cet élément est inclus dans l’évaluation initiale ainsi que dans les évaluations suivantes.
- **Identité de genre autodéclarée de la personne :** Ce champ de saisie libre s’affiche si la personne sélectionne le genre « Autre ». Si la personne répond « Autre » dans les instruments SD interRAI et SLD interRAI, le champ de saisie libre est utilisé pour consigner mot pour mot sa réponse.
- **Identificateurs d’organisation externe :** Identificateurs générés par le logiciel du fournisseur si l’autorité compétente est incapable d’utiliser les identificateurs générés par l’ICIS pour le patient, l’épisode administratif et les ressources d’évaluation (questionnaire). Ils sont envoyés par le système du fournisseur à l’ICIS pour être mis en correspondance avec les identificateurs d’organisation de l’ICIS. Les utilisateurs peuvent les utiliser pour corriger, mettre à jour ou supprimer des enregistrements. Le recours à ces identificateurs est requis puisqu’il permet d’identifier clairement la personne, l’épisode administratif ou l’évaluation auxquels les données se rapportent dans le système de l’établissement ou de l’organisme.

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. Il 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 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.

Le SISD et le SISLD, respectivement mis en service en 2005 et en 2003, ont été créés en consultation avec des intervenants de partout au pays. Ces bases de données ne contiennent que les éléments de données jugés nécessaires à la réalisation de leurs objectifs.

Comme le SISD et le SISLD, le SIIR se limite aux éléments de données qui saisissent les renseignements sur la santé des clients, leur état fonctionnel et cognitif, les renseignements démographiques et administratifs et les renseignements sur les ressources utilisées pour dispenser les soins et services qui sont nécessaires à la réalisation de ses objectifs, tels qu’ils sont décrits à la section 3.4.

Voir la section 3.7 pour savoir comment l’ICIS minimise la collecte, l’utilisation et la divulgation des renseignements personnels sur la santé qui pourraient être entrés dans les quelques champs de saisie libre.

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

L'ICIS restreint l'utilisation des données du SIIR 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 ou 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, 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 comprend le retrait du numéro d'assurance maladie original (remplacé par un numéro d'assurance maladie chiffré), de la date de naissance complète et du code postal complet (remplacés par un ensemble de variables dérivées standards). Les fichiers pour usage général du SIIR devraient être produits au cours de l'exercice 2021-2022.

Ce processus garantit que toutes les demandes d'accès, y compris aux données du SIIR, sont vérifiables et autorisées, conformément à l'article 10 de la *Politique de respect de la vie privée, 2010* de l'ICIS. Le système 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. 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 du SIIR et de sécuriser les données de toute autre manière.

- Les utilisateurs qui saisissent l’information au point de prestation des soins reçoivent de la formation, notamment sur la façon de faire une évaluation et de codifier les résultats, et sur la façon d’éviter d’entrer des identificateurs personnels (p. ex. nom complet ou partiel ou numéro d’assurance maladie de la personne) dans les champs de saisie libre. Voir la section 3.4 pour en savoir plus sur les champs de saisie libre du SIIR. En ce qui concerne plus précisément le champ **Identité de genre autodéclarée de la personne**, les directives de codification du SIIR indiquent de ne pas inclure de nom (partiel ou complet), de numéro d’assurance maladie ni de date de naissance. Dans le champ **Objectifs relatifs aux soins exprimés par la personne**, les directives de codification demandent de ne pas saisir de nom (partiel ou complet), de numéro d’assurance maladie, de date de naissance, de sexe ni de genre. En ce qui a trait au **numéro de dossier**, les spécifications à l’intention des fournisseurs comprennent des directives soulignant que le champ ne doit pas comprendre de numéro d’assurance maladie, de date de naissance, de sexe, ni de nom partiel ou complet.
- L’ICIS effectue des contrôles de validation automatisés pour déterminer si des numéros d’assurance maladie, des dates de naissance et des codes postaux ont été entrés en entier dans les champs de saisie libre. Une évaluation des champs de saisie libre a été réalisée dans le cadre de l’évaluation des risques liés au respect de la vie privée de l’ICIS et des stratégies de réduction des risques ont été mises en place pour minimiser la collecte, l’utilisation, la divulgation et la conservation des renseignements personnels sur la santé qu’ils contiennent.
- Les renseignements recueillis dans les champs de saisie libre sont séparés des autres données du SIIR. L’accès aux renseignements des champs de saisie libre ci-dessus et leur utilisation sont restreints à l’interne. Les fichiers analytiques SAS utilisés par le personnel des Soins spécialisés de l’ICIS ne contiennent pas de données recueillies dans ces champs. Les données qui y sont entrées sont accessibles en cas de nécessité seulement et l’accès doit être approuvé par le directeur des Soins spécialisés. Tout autre accès à ces données ou toute autre utilisation de ces données par un système ou une base de données interne de l’ICIS (voir la section 3.2) doit être approuvé par le directeur. Avant toute divulgation à un tiers, les champs sont examinés. Aucun renseignement personnel sur la santé ne doit s’y trouver. Cette exigence est inscrite dans les procédures opérationnelles standards pour répondre aux demandes de données du SIIR.

De plus, un outil de soutien à la clientèle a été mis au point pour qu’un nombre limité de membres du personnel des Soins spécialisés puissent offrir du soutien aux clients qui soumettent des données et faciliter les essais des fournisseurs. Cet outil indépendant limite l’accès aux données en excluant les dates de naissance, les numéros d’assurance maladie, les codes postaux et les données saisies dans les champs de saisie libre.

Couplage des données

Les données du SIIR 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 des données sur les clients de l'ICIS

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

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), ou tel qu'il est indiqué dans l'entente de partage des données ou un autre instrument juridique. Le renvoi des données au fournisseur est considéré comme une utilisation et non comme une divulgation.

Restriction de la divulgation

Comme il a été mentionné auparavant, l'information recueillie dans les champs de saisie libre définis à la section 3.7 sera conservée dans une table distincte de la base de données du SIIR. Tout accès à ces données visant à les divulguer à une personne externe (p. ex. un consultant), à des chercheurs tiers ou à interRAI en vertu de l'entente de partage des données (voir la section 3.2) requiert également l'approbation du directeur. Avant toute divulgation à un tiers, les champs doivent être examinés. Aucun renseignement personnel sur la santé ne doit s'y trouver.

Les fournisseurs de données qui soumettent des données du SLD interRAI doivent signer l'Entente de services de rapports électroniques de l'ICIS afin d'accéder aux rapports électroniques du SISLD. L'entente précise les exigences concernant la divulgation des renseignements identifiant un établissement de santé et la suppression des cellules de faible valeur.

Demandes de données formulées par des tiers

Différents utilisateurs externes, comme les gouvernements, les décideurs du milieu de la santé et les chercheurs, pourraient demander qu'on leur fournisse des données dépersonnalisées au niveau de l'enregistrement ou des données agrégées sur mesure provenant du SIIR.

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, par exemple, 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.

L'ICIS a adopté une approche de gestion axée sur le cycle de vie en ce qui a trait aux demandes de données au niveau de l'enregistrement provenant de tiers. Le Secrétariat à la vie privée et aux services juridiques a élaboré un processus de surveillance continue de la conformité qui fait partie intégrante de ce cycle de vie. Dans le cadre de ce processus, dont il est responsable, 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 ils sont tenus d'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 n'utiliser les données qu'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 à l'extérieur 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 à 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.

Tel qu'il est indiqué à la section 2.2, le SIIR contient un champ Identité autochtone. 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. Des statistiques agrégées et des analyses sont 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

Le SIIR fait partie des banques de données de l'ICIS. Conformément à son mandat et à ses fonctions de base, l'ICIS peut conserver ces informations aussi longtemps que nécessaire pour la réalisation des fins déterminées.

3.8 Sixième principe : Exactitude des renseignements personnels sur la santé

L'ICIS possède 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 SIIR doit régulièrement subir 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 SIIR.

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 du SIIR.

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 a adopté un ensemble exhaustif de politiques qui précisent les contrôles nécessaires à la protection de l'information en format physique et électronique jusqu'à l'étape du chiffrement et de la destruction sécurisée. 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. 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 qu'il détient 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 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 de l'information 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 aux renseignements personnels sur la santé et modification de ceux-ci

L'ICIS n'utilise pas les renseignements personnels sur la santé qu'il détient pour prendre des décisions administratives ou relatives à la santé au sujet des 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 des renseignements personnels sur la santé à l'ICIS

Comme il est précisé aux 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 SIRR réalisée par l'ICIS a permis de détecter 7 risques pour la vie privée ou la sécurité lors de l'inscription et de l'authentification des systèmes, lesquels ont tous été ajoutés au registre des risques liés au respect de la vie privée et à la sécurité de l'ICIS. Tous les risques ont été évalués et réduits jusqu'à ce qu'ils soient jugés comme faibles selon la méthodologie de gestion des risques liés au respect de la vie privée et à la sécurité de l'ICIS.

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

Références

1. interRAI. Instruments overview: Home Care (HC). Consulté le 30 août 2021.
2. interRAI. Instruments overview: Long-Term Care Facilities (LTCF). Consulté le 30 août 2021.
3. interRAI. Instruments overview. Consulté le 30 août 2021.
4. Wikipedia. Fast Healthcare Interoperability Resources. Consulté le 30 août 2021.

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

53029-0524