



Évaluation des incidences sur la vie privée du
Système national d'information sur la réadaptation,
septembre 2015



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



Notre vision

De meilleures données pour de meilleures décisions : des Canadiens en meilleure santé

Notre mandat

Exercer le leadership visant l'élaboration et le maintien d'une information sur la santé exhaustive et intégrée pour des politiques avisées et une gestion efficace du système de santé qui permettent d'améliorer la santé et les soins de santé

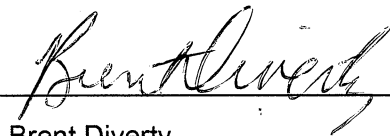
Nos valeurs

Respect, intégrité, collaboration, excellence, innovation

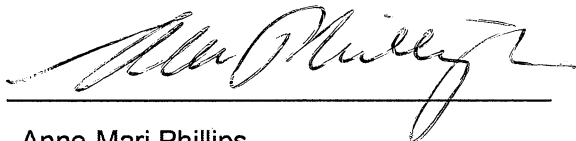
L'Institut canadien d'information sur la santé (ICIS) est fier de publier l'évaluation des incidences sur la vie privée suivante conformément à sa *Politique d'évaluation des incidences sur la vie privée* :

- Système national d'information sur la réadaptation, septembre 2015

Approuvé par :



Brent Diverty
Vice-président, Programmes



Anne-Mari Phillips
Chef de la protection des
renseignements personnels et
avocate générale

Ottawa, septembre 2015

Table des matières

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Faits saillants sur l'ICIS et le Système national d'information sur la réadaptation | 7 |
| 1 Introduction | 8 |
| 2 Contexte..... | 8 |
| 2.1 Fournisseurs de données..... | 9 |
| 2.2 Données recueillies | 9 |
| 2.3 Cheminement des données | 10 |
| 3 Analyse du respect de la vie privée | 12 |
| 3.1 Textes législatifs régissant les données du SNIR | 12 |
| Généralités..... | 12 |
| Législation..... | 12 |
| Ententes..... | 12 |
| 3.2 Premier principe : Responsabilité à l'égard des renseignements personnels sur la santé | 13 |
| Organisation et gouvernance | 13 |
| 3.3 Deuxième principe : Établissement de l'objet des renseignements personnels sur la santé | 13 |
| 3.4 Troisième principe : Consentement pour la collecte, l'utilisation ou la divulgation de renseignements personnels sur la santé | 14 |
| 3.5 Quatrième principe : Restriction de la collecte de renseignements personnels | 14 |
| 3.6 Cinquième principe : Restriction de l'utilisation, de la divulgation et de la conservation des renseignements personnels sur la santé | 15 |
| Restriction de l'utilisation..... | 15 |
| Couplage de données | 15 |
| Renvoi des données au fournisseur de données..... | 17 |
| Restriction de la divulgation | 17 |
| Restriction de la conservation | 20 |
| 3.7 Sixième principe : Exactitude des renseignements personnels sur la santé | 20 |
| 3.8 Septième principe : Mesures de protection des renseignements personnels sur la santé | 21 |
| Cadre de respect de la vie privée et de sécurité de l'ICIS | 21 |
| Sécurité des systèmes | 21 |
| 3.9 Huitième principe : Transparence de la gestion des renseignements personnels sur la santé | 22 |
| 3.10 Neuvième principe : Accès individuel aux renseignements personnels sur la santé et modification de ceux-ci..... | 22 |

| | |
|-----------------------------------------------------------------------------------------------------------------------|----|
| 3.11 Dixième principe : Plaintes concernant le traitement par l'ICIS des renseignements personnels sur la santé | 23 |
| 4 Conclusion | 23 |

Faits saillants sur l'ICIS et le Système national d'information sur la réadaptation

- La réadaptation constitue un élément important du continuum des services de santé. L'ICIS exploite le Système national d'information sur la réadaptation (SNIR) afin de faciliter la planification et la gestion des services de réadaptation au Canada.
- Le SNIR recueille des données normalisées sur les services de réadaptation pour patients hospitalisés. En 2015, environ 100 établissements de réadaptation pour patients hospitalisés soumettaient des données au SNIR. Il peut s'agir aussi bien d'hôpitaux autonomes de réadaptation que d'unités de réadaptation d'hôpitaux de soins de courte durée. Ces établissements 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.
- Les établissements soumettent des enregistrements à l'ICIS conformément aux exigences relatives au fichier minimal du SNIR. Celui-ci se compose d'éléments de données regroupés dans les principales catégories suivantes : identificateurs du patient, données sociodémographiques, données administratives, caractéristiques de santé, et activités et participation. Afin d'accroître la comparabilité, l'ICIS regroupe les enregistrements du SNIR en fonction de la nature de la maladie ou de la blessure (p. ex. AVC, arthrite). En 2015, le SNIR comptait plus de 450 000 paires complètes d'enregistrements d'admission et de sortie (c.-à-d. des épisodes de soins).
- L'équipe du SNIR analyse les données soumises par les établissements afin de produire de l'information exacte, actuelle et comparable sur divers sujets comme les temps d'attente pour des services de réadaptation, l'efficacité de ces services et les ressources utilisées.
- Cette information permet aux établissements, aux ministères de la Santé, aux régies régionales de la santé, aux chercheurs et au public de prendre des décisions plus éclairées en matière de réadaptation.

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 exercer le leadership visant l'élaboration et le maintien d'une information sur la santé exhaustive et intégrée, pour des politiques avisées et une gestion efficace du système de santé qui permettent d'améliorer la santé et les soins de santé. L'ICIS obtient les données auprès des hôpitaux et d'autres établissements de santé, des centres de soins de longue durée, des régies régionales de la santé, 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 celle réalisée en 2009 et comprend un examen des 10 principes énoncés dans le *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation qui s'appliquent au SNIR. La présente évaluation des incidences sur la vie privée repose surtout sur le respect de la [*Politique d'évaluation des incidences sur la vie privée*](#) de l'ICIS.

2 Contexte

La réadaptation constitue un élément important du continuum des services de santé. Des professionnels 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 leur collectivité après une maladie ou une blessure.

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. L'ICIS est un collecteur secondaire de données sur la réadaptation. À l'origine, ces données sont recueillies et soumises par les établissements de réadaptation. Les données du SNIR portent sur l'amélioration des capacités physiques et fonctions cognitives des patients pendant leur séjour en réadaptation. 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.

Cette information permet aux établissements, aux ministères de la Santé, aux régies régionales de la santé, aux chercheurs et au public de prendre des décisions plus éclairées en matière de réadaptation.

2.1 Fournisseurs de données

Tous les établissements qui soumettent des données au SNIR fournissent des services de réadaptation en milieu hospitalier pour patients hospitalisés. Ces services peuvent être dispensés dans des hôpitaux autonomes de réadaptation ou à l'unité de réadaptation des hôpitaux de soins de courte durée. Les établissements qui participent au SNIR se classent eux-mêmes comme « généraux » ou « spécialisés ». Cette classification, propre au SNIR, vise à faciliter la production de rapports comparatifs. Elle n'est pas nécessairement conforme aux méthodes de classification des établissements utilisées dans diverses provinces ou régions.

Selon la définition du SNIR, un établissement général de réadaptation est une unité de réadaptation ou un ensemble de lits destinés à la réadaptation qui fait partie d'un hôpital général offrant de multiples niveaux ou types de soins de santé. L'établissement spécialisé en réadaptation, pour sa part, dispense des services plus spécialisés et plus étendus de réadaptation pour patients hospitalisés. Il s'agit souvent d'un établissement autonome de réadaptation ou d'une unité spécialisée dans un hôpital. L'équipe de réadaptation de l'établissement décide lequel des 2 profils reflète le mieux ses programmes de réadaptation et choisit une catégorie, soit « général » ou « spécialisé », avant de commencer à soumettre des données au SNIR.

En 2015, environ 100 établissements de réadaptation pour patients hospitalisés soumettaient des données au SNIR. Ces établissements 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 soumettent volontairement leurs données. Certains sont toutefois tenus de soumettre des données par leur ministère de la Santé ou régie régionale de la santé.

2.2 Données recueillies

Le SNIR recueille auprès des établissements de l'information sur la mesure dans laquelle les capacités physiques et fonctions cognitives des patients se sont améliorées pendant leur séjour en réadaptation. Il recueille également divers renseignements complémentaires, par exemple le moment où les services de réadaptation commencent et prennent fin, les ressources estimées utilisées pour la prestation des services de réadaptation et les caractéristiques sociodémographiques pertinentes à la réadaptation.

Le fichier minimal du SNIR (consulter la section 3.5) vise 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. Les groupes de patients, appelés groupes de clients en réadaptation (GCR), englobent les patients qui ont des déficiences, des limitations d'activité ou des restrictions de participation secondaires à divers types de troubles. Voici la liste de ces GCR :

Groupes de clients en réadaptation

- Accident vasculaire cérébral
- 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 GCR relatifs aux troubles orthopédiques et à l'accident vasculaire cérébral sont les 2 groupes dans lesquels les cas sont le plus souvent classés. Ils représentent plus de la moitié de tous les enregistrements. La plupart des patients admis dans des établissements qui participent au SNIR (plus de 90 %) proviennent d'une unité de soins de courte durée du même hôpital ou d'un autre hôpital. En 2015, le SNIR comptait plus de 450 000 paires complètes d'enregistrements d'admission et de sortie (c.-à-d. des épisodes de soins).

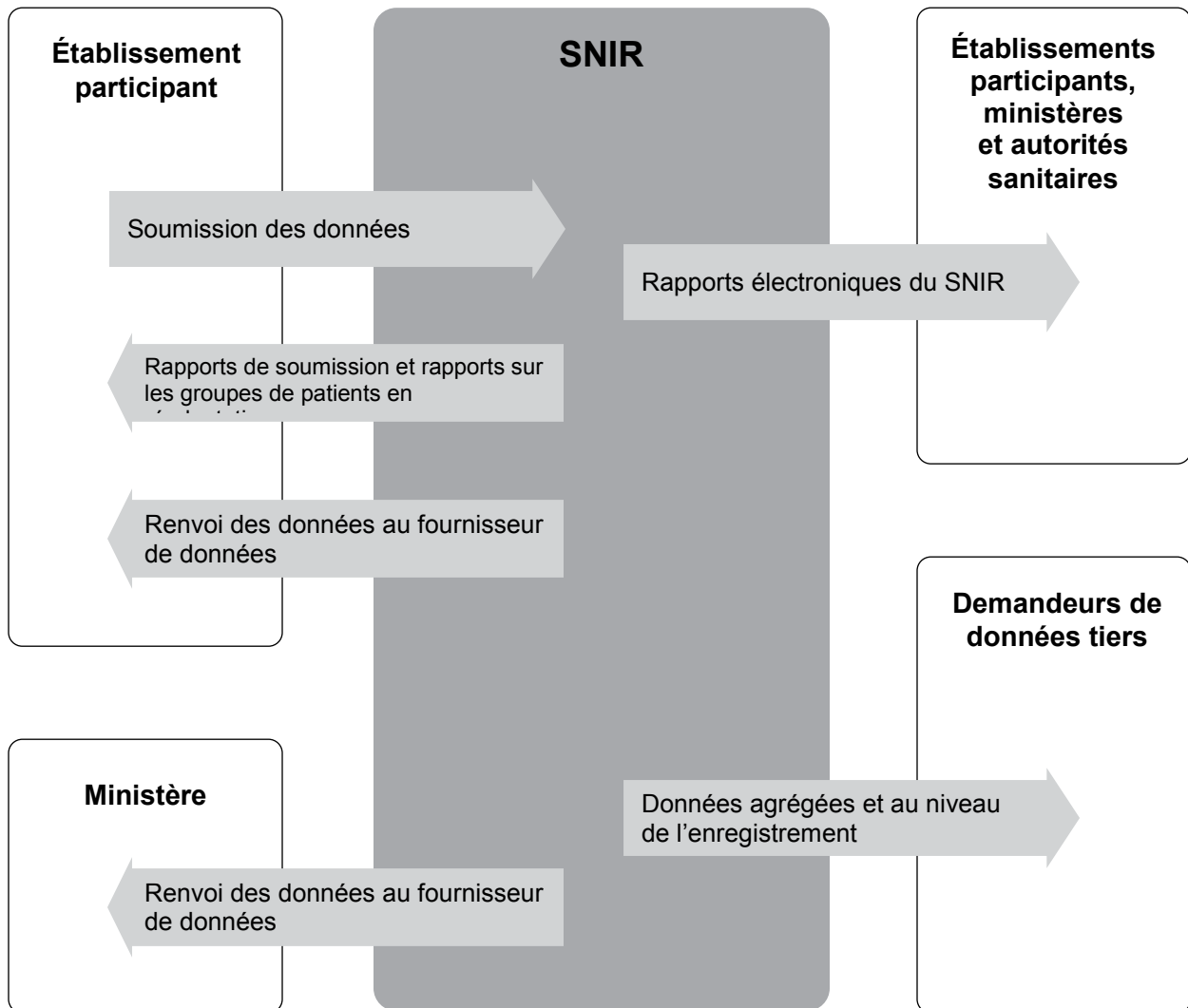
Les services de réadaptation liés à des troubles de santé mentale (p. ex. les dépendances) sont abordés dans l'[Évaluation des incidences sur la vie privée de la Base de données sur la santé mentale en milieu hospitalier](#).

2.3 Cheminement des données

Les établissements soumettent leurs données au SNIR par l'entremise de l'application de soumission sécurisée en ligne de l'ICIS. Les spécifications de données et d'autres documents connexes, tels que la disposition des fichiers, sont fournis par l'ICIS. Toutes les soumissions à l'ICIS doivent respecter les spécifications de soumission et de vérification.

Les sections 3.5 et 3.6 examinent de plus près le cheminement des données à destination et en provenance du SNIR. La figure 1 illustre le cheminement général des données.

Figure 1 Cheminement des données du SNIR



3 Analyse du respect de la vie privée

3.1 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 législation ou entente applicable.

Législation

L'ICIS est un collecteur secondaire de renseignements personnels sur la santé, plus particulièrement à des fins de planification et de gestion du système de santé, y compris d'analyse statistique et de production de rapports. Il incombe aux fournisseurs de données de respecter les obligations légales de leur province ou de leur territoire, le cas échéant, au moment de la collecte des données.

Terre-Neuve-et-Labrador, la Nouvelle-Écosse, le Nouveau-Brunswick, l'Ontario, le Manitoba, la Saskatchewan et l'Alberta disposent de lois sur la protection des renseignements personnels sur la santé. En outre, le Yukon, les Territoires du Nord-Ouest et l'Île-du-Prince-Édouard travaillent à la mise en œuvre de telles lois. Ces lois octroient aux établissements l'autorisation de divulguer des renseignements personnels sur la santé sans le consentement du patient pour les besoins du système 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 cette province 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 en 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](#) de l'Institut, la législation en vigueur dans les provinces et territoires et les ententes de partage déjà mises en place 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.

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

Il incombe au président-directeur général de l'ICIS de s'assurer du respect de 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, une équipe du respect de la vie privée, de la confidentialité et de la sécurité, un comité de gouvernance et de respect de la vie privée au sein de son 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.

| Poste/groupe | Rôles et responsabilités |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Vice-président, Programmes | Responsable du leadership et de la supervision en matière d'acquisition, de gestion et de diffusion des données du SNIR |
| Directeur, Méthodologies et Soins spécialisés | Responsable de la prise de décisions stratégiques et opérationnelles concernant les données du SNIR |
| Gestionnaire, Réadaptation et Santé mentale | Responsable de la gestion continue des données du SNIR, y compris la qualité des données et la production de rapports |
| 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 pour l'exploitation et l'amélioration des données du SNIR |
| Gestionnaire, Services centraux à la clientèle | Responsable de la gestion de l'accès aux applications en ligne d'échange de données du SNIR |

3.3 Deuxième principe : Établissement de l'objet des renseignements personnels sur la santé

Les données du SNIR servent à produire des rapports exacts, actuels et comparables sur les services de réadaptation pour patients hospitalisés. Cette information permet aux établissements, aux ministères de la Santé, aux régies régionales de la santé, aux chercheurs et au public de prendre des décisions plus éclairées en matière de réadaptation. Les types de données saisies dans le SNIR et leur utilité sont abordés à la section 3.5.

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

L'ICIS est un collecteur secondaire et n'a aucun contact direct avec les patients. L'ICIS s'attend à ce que les fournisseurs de données respectent les règles régissant la collecte, l'utilisation et la divulgation des données et s'acquittent de leurs responsabilités en la matière, 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.

3.5 Quatrième principe : Restriction de la collecte de renseignements personnels

L'ICIS s'engage à respecter le principe de la minimisation des données. Conformément aux 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 du système de santé canadien. Conformément à ce principe, le SNIR ne recueille que les renseignements requis pour faciliter la planification et la gestion des services de réadaptation pour patients hospitalisés financés par le secteur public au Canada.

Le fichier minimal du SNIR se compose d'éléments de données regroupés dans les principales catégories suivantes :

- Identificateurs du patient : Il s'agit des éléments de données qui servent à distinguer chaque enregistrement. Le nom des patients n'apparaît nulle part dans le SNIR.
- Données sociodémographiques : Les données sur la date de naissance, le sexe, le milieu de vie, le statut d'emploi, etc., sont une source d'information très utile sur les types de patients admis dans les programmes de réadaptation.
- Données administratives : Les données sur les temps d'attente, à l'admission et à la sortie, sur les interruptions de service et sur les types de dispensateurs permettent de mieux comprendre l'accès aux services de réadaptation, l'utilisation des ressources et les facteurs qui influencent la durée du séjour.
- Caractéristiques de santé : Les diagnostics et les comorbidités connexes à l'admission renseignent sur les problèmes les plus communs en réadaptation et sur ceux qui peuvent avoir des répercussions sur la capacité du patient à progresser dans le programme de réadaptation.
- Activités et participation : Il s'agit de la section du fichier minimal où sont consignées les données cliniques sur les capacités fonctionnelles motrices et cognitives des patients en réadaptation. L'instrument FIM^{MDi} sert à mesurer les résultats liés à l'autonomie fonctionnelle

i. L'instrument FIM^{MD} et les codes de déficiences auxquels fait référence le présent document sont reproduits avec la permission de UB Foundation Activities, Inc. et appartiennent à la Uniform Data System for Medical Rehabilitation (UDSMR), une division de UB Foundation Activities, Inc. Les groupes clients en réadaptation (GCR) ont été adaptés à partir des codes de déficiences, avec la permission de UB Foundation Activities, Inc. L'instrument FIM^{MD} est une marque déposée qui est la propriété de la Uniform Data System for Medical Rehabilitation, une division de UB Foundation Activities, Inc.

à l'admission et à la sortie et, à titre facultatif, au suivi après la sortie. Il se compose de 18 éléments (13 éléments moteurs et 5 cognitifs) qui servent à évaluer la maîtrise de certaines activités. L'échelle varie de 1 à 7, selon le niveau d'autonomie (un représentant la dépendance totale et 7, l'autonomie totale); la note maximale est de 126 (18 éléments x 7). L'instrument FIM^{MD} mesure le niveau d'incapacité et examine le fardeau qu'impose ce niveau d'incapacité au soignant. La note globale de l'instrument FIM^{MD} peut être subdivisée en éléments moteurs et cognitifs, ce qui permet de cerner plus en détail les zones de perte fonctionnelle.

Outre les données recueillies à l'aide de l'instrument FIM^{MD}, des éléments liés aux fonctions cognitives, des éléments qui évaluent les activités instrumentales de la vie quotidienne et l'état de santé, les caractéristiques sociodémographiques, administratives et de santé sont également recueillis pour chaque patient en réadaptation.

Une liste complète des éléments de données du SNIR est accessible sur le [site Web de l'ICIS](#).

3.6 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 à l'article 3.3. Cela comprend les analyses comparatives au sein des provinces et territoires ainsi qu'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. Le personnel de l'ICIS est autorisé à accéder aux données et à les utiliser uniquement lorsque cela est nécessaire, 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.

Depuis 2009, les fichiers de données utilisés à l'interne par l'ICIS à des fins d'analyse ne contiennent aucun identificateur direct, comme les numéros d'assurance-maladie non chiffrés. Le personnel de l'ICIS a accès aux numéros d'assurance-maladie non chiffrés de façon exceptionnelle, uniquement en cas de nécessité. Cet accès est assujéti aux processus internes d'approbation, comme précisé dans les *Procédures de respect de la vie privée 2010* de l'ICIS.

Couplage de données

Les données du SNIR sont couplées à celles d'autres sources de données de l'ICIS. Afin d'atténuer les risques potentiels d'identification des personnes qui découlent du couplage, l'ICIS prendra les mesures qui suivent.

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](#) de l'ICIS.

Les critères d'approbation du couplage de données sont énoncés comme suit à l'article 24 de la [Politique de respect de la vie privée 2010](#) de l'ICIS :

1. Les personnes dont les renseignements personnels sur la santé sont utilisés pour le couplage de données y consentent au préalable; ou
2. 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.

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 reconstruction ne soit pas raisonnablement prévisible.

L'article 29 de la [Politique de respect de la vie privée 2010](#) de l'ICIS prévoit également 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. Dans le cas des données couplées dans le cadre d'un programme de travail continu de l'ICIS, 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 pour l'usage exclusif de l'ICIS comme aux demandes formulées par des tiers.

Renvoi des données au fournisseur de données

L'article 34 de la [Politique de respect de la vie privée 2010](#) de l'ICIS stipule que le renvoi des données à l'établissement qui les avait fournies à l'ICIS ne constitue pas un acte de divulgation, mais bien une utilisation de données. Le SNIR renvoie donc les données aux établissements qui les ont soumises dans les contextes suivants.

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

Les établissements 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 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 une copie des données qu'il a soumises au SNIR, sous forme de renvoi des données au fournisseur.

En plus du renvoi des données aux établissements déclarants, l'article 34 de la [Politique de respect de la vie privée 2010](#) de l'ICIS stipule que l'ICIS peut remettre les enregistrements au ministère de la Santé concerné, pour des motifs de qualité des données ou à d'autres fins inscrites dans son mandat, comme la planification, l'évaluation et l'affectation des ressources relativement à la gestion des services de santé et de la santé de la population.

Restriction de la divulgation

Divulgation aux fournisseurs de données

L'ICIS rend les données du SNIR accessibles aux fournisseurs au moyen des rapports électroniques du SNIR. Cette application en ligne sécurisée fournit aux utilisateurs des renseignements sur les services de réadaptation qui sont agrégés et permettent d'identifier un établissement. Les établissements qui soumettent des données au SNIR, les ministères de la Santé, les régies régionales de la santé et d'autres organismes approuvés ont accès aux rapports électroniques du SNIR.

Les rapports électroniques du SNIR fournissent de l'information sur divers sujets, notamment

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

- le nombre de jours pendant lesquels les services de réadaptation ont été dispensés;
- l'ampleur dans laquelle les capacités physiques et fonctions cognitives des patients se sont améliorées grâce à la réadaptation;
- les ressources estimées utilisées pour la prestation des services de réadaptation;
- les caractéristiques démographiques des patients (p. ex. statut d'emploi) pertinentes à la réadaptation.

Les utilisateurs autorisés accèdent aux rapports à l'aide d'un outil d'exploitation des données en ligne sécurisé qui leur permet de consulter et de personnaliser les rapports en fonction de leurs besoins opérationnels. Les utilisateurs peuvent par exemple personnaliser les rapports de sorte à obtenir des renseignements ciblés sur

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

Les organismes doivent signer une entente de service auprès de l'ICIS avant de pouvoir accéder aux rapports électroniques du SNIR. L'entente est signée par un cadre supérieur de l'organisme afin de s'assurer que l'organisme connaît ses responsabilités ainsi que celles de ses utilisateurs. L'entente de service comprend des règles visant notamment à

- restreindre l'utilisation du système d'information aux fins déterminées;
- empêcher les utilisateurs d'essayer d'identifier une personne représentée dans un rapport;
- interdire la publication de cellules comprenant moins de 5 observations;
- garantir la sécurité de l'information (p. ex. en protégeant les mots de passe des utilisateurs);
- informer l'ICIS de tout accès non autorisé au système d'information;
- désigner une personne-ressource au sein de l'organisme ayant pour responsabilité d'indiquer les utilisateurs désignés aux Services centraux à la clientèle de l'ICIS.

Les demandes d'accès aux rapports électroniques du SNIR sont acheminées au groupe des SCC de l'ICIS. Celui-ci

- s'assure que l'utilisateur est associé à l'organisme;
- confirme, auprès de la personne-ressource de l'organisme, que le demandeur est un utilisateur désigné ainsi que les privilèges d'accès associés à son profil;
- accorde à l'utilisateur désigné les privilèges d'accès appropriés.

Chaque fois qu'il accède aux rapports électroniques du SNIR, l'utilisateur désigné doit accepter les conditions d'utilisation dont les règles sont semblables à celles définies dans l'entente de service.

Outre les rapports électroniques du SNIR, les utilisateurs autorisés ont accès à des données agrégées et permettant d'identifier un établissement à partir du Portail de l'ICIS, un autre outil de production de rapports qui comprend des données du SNIR depuis 2011. Le Portail de l'ICIS fait l'objet d'une [évaluation des incidences sur la vie privée](#) distincte.

Diffusion publique des données du SNIR

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. Des statistiques agrégées et des analyses sont publiées dans les documents et sur le site Web de l'ICIS. En général, il faut un regroupement d'au moins 5 observations par cellule.

Demandes de données formulées par de tierces parties

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

L'ICIS administre un programme de demandes de données par des tiers qui contient des mesures de contrôle appropriées de la vie privée et de la sécurité et s'assure de leur respect par l'organisme demandeur. En outre, comme le stipulent les articles 45 à 47 de sa [Politique de respect de la vie privée 2010](#), l'ICIS s'efforce de divulguer les données dans le plus grand anonymat possible tout en répondant aux exigences de la recherche ou de l'analyse. 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 divulguer au destinataire des données au niveau de l'enregistrement qui ont été dépersonnalisées. La décision est prise en fonction de chaque cas, et le destinataire doit au préalable signer une entente de protection des données ou un autre instrument juridique. Seuls les éléments de données nécessaires aux fins prévues seront divulgués.

En 2009, l'ICIS a adopté une approche de gestion qui tient compte du cycle de vie complet des données. 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 destinataires tiers de données 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 doivent 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 précisent que les organismes destinataires doivent veiller à la stricte confidentialité des données dépersonnalisées 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.

Depuis janvier 2011, outre le processus de surveillance de la conformité, qui consiste à s'assurer que les données saisies satisfont aux exigences en matière de destruction de données, 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 signés.

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 peut conserver les données de ce système aussi longtemps que nécessaire pour la réalisation des fins déterminées.

3.7 Sixième principe : Exactitude des renseignements personnels sur la santé

L'ICIS s'est doté d'un programme exhaustif sur la qualité des données. Tout problème connu de qualité des données est 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 subir régulièrement une évaluation de la qualité des données fondée sur le *cadre de la qualité des données* 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.

3.8 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](#) en vue d'offrir une approche globale de gestion du respect de la vie privée et de la sécurité. Fondé sur les pratiques exemplaires qui ont cours dans les secteurs public, privé et de la santé, le cadre 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 et de collecte, d'accès, de conservation, de stockage, d'utilisation, de divulgation et d'élimination. Par conséquent, l'ICIS a adopté un ensemble complet de politiques qui précisent les contrôles nécessaires à la protection de l'information en format physique et électronique, y compris à l'étape du chiffrement et de l'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 dossiers, afin de garantir la confidentialité, l'intégrité et la disponibilité des actifs informationnels de l'ICIS.

Les registres de contrôle et de vérification du système font partie intégrante du programme de sécurité de l'information de l'ICIS. Qui plus est, ces registres sont immuables. En général, l'ICIS utilise des données dépersonnalisées au niveau de l'enregistrement (où le numéro d'assurance-maladie a été supprimé ou chiffré) pour réaliser ses analyses. Exceptionnellement, le personnel doit avoir accès aux numéros d'assurance-maladie d'origine. La Politique de respect de la vie privée 2010 de l'ICIS prévoit des contrôles stricts qui garantissent que l'accès est autorisé au niveau et dans les circonstances 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 exceptionnellement extraits des bases de données de production de l'ICIS et mis à la disposition des analystes internes;
- 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 préalable expresse de l'ICIS ni au-delà de cette autorisation.

L'ICIS s'emploie à protéger son système de technologie 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 de l'ICIS. Toutes les recommandations issues de ces 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.

3.9 Huitième principe : Transparence de la gestion des renseignements personnels sur la santé

L'ICIS publie de l'information concernant ses politiques sur le respect de la vie privée, ses pratiques relatives aux données et ses programmes de gestion des renseignements personnels sur la santé. Plus précisément, le [Cadre de respect de la vie privée et de sécurité](#) et la [Politique de respect de la vie privée 2010](#) de l'ICIS sont accessibles au public sur son site Web (www.icis.ca).

3.10 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.

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

Comme il est précisé aux articles 64 et 65 de la [Politique de respect de la vie privée 2010](#) de l'ICIS, les plaintes concernant le traitement par l'ICIS des renseignements personnels sur la santé sont examinées par la chef de la protection des renseignements personnels. Cette dernière 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

Aucune recommandation n'a été formulée jusqu'ici. Les risques de violation de la vie privée décelés dans le cadre de la présente évaluation des incidences sur la vie privée ont été atténués. L'évaluation sera mise à jour ou révisée conformément à la [Politique d'évaluation des incidences sur la vie privée](#) de l'ICIS.

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.

Tous droits réservés.

Le contenu de cette publication peut être reproduit tel quel, en tout ou en partie et par quelque moyen que ce soit, uniquement à des fins non commerciales pourvu que l'Institut canadien d'information sur la santé soit clairement identifié comme le titulaire du droit d'auteur. Toute reproduction ou utilisation de cette publication et de son contenu à des fins commerciales requiert l'autorisation écrite préalable de l'Institut canadien d'information sur la santé. La reproduction ou l'utilisation de cette publication ou de son contenu qui sous-entend le consentement de l'Institut canadien d'information sur la santé, ou toute affiliation avec celui-ci, est interdite.

Pour obtenir une autorisation ou des renseignements, veuillez contacter l'ICIS :

Institut canadien d'information sur la santé
495, chemin Richmond, bureau 600
Ottawa (Ontario) K2A 4H6

Téléphone : 613-241-7860

Télécopieur : 613-241-8120

www.icis.ca

droitdauteur@icis.ca

© 2015 Institut canadien d'information sur la santé

This publication is also available in English under the title *National Rehabilitation Reporting System Privacy Impact Assessment, September 2015*.

Parlez-nous

ICIS Ottawa

495, rue Richmond, bureau 600
Ottawa (Ontario) K2A 4H6
Téléphone : 613-241-7860

ICIS Toronto

4110, rue Yonge, bureau 300
Toronto (Ontario) M2P 2B7
Téléphone : 416-481-2002

ICIS Victoria

880, rue Douglas, bureau 600
Victoria (Colombie-Britannique) V8W 2B7
Téléphone : 250-220-4100

ICIS Montréal

1010, rue Sherbrooke Ouest, bureau 300
Montréal (Québec) H3A 2R7
Téléphone : 514-842-2226

ICIS St. John's

140, rue Water, bureau 701
St. John's (Terre-Neuve-et-Labrador) A1C 6H6
Téléphone : 709-576-7006