Évaluation des incidences sur la vie privée du Système national d'information sur la réadaptation

2022

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

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

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. *Évaluation des incidences sur la vie privée du Système national d'information sur la réadaptation, 2022*. Ottawa, ON : ICIS; 2022.

This publication is also available in English under the title *National Rehabilitation Reporting System Privacy Impact Assessment, 2022*.

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

- *Évaluation des incidences sur la vie privée du Système national d’information sur la réadaptation, 2022*

Approuvé par

Brent Diverty
Vice-président, Stratégies de données et Statistiques

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

Ottawa, mars 2022

Table des matières

Le Système national d'information sur la réadaptation en bref

1. La réadaptation pour patients hospitalisés constitue un élément important du réseau de services de santé. Les interventions multidimensionnelles (physiques, cognitives, psychosociales), soit le diagnostic, l'évaluation, le traitement et la planification des services, permettent d'améliorer les fonctions des patients. Ces services sont habituellement de nature interdisciplinaire ou multidisciplinaire. La réadaptation vise à préparer les patients à réintégrer la collectivité après une maladie ou une blessure.
2. L'Institut canadien d'information sur la santé (ICIS) exploite le Système national d'information sur la réadaptation (SNIR) afin de soutenir la planification et la gestion des services de réadaptation pour patients hospitalisés financés par le secteur public au Canada.
3. En 1995, l'ICIS a entrepris un important projet afin d'élaborer et d'évaluer un fichier minimal et une méthodologie de regroupement pour les services de réadaptation dans les milieux de services à l'échelle du Canada. En 1998, l'ICIS avait recueilli et analysé un large échantillon de données cliniques sur la réadaptation provenant de plus de 30 établissements du Canada et avait consulté plus de 350 experts et intervenants clés dans le domaine de la réadaptation. Les résultats de l'analyse statistique, les évaluations des établissements pilotes et l'examen externe sur le terrain ont prouvé clairement que le fichier était fiable et valide pour divers groupes clients d'adultes en réadaptation dans un établissement pour patients hospitalisés. En 1999, un prototype du SNIR a été testé (une étape clé pour le Canada en matière de normes de données sur la réadaptation), puis intégré à une base de données de production régulière à l'automne 2001.
4. En 2020, environ 100 établissements et organismes de réadaptation pour patients hospitalisés soumettaient des données au SNIR. Ces établissements et organismes se trouvent à Terre-Neuve-et-Labrador, à l'Île-du-Prince-Édouard, en Nouvelle-Écosse, au Nouveau-Brunswick, en Ontario, au Manitoba, en Saskatchewan, en Alberta et en Colombie-Britannique. Toujours en 2020, le SNIR comptait plus de 670 000 paires complètes d'enregistrements d'admission et de sortie (c.-à-d. d'épisodes de soins).
5. Le SNIR recueille des données sur les patients en réadaptation dans les établissements et organismes de réadaptation. Afin d'accroître la comparabilité des données, il regroupe les enregistrements en fonction de la nature de la maladie ou de la blessure ayant mené le patient en réadaptation (p. ex. AVC, arthrite). Les enregistrements sont soumis à l'ICIS conformément aux exigences du fichier minimal du SNIR et incluent
   - des renseignements sur le patient;
   - des renseignements sur les caractéristiques de santé du patient;
   - des données administratives (p. ex. dates d'admission et de sortie de réadaptation);
   - les identificateurs de l'établissement de santé;
   - les identificateurs du dispensateur de services de santé.

6. Le SNIR utilise les données recueillies pour produire de l'information exacte, actuelle et comparable sur des sujets comme le temps d'attente des patients pour des services de réadaptation, l'efficacité des services de réadaptation et les ressources utilisées pour fournir les services de réadaptation.
7. L'information produite par le SNIR sert aux établissements et organismes de soins de santé, aux ministères de la Santé, aux autorités sanitaires régionales, aux chercheurs et au public. L'information est présentée dans divers formats, comme des rapports électroniques interactifs (p. ex. des tableaux de données, des graphiques) à l'échelle de l'établissement ou de l'organisme, de la région et de la province. Les rapports contiennent un large éventail d'attributs et de mesures pratiques pour les utilisateurs. Les données du SNIR contribuent aussi à étayer une variété de rapports publics (p. ex. les Statistiques éclair) qui brossent le portrait des services de réadaptation pour patients hospitalisés au Canada.

1 Introduction

L'Institut canadien d'information sur la santé (ICIS) recueille de l'information sur la santé et les soins de santé au Canada et l'analyse. 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 de la chaîne des soins. L'ICIS obtient des données des hôpitaux et d'autres établissements ou organismes de soins 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 objet d'examiner les risques de violation de la vie privée, de la confidentialité et de la sécurité associés au Système national d'information sur la réadaptation (SNIR). Elle remplace la version de septembre 2015 et 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 leur application au SNIR. Elle se penche également sur 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 le respect de la *Politique d'évaluation des incidences sur la vie privée* de l'ICIS.

2 Contexte

2.1 Présentation du Système national d'information sur la réadaptation

La réadaptation constitue un maillon important de la chaîne des services de santé. Des dispensateurs de services de santé tels que des infirmières, des physiothérapeutes, des ergothérapeutes et des médecins aident les patients à améliorer leurs capacités physiques et leurs fonctions cognitives au moyen d'exercices et d'éducation. La réadaptation vise à préparer les patients à réintégrer la collectivité après une maladie ou une blessure.

En 1995, l'ICIS a entrepris un important projet afin d'élaborer et d'évaluer un fichier minimal et une méthodologie de regroupement pour les services de réadaptation dans les milieux de services à l'échelle du Canada. En 1998, l'ICIS avait recueilli et analysé un large échantillon de données cliniques sur la réadaptation provenant de plus de 30 établissements du Canada et avait consulté plus de 350 experts et intervenants clés dans le domaine de la réadaptation. Les résultats de l'analyse statistique, les évaluations des établissements pilotes et l'examen externe sur le terrain ont prouvé clairement que le fichier était fiable et valide pour divers groupes clients d'adultes en réadaptation dans un établissement pour patients hospitalisés. En 1999, un prototype du SNIR a été testé (une étape clé pour le Canada en matière de normes de données sur la réadaptation), puis intégré à une base de données de production régulière à l'automne 2001.

L'ICIS exploite le SNIR afin de faciliter la planification et la gestion des services de réadaptation pour patients hospitalisés financés par le secteur public au Canada[i]. L'ICIS est un collecteur secondaire de données, qui sont d'abord recueillies par les établissements et organismes de réadaptation. Les données du SNIR indiquent si les capacités physiques et les fonctions cognitives des patients se sont améliorées pendant leur séjour en réadaptation et de quelle manière. Ces données servent à produire de l'information exacte, actuelle et comparable sur divers sujets, notamment

- le temps d'attente avant de recevoir des services de réadaptation;
- l'efficacité des services de réadaptation;
- les ressources utilisées pour la prestation des services de réadaptation.

i. Les services de réadaptation liés à des troubles de santé mentale tels que la toxicomanie sont abordés dans l'*Évaluation des incidences sur la vie privée de la Base de données sur la santé mentale en milieu hospitalier*.

L'information produite par le SNIR sert aux établissements et organismes de soins de santé, aux ministères de la Santé, aux autorités sanitaires régionales, aux chercheurs et au public. L'information est présentée dans divers formats, comme des rapports électroniques interactifs (p. ex. des tableaux de données, des graphiques) à l'échelle de l'établissement ou de l'organisme, de la région et de la province. Les rapports contiennent un large éventail d'attributs et de mesures pratiques pour les utilisateurs. Les données du SNIR contribuent aussi à étayer une variété de rapports publics (p. ex. les Statistiques éclair) qui brossent le portrait des services de réadaptation pour patients hospitalisés au Canada.

2.2 Collecte de données

En 2020, environ 100 établissements et organismes de réadaptation pour patients hospitalisés soumettaient des données au SNIR. Ces établissements et organismes se trouvent à Terre-Neuve-et-Labrador, à l'Île-du-Prince-Édouard, en Nouvelle-Écosse, au Nouveau-Brunswick, en Ontario, au Manitoba, en Saskatchewan, en Alberta et en Colombie-Britannique. La plupart des établissements et organismes soumettent volontairement leurs données au SNIR. Certains sont toutefois tenus de le faire par leur ministère de la Santé ou autorité sanitaire régionale. Toujours en 2020, le SNIR comptait plus de 670 000 paires complètes d'enregistrements d'admission et de sortie (c.-à-d. d'épisodes de soins).

Le fichier minimal du SNIR vise essentiellement les patients de 18 ans et plus, mais accepte néanmoins des données sur toutes les personnes âgées de 13 ans et plus. Afin d'accroître la comparabilité, l'ICIS regroupe les enregistrements de patients soumis au SNIR selon la nature de la maladie ou de la blessure. Ces groupes de patients, appelés groupes de clients en réadaptation (GCR), regroupent les patients selon des caractéristiques comme les déficiences ou limitations d'activité secondaires à divers types de problèmes de santé. Voici la liste de ces GCR :

Groupes de clients en réadaptation

- Accident vasculaire cérébral (AVC)
- Dysfonctionnement cérébral
- Troubles neurologiques
- Dysfonctionnement de la moelle épinière
- Amputation d'un membre
- Arthrite
- Syndromes algiques
- Déficiences développementales
- Troubles médicalement complexes
- Troubles orthopédiques
- Troubles cardiaques

- Troubles pulmonaires
- Brûlures
- Malformations congénitales
- Autres déficiences invalidantes
- Lésions traumatiques multiples graves
- Débilité

Les 2 GCR les plus fréquents sont les troubles orthopédiques et l'AVC, qui représentent à eux seuls plus de la moitié des enregistrements. La plupart des patients admis dans des établissements ou organismes qui participent au SNIR (plus de 90 %) proviennent d'une unité de soins de courte durée du même hôpital ou d'un autre hôpital.

Chaque enregistrement soumis au SNIR respecte les exigences du fichier minimal et comprend des identificateurs du patient, des renseignements démographiques à son sujet, ses caractéristiques de santé, des données administratives, des identificateurs de l'établissement de soins de santé, des identificateurs du dispensateur de services de santé et des champs de texte libre. Une liste complète des éléments de données du fichier minimal du SNIR est disponible sur le site Web de l'ICIS.

2.3 Gestion de l'accès au SNIR, soumission des données et cheminement des données

Gestion de l'accès

L'accès aux applications sécurisées de l'ICIS est régi par le processus de gestion de l'accès en fonction du type d'utilisateur de l'ICIS. Celui-ci détermine 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).

Cheminement des données

Une fois authentifiés dans le SGA de l'ICIS, les établissements ou organismes soumettent leurs données — qui ont été saisies électroniquement au moyen d'un logiciel spécialisé — par le biais des systèmes de soumission sécurisée en ligne de l'ICIS.

Au moment du traitement, les données soumises au SNIR font automatiquement l'objet de validations et de contrôles de la qualité qui permettent de repérer les erreurs et les incohérences par rapport aux spécifications énoncées dans le *Manuel du fichier minimal de la réadaptation*. Le système de traitement des données est un processus interne; aucun accès hors de l'ICIS n'y est possible.

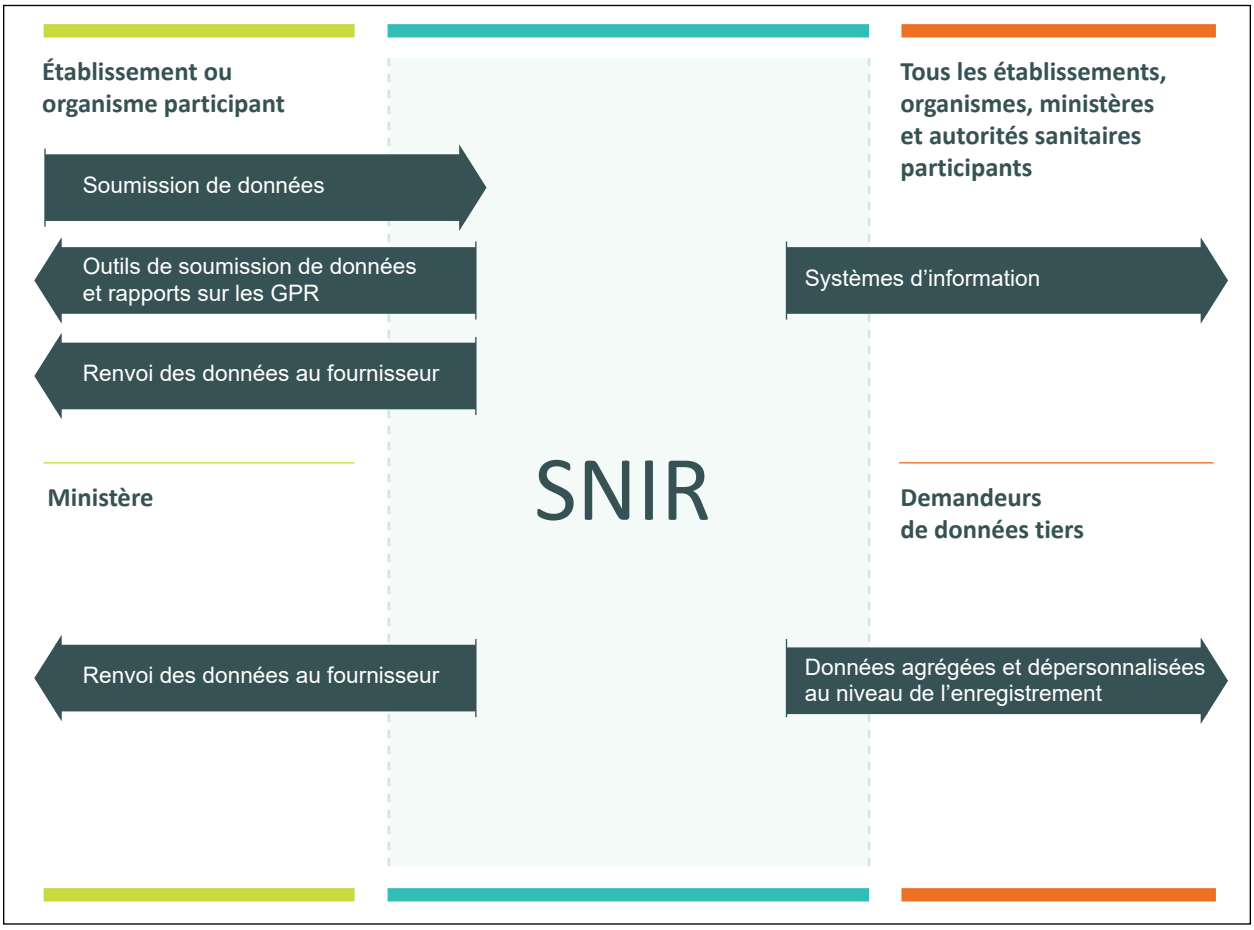
Les établissements et organismes ont accès aux rapports d'erreurs et de validation générés au moment du traitement par l'intermédiaire de l'outil en ligne sécurisé, conformément à la *norme sur le transfert sécuritaire de l'information* de l'ICIS. Ces rapports font ressortir les enregistrements qui contiennent des erreurs (à l'aide du numéro de dossier et des dates d'admission), indiquent le nombre d'enregistrements soumis qui ont été acceptés et précisent les motifs des rejets ou tout message d'avertissement pertinent. Ils permettent ainsi à l'établissement ou à l'organisme de corriger les enregistrements puis de les soumettre de nouveau au SNIR.

Tous les enregistrements traités sans erreur sont ajoutés au SNIR, et les fournisseurs de données peuvent vérifier l'inclusion de leurs enregistrements en demandant un Rapport de vérification de la qualité dans un outil en ligne sécurisé. Cet outil contient un nombre limité d'éléments de données, notamment le numéro de dossier, la date d'admission et la date de sortie.

Une copie dépersonnalisée du fichier de données du SNIR est intégrée à l'environnement analytique de l'ICIS à l'intention du personnel autorisé de l'ICIS. Sur demande ou selon l'entente, l'ICIS renvoie les données du SNIR à l'établissement ou l'organisme qui a d'abord fourni les données ainsi qu'au ministère de la Santé concerné. L'ICIS divulgue aussi des données agrégées et dépersonnalisées au niveau de l'enregistrement aux tiers qui en font la demande, et des données agrégées au public. La figure ci-dessous illustre le cheminement général des données du SNIR.

L'accès du personnel à l'environnement analytique SAS est fourni au moyen du processus centralisé d'accès aux données SAS de l'ICIS, conformément aux politiques en matière d'accès de l'ICIS. Ce processus garantit que toutes les demandes d'accès aux données analytique, y compris aux données du SNIR, sont vérifiables et autorisées. 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 SNIR et de sécuriser les données de toute autre manière.

Figure Aperçu du cheminement typique des données pour le SNIR



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 liés au respect de la vie privée et à la sécurité est un processus officiel et reproductible qui vise la détection, l'évaluation, le traitement et la surveillance des risques dans le but de réduire au minimum la probabilité qu'ils se matérialisent ou leur éventuelle incidence. 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 traiter, 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. 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 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, un traitement supplémentaire est nécessaire jusqu'à l'obtention d'un risque faible, ou jusqu'à ce que le risque non traité ou résiduel soit accepté par le Comité exécutif de l'ICIS au nom de l'organisme.

3.2 Textes législatifs régissant les données du SNIR

Généralités

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

Lois sur la protection de la vie privée

L'ICIS est un collecteur secondaire de données sur la santé, expressément à des fins de planification et de gestion du système de santé, ce qui comprend l'analyse statistique et la production de rapports. Il incombe aux fournisseurs de données de respecter les obligations légales de leur autorité compétente, 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, sous réserve de certaines exigences. Par exemple, l'ICIS est reconnu comme une entité prescrite en vertu de la *Loi sur la protection des renseignements personnels sur la santé* de l'Ontario; les dépositaires de renseignements sur la santé de l'Ontario peuvent donc divulguer de tels renseignements à l'ICIS sans le consentement des patients en vertu de l'article 29, comme le prévoit l'alinéa 45(1) de la Loi.

Les établissements situés dans des provinces et territoires qui ne disposent pas de lois sur la protection des renseignements personnels sur la santé sont assujettis aux lois régissant le secteur public. 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 SNIR sont régies par la *Politique de respect de la vie privée, 2010*, la législation en vigueur dans les provinces et territoires et les ententes de partage de données conclues avec les provinces et territoires. Les ententes de partage des données établissent les critères relatifs au but, à l'utilisation, à la divulgation, à la conservation et à la destruction des renseignements personnels sur la santé fournis à l'ICIS, ainsi que toute divulgation subséquemment permise. Les ententes décrivent aussi l'autorité législative selon laquelle les renseignements personnels sur la santé sont divulgués à l'ICIS.

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

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

Organisation et gouvernance

Le tableau ci-dessous présente les principaux postes de direction à l'ICIS responsables de la gestion des risques associés au respect de la vie privée et à la sécurité pour le SNIR.

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 SNIR
Directeur, Soins spécialisés	Responsable du fonctionnement général du SNIR et des décisions administratives stratégiques connexes
Gestionnaire, Gestion des données, Soins spécialisés	Responsable de la gestion quotidienne des données du SNIR, y compris la qualité des données et la production de rapports 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	Responsable de l'orientation stratégique et de la mise en œuvre générale du programme de respect de la vie privée de l'ICIS
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 continues des données du SNIR
Gestionnaire, Gestion de produits et Expérience client	Responsable de la gestion de l'accès aux applications en ligne d'échange de données du SNIR

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 de soins. L'organisme produit notamment de l'information sur les services de réadaptation pour patients hospitalisés afin de soutenir la planification et la gestion de ces services financés par le secteur public au Canada. Pour ce faire, l'ICIS recueille les types suivants de données du SNIR aux fins indiquées :

Identificateurs personnels et renseignements démographiques

Ces éléments de données comprennent entre autres le numéro d'assurance maladie, le numéro de dossier de l'établissement, la date de naissance, le code postal, le sexe, la langue, le statut d'emploi et l'identité autochtone. L'ICIS utilise ces informations pour brosser le portrait complet des soins fournis à la personne en regroupant les enregistrements décrivant les divers types de soins qui lui ont été fournis à divers moments par divers établissements. Afin de pouvoir réunir les enregistrements, l'ICIS doit savoir lesquels se rapportent à la personne. Pour cette raison, tous les enregistrements doivent inclure des identificateurs, surtout le numéro d'assurance maladie de la personne. L'ICIS utilise l'âge (calculé avec la date de naissance), l'information géographique dérivée du code postal, le sexe, la langue, le statut d'emploi et l'identité autochtone pour réaliser des analyses démographiques des services de santé fournis et de leurs résultats.

Caractéristiques de santé

Ces éléments comprennent les diagnostics et les comorbidités connexes à l'admission et à la sortie. L'ICIS se sert de cette information pour évaluer les types de problèmes de santé qui nécessitent une réadaptation, la qualité des soins fournis à la personne et les coûts associés au traitement.

Données administratives

Ces éléments incluent la date où le besoin de réadaptation du patient a été défini, la date où il a été admis dans l'établissement ou l'organisme, et la date de sortie de l'établissement ou de l'organisme. À l'aide de ces informations, l'ICIS évalue le temps d'attente pour les soins, de même que les ressources consommées pour la prestation des soins.

Identificateurs de l’établissement de santé

Ces éléments sont composés des noms et des codes des hôpitaux ou établissements de soins en hébergement qui ont orienté le patient vers les services de réadaptation, qui ont fourni les services de réadaptation ou qui ont accueilli la personne après sa réadaptation. Ces informations permettent à l’ICIS de comparer les établissements et les groupes d’établissements.

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

Les champs de texte libre peuvent par exemple servir à recueillir des données sur les projets spéciaux nécessaires pour répondre aux besoins de l’ICIS, des provinces et territoires ou des établissements de soins de santé.

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

À titre de collecteur secondaire de données, l’ICIS n’a pas de contact direct avec les patients. L’ICIS s’attend à ce que les fournisseurs de données respectent les règles et leurs responsabilités en matière de collecte, d’utilisation et de divulgation de données, y compris en ce qui concerne le consentement et les avis, conformément aux lois, aux règlements et aux 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 du système de santé, dont l'analyse statistique et la production de rapports connexes, à des fins de gestion, d'évaluation ou de surveillance des systèmes de santé. L'information nécessaire à ces fins recueillie par le SNIR est décrite à la section 2.2.

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 SNIR aux objectifs autorisés décrits aux articles 2.1, 2.2 et 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 consiste à supprimer le numéro d'assurance maladie non chiffré, la date de naissance complète et le code postal complet, et à les remplacer par un ensemble de variables dérivées standards.

Ce processus garantit que toutes les demandes d'accès, y compris aux données du SNIR, 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 SNIR et de sécuriser les données de toute autre manière.

Couplage des données

Les données du SNIR 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 seule banque de données pour l'usage exclusif de l'ICIS. Le couplage de données à partir de multiples banques de données pour l'usage exclusif de l'ICIS et toutes les demandes de couplage de données formulées par des tiers sont soumis à un processus interne d'examen et d'approbation. Lors du couplage, l'ICIS utilise généralement des numéros d'assurance maladie chiffrés. Les données couplées demeurent assujetties aux dispositions en matière d'utilisation et de divulgation de la *Politique de respect de la vie privée, 2010*.

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

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

Article 24 Tous les critères suivants sont respectés :

a. l'objectif du couplage de données s'inscrit dans le mandat de l'ICIS;
b. les avantages pour le public sont considérablement plus importants que les risques de violation de la vie privée des personnes;
c. les résultats du couplage de données ne porteront pas préjudice aux personnes concernées;

d. le couplage de données s'inscrit dans un projet précis et ponctuel, et les données couplées seront par la suite détruites dans le respect des règles énoncées aux articles 28 et 29;
e. le couplage de données est effectué dans le cadre d'un programme de travail continu et approuvé de l'ICIS; les données sont conservées aussi longtemps que nécessaire pour la réalisation des fins déterminées, après quoi elles sont détruites dans le respect des règles énoncées aux articles 28 et 29;
f. le couplage de données permet de réaliser des économies évidentes par rapport à d'autres méthodes ou est l'unique méthode envisageable.

Norme de couplage de données sur les clients

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

Destruction des données couplées

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

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

Renvoi des données au fournisseur

Un établissement ou organisme déclarant peut accéder aux rapports de soumission en ligne sécurisés, qui indiquent combien d'enregistrements l'établissement ou l'organisme a soumis avec succès au SNIR. Ces rapports précisent également quels enregistrements ont été rejetés et pour quelle raison (p. ex. information manquante). Ces rapports permettent à l'établissement ou l'organisme de cerner et corriger les erreurs, puis de soumettre de nouveau les enregistrements. Le rapport utilise le numéro de dossier que l'établissement ou l'organisme a attribué à chaque patient (le rapport ne contient aucun numéro d'assurance maladie) pour identifier les enregistrements problématiques.

Les établissements ou organismes déclarants ont également accès aux rapports sur les groupes de patients en réadaptation (GPR). Ces rapports en ligne sécurisés permettent à l'utilisateur d'examiner certains éléments de données des enregistrements soumis par l'établissement ou l'organisme au SNIR, notamment l'évaluation des capacités fonctionnelles motrices et cognitives, les dates d'admission et de sortie, et les ressources estimées utilisées pour la prestation des services de réadaptation. Les rapports sur les GPR identifient les enregistrements au moyen du numéro de dossier.

Sur demande, l'ICIS peut fournir à un établissement ou organisme une copie des données qu'il a soumises au SNIR, sous forme de 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 établissements ou organismes déclarants, peut également remettre les enregistrements au ministère concerné, pour des motifs de qualité des données ou à d'autres fins inscrites dans son mandat (p. ex. la gestion des services de santé et de la santé de la population, qui comprend la planification, l'évaluation et l'affectation des ressources). Le renvoi des données au fournisseur de données est considéré comme une utilisation et non comme une divulgation.

Restriction de la divulgation

Les rapports électroniques du SNIR sont un outil en ligne sécurisé qui fournit aux utilisateurs autorisés de l'information agrégée sur les services de réadaptation permettant d'identifier les établissements et organismes déclarants. Les établissements et organismes qui soumettent des données au SNIR, les ministères de la Santé, les autorités sanitaires régionales et d'autres organismes approuvés y ont accès. Ces rapports contiennent les informations suivantes :

- le nombre de patients qui ont reçu des services de réadaptation, par problème de santé (p. ex. l'AVC);
- le nombre de jours d'attente avant de recevoir des services de réadaptation;
- le nombre de jours où les services de réadaptation ont été dispensés;

- les progrès réalisés dans les capacités physiques et fonctions cognitives des patients grâce à la réadaptation;
- les ressources estimées utilisées pour la prestation des services de réadaptation;
- les caractéristiques sociodémographiques des patients (p. ex. la langue, le statut d'emploi) pertinentes à la réadaptation.

Les utilisateurs autorisés peuvent adapter le contenu et l'apparence des rapports à leurs besoins opérationnels. Ils peuvent par exemple personnaliser les rapports de façon à obtenir des renseignements ciblés sur

- les services de réadaptation dispensés pour un type d'affection particulier;
- un établissement ou organisme de réadaptation particulier ou des établissements ou organismes d'une taille, d'une région ou d'un type donné;
- les activités de réadaptation dispensées à un moment précis de l'année.

Avant d'avoir accès aux rapports contenant des données du SNIR, les utilisateurs doivent signer une entente de service qui comprend notamment des règles visant à

- restreindre l'utilisation de l'information à des fins non commerciales aux activités de gestion interne, d'assurance de la qualité des données, de planification, de recherche, d'analyse ou d'appui à la prise de décisions reposant sur des données probantes des clients;
- interdire la divulgation des données à des tiers, sauf s'il s'agit des données du client;
- permettre la publication de l'information uniquement lorsque toutes les mesures raisonnables ont été prises pour préserver l'identité des personnes et que les données ne contiennent pas de cellules comprenant moins de 5 observations;
- interdire la publication de renseignements permettant d'identifier un établissement ou organisme de santé, à moins que le client en informe préalablement l'ICIS afin de lui permettre d'aviser le ministère concerné.

Demandes de données formulées par des tiers

Divers tiers peuvent demander qu'on leur fournisse des données au niveau de l'enregistrement ou des données agrégées sur mesure provenant du SNIR.

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 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 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.

Comme indiqué à la section 3.4 de cette évaluation des incidences sur la vie privée, le SNIR 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 les Statistiques éclair.

Restriction de la conservation

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

3.8 Sixième principe : Exactitude des renseignements personnels sur la santé

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

À l'instar d'autres banques de données de l'ICIS, le SNIR 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 SNIR.

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 SNIR.

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

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

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

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

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

4 Conclusion

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

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

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

12020-0322