



# Évaluation des incidences sur la vie privée du Portail de l'ICIS

Octobre 2020



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.

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

[icis.ca](http://icis.ca)

[droitdauteur@icis.ca](mailto:droitdauteur@icis.ca)

© 2021 Institut canadien d'information sur la santé

Comment citer ce document :

Institut canadien d'information sur la santé. *Évaluation des incidences sur la vie privée du Portail de l'ICIS, octobre 2020*. Ottawa, ON : ICIS; 2021.

This publication is also available in English under the title *CIHI Portal Privacy Impact Assessment, October 2020*.

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](#) :

- *Portail de l'ICIS, octobre 2020*

Approuvé par

Brent Diverty

Vice-président, Stratégies de données et Statistiques

Rhonda Wing

Chef de la protection des renseignements personnels et avocate générale

Ottawa, octobre 2020

# Table des matières

Le Portail de l'ICIS en bref . . . . .	5
Définitions . . . . .	6
1 Introduction . . . . .	7
2 Renseignements contextuels . . . . .	8
2.1 Présentation du Portail de l'ICIS . . . . .	8
2.2 Sources de données . . . . .	10
2.3 Gestion de l'accès et cheminement des données du Portail de l'ICIS . . . . .	14
3 Analyse du respect de la vie privée . . . . .	17
3.1 Programme de gestion des risques liés au respect de la vie privée et à la sécurité . . . . .	17
3.2 Autorités régissant les données du Portail de l'ICIS . . . . .	18
3.3 Premier principe : responsabilité à l'égard des renseignements personnels sur la santé. . . . .	20
3.4 Deuxième principe : établissement des objectifs de la collecte de renseignements personnels sur la santé. . . . .	22
3.5 Troisième principe : consentement pour la collecte, l'utilisation ou la divulgation de renseignements personnels sur la santé . . . . .	22
3.6 Quatrième principe : restriction de la collecte de renseignements personnels sur la santé . . . . .	22
3.7 Cinquième principe : restriction de l'utilisation, de la divulgation et de la conservation des renseignements personnels sur la santé . . . . .	23
3.8 Sixième principe : exactitude des renseignements personnels sur la santé . . . . .	26
3.9 Septième principe : mesures de protection des renseignements personnels sur la santé . . . . .	26
3.10 Huitième principe : transparence de la gestion des renseignements personnels sur la santé . . . . .	28
3.11 Neuvième principe : accès individuel aux renseignements personnels sur la santé et modification de ceux-ci . . . . .	28
3.12 Dixième principe : plaintes concernant le traitement par l'ICIS des renseignements personnels sur la santé . . . . .	28
4 Conclusion . . . . .	29
Annexe . . . . .	29
Texte de remplacement pour les figures . . . . .	29

# Le Portail de l'ICIS en bref

1. Le Portail de l'ICIS est une façon sûre d'accéder à certaines données qui figurent déjà dans les Bases de données clinico-administratives (BDCA)<sup>i</sup>, le Système national d'information sur la réadaptation (SNIR) et la Base de données canadienne SIG (BDCS) de l'Institut canadien d'information sur la santé (ICIS). Il contient également des fichiers publics de Statistique Canada.
2. Sur le Portail de l'ICIS, les données des banques de données existantes (p. ex. BDCA, SNIR et BDCS) sont présentées séparément. Toutes les données confidentielles ou sensibles sur les patients, telles que les numéros d'assurance maladie, de dossier, d'inscription ou du dispensateur ainsi que les dates de naissance complètes et les codes postaux complets, ont été supprimées ou tronquées.
3. Grâce à cet outil, les clients peuvent créer des rapports sur les activités clinico-administratives, les ressources, la prestation de services, l'efficacité et les caractéristiques démographiques de la population.
4. Le Portail de l'ICIS constitue une plaque tournante pour la collaboration et l'établissement de communautés de pratique. Il permet également aux clients de
  - partager et consulter des rapports préétablis, rechercher des données en fonction de leurs propres critères et créer des rapports personnalisés aux fins d'évaluation, de prise de décisions et de transfert des connaissances;
  - favoriser la mesure de la performance sur une base régulière et l'établissement de pratiques exemplaires en leur offrant la possibilité de comparer leur organisme avec des groupes homologues à l'échelle locale, régionale, provinciale et nationale.
5. Les clients sont notamment des hôpitaux, des autorités sanitaires régionales, des ministères de la Santé ou d'autres organismes publics liés aux soins de santé.
6. Avant d'utiliser le Portail de l'ICIS, les clients doivent signer l'Entente de services de rapports électroniques sécurisés de l'ICIS. Cette entente balise l'utilisation et la divulgation par les clients de données dépersonnalisées et de renseignements permettant d'identifier un établissement de santé obtenus par l'intermédiaire du Portail de l'ICIS. Plus précisément, les clients et leurs utilisateurs désignés peuvent se servir de ces données uniquement aux fins d'utilisation interne non commerciale liée à leurs activités de gestion, de qualité des données, de planification, de recherche, d'analyse ou de prise de décisions reposant sur des données probantes.

---

i. Les BDCA sont la Base de données sur les congés des patients (BDCA) et le Système national d'information sur les soins ambulatoires (SNISA).

7. Le Portail de l'ICIS n'offre aucun accès direct aux enregistrements. Les utilisateurs désignés qui font des demandes liées à la création de rapports peuvent obtenir comme résultat des rangées indiquant des nombres d'enregistrements, mais ils ne peuvent pas consulter un enregistrement particulier ni en demander l'extraction.
8. L'une des caractéristiques uniques du Portail de l'ICIS est la présence d'une fonction d'analyse des données au niveau du patient, qui permet aux clients de dégager des tendances dans les réadmissions au fil du temps et selon l'emplacement géographique. Cette fonction est le résultat du couplage des données de la BDCP et du SNISA seulement.

## Définitions

Les définitions suivantes s'appliquent aux termes utilisés dans la présente évaluation des incidences sur la vie privée :

**Entente de services** désigne l'Entente de services de rapports électroniques sécurisés de l'ICIS.

**Client** désigne l'organisme mentionné dans l'Entente de services qui accepte d'être lié par les modalités de l'Entente de services pour accéder au Portail de l'ICIS.

**Utilisateur désigné** désigne un employé du client ou un entrepreneur autorisé par le client auquel le client a autorisé l'accès au Portail de l'ICIS et son utilisation.

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

**Renseignements identifiant un établissement de santé** désigne toute information qui identifie directement un établissement de santé par son nom.

# 1 Introduction

L'Institut canadien d'information sur la santé (ICIS) recueille et analyse de l'information sur la santé et les soins de santé au Canada. Il a pour mandat de fournir une information comparable et exploitable qui favorise une amélioration rapide des soins de santé, de la performance des systèmes de santé et de la santé de la population dans l'ensemble du continuum de soins. L'ICIS recueille les données auprès des hôpitaux et d'autres établissements de santé, des centres 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 offrent ces services et sur le coût des services de santé.

La présente Évaluation des incidences sur la vie privée (EIVP) a pour but d'examiner les risques liés au respect de la vie privée, à la confidentialité et à la sécurité associés au Portail de l'ICIS. Elle remplace la version de mai 2014 et comprend 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 Portail de l'ICIS. Elle passe également en revue l'application du [Cadre de gestion des risques liés au respect de la vie privée et à la sécurité](#) de l'ICIS.

Cette évaluation vise surtout à respecter la [Politique d'évaluation des incidences sur la vie privée](#) de l'ICIS.

## 2 Renseignements contextuels

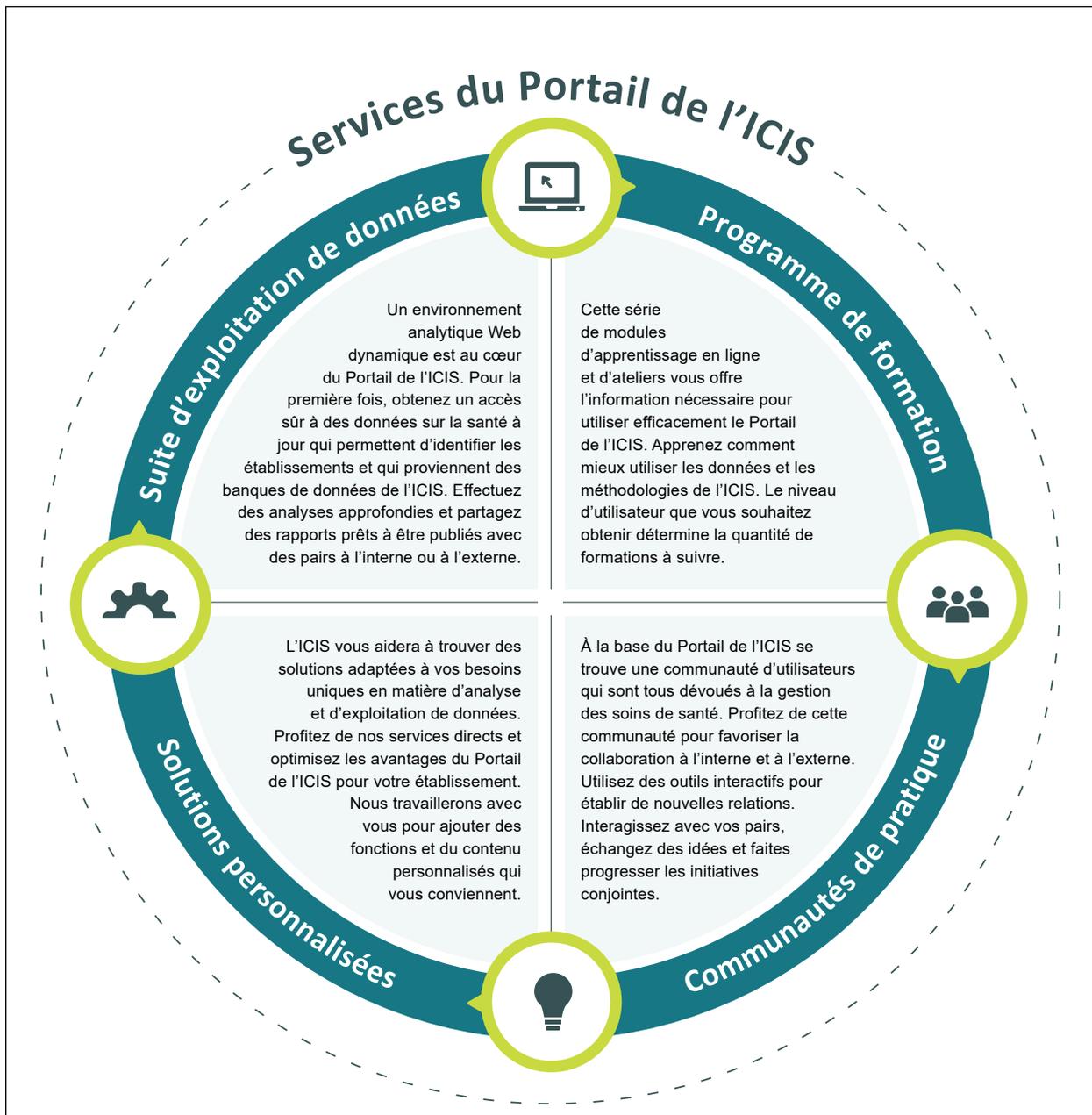
### 2.1 Présentation du Portail de l'ICIS

Le Portail de l'ICIS est un outil analytique Web consacré aux données sur les soins de santé. Conçu par l'ICIS, il vise à répondre aux besoins de ses clients, qui sont également, pour la plupart, ses fournisseurs de données.

Cet outil a pour but d'aider les organismes de services de soins de santé, comme les hôpitaux, les autorités sanitaires régionales et les ministères de la Santé, en leur fournissant un accès en ligne à des données pancanadiennes sur les soins de santé dans un environnement sécuritaire qui protège la vie privée et la confidentialité aux fins de surveillance, de planification et de prise de décisions liées à la prestation des services de santé. L'équipe du Portail de l'ICIS propose un programme de formation complet, de l'aide pour la création de communautés de pratique, des solutions personnalisées pour la production de rapports et du soutien continu aux clients.

Le Portail de l'ICIS offre à ses clients la possibilité de partager et de consulter des rapports préétablis, de rechercher des données en fonction de leurs propres critères et de créer des rapports personnalisés aux fins d'évaluation, de prise de décisions et de transfert de connaissances. Il favorise la mesure de la performance sur une base régulière et l'établissement de pratiques exemplaires en permettant aux clients de comparer leur organisme avec des groupes homologues à l'échelle locale, régionale, provinciale et nationale. Les clients peuvent mener des activités de recherche et de planification en matière d'administration clinique, de ressources, de prestation de services, d'efficacité et de caractéristiques démographiques de la population. Le Portail de l'ICIS constitue une plaque tournante pour la collaboration et l'établissement de communautés de pratique. Par l'intermédiaire du portail, les clients ont la possibilité de faire partager leurs rapports, leurs méthodologies et leurs résultats auprès de pairs de divers organismes. Collectivement, ils peuvent créer des réseaux internes et externes de collaboration. Cet ensemble unique de caractéristiques permet aux utilisateurs de différents paliers de gestion des soins de santé au pays de répondre aux questions qui leur sont propres.

**Figure 1** Services du Portail de l'ICIS



Le Portail de l'ICIS vise 2 types de clients :

1. **Organismes soumettant des données** : Fournisseurs de données, tels que des établissements de soins de santé, des autorités sanitaires régionales, certaines communautés de pratique et les ministères de la Santé provinciaux et territoriaux participants.
2. **Organismes ne soumettant pas de données** : Provinciaux ou territoriaux : Avec le soutien ou l'approbation du ministre de la Santé de la province ou du territoire de l'organisme à l'origine de la demande.

Fédéraux : En ce qui concerne les ministères ou les organismes fédéraux ou les organismes pancanadiens qui ne relèvent pas de provinces ou de territoires, les critères suivants doivent être pris en compte :

- L'organisme à l'origine de la demande est responsable de planifier et de gérer les systèmes de santé ou a un pouvoir décisionnel relatif aux politiques de ces systèmes (voir les articles 37a) et b) de la [Politique de respect de la vie privée, 2010](#));
- L'organisme à l'origine de la demande possède une expertise dans la gestion des données au niveau de l'enregistrement, y compris les politiques et les processus appropriés de sécurité et de respect de la vie privée.

Les demandes d'accès au Portail de l'ICIS sont soumises à l'approbation du vice-président, Communications et Expérience client de l'ICIS. Le Comité exécutif de l'ICIS est ensuite informé de toutes les approbations d'organismes qui ne soumettent pas de données.

## 2.2 Sources de données

Le Portail de l'ICIS est alimenté par 2 sources de données : des sous-ensembles de banques de données existantes de l'ICIS et les fichiers publics de Statistique Canada. Les banques de données existantes de l'ICIS sont les Bases de données clinico-administratives (BDCA), le Système national d'information sur la réadaptation (SNIR) et la Base de données canadienne SIG (BDCS) (vous trouverez ci-dessous plus de renseignements sur ces banques de données).

Sur le Portail de l'ICIS, les données de ces banques de données existantes sont présentées séparément. Toutes les données confidentielles ou sensibles sur les patients, telles que les numéros d'assurance maladie, de dossier, d'inscription ou du dispensateur ainsi que les dates de naissance complètes et les codes postaux complets, ont été tronquées ou supprimées du dépôt de données. Le groupe de travail sur les données sensibles de l'ICIS, un sous-comité du Comité sur le respect de la vie privée, la confidentialité et la sécurité, est responsable du masquage des données confidentielles ou sensibles sur les patients dans les cas d'avortement ou d'aide médicale à mourir.

Actuellement, le Portail de l'ICIS conserve certaines données pour les 5 à 10 dernières années, selon la banque de données.

## Données de l'ICIS

### Bases de données clinico-administratives

Les BDCA sont 2 bases de données pancanadiennes distinctes : la Base de données sur les congés des patients-Base de données sur la morbidité hospitalière (BDCA-BDMH) et le Système national d'information sur les soins ambulatoires (SNISA). Ces bases de données administratives contiennent des renseignements sur les patients, les fournisseurs et les établissements de santé. On y trouve par exemple des données personnelles, géographiques et démographiques sur les patients ainsi que des renseignements cliniques, diagnostiques, administratifs ou encore liés aux interventions ou à d'autres aspects de la prestation de soins obtenus lors des sorties des patients hospitalisés en soins de courte durée, des sorties du service d'urgence ou encore des sorties des patients en consultation externe (soins ambulatoires, p. ex. clinique, chirurgie d'un jour). Parmi les renseignements sur les fournisseurs de soins de santé compris dans les BDCA, mentionnons leur type de services (p. ex. cardiologie) et leur rôle dans le traitement du patient (p. ex. médecin principal, consultant). Les renseignements permettant d'identifier les établissements de santé (c.-à-d. ceux qui identifient directement un établissement de santé par son nom) sont entre autres fournis pour les établissements où les patients ont reçu des soins. Il s'agit notamment de renseignements sur les établissements de départ ou de destination en cas de transfert. De plus, les BDCA comprennent des variables dérivées à valeur ajoutée, comme les groupes de maladies analogues.

Les BDCA recueillent également des renseignements dans des champs de projet spécial, utilisés par les fournisseurs de données pour saisir à l'aide de caractères alphanumériques des renseignements complémentaires qui ne sont pas déclarés de façon systématique.

Pour obtenir un complément d'information, consultez l'[EIVP des BDCA](#).

### Système national d'information sur la réadaptation

Le SNIR recueille des renseignements sur l'ampleur de l'amélioration des aptitudes physiques et cognitives des patients hospitalisés en réadaptation ainsi qu'une multitude de renseignements complémentaires comme les dates de début et de fin des services de réadaptation du patient, des estimations des ressources consommées pour la prestation de ces services ainsi que des caractéristiques sociodémographiques des patients pertinentes pour la réadaptation. Il contient des données sur les patients hospitalisés qui reçoivent des services de réadaptation pour diverses affections, comme un traumatisme ou une chirurgie orthopédique, un accident vasculaire cérébral et un dysfonctionnement de la moelle épinière.

Pour obtenir un complément d'information, consultez l'[EIVP du SNIR](#).

## Base de données canadienne SIG (BDCS)

La BDCS recueille des données sur les activités quotidiennes des organismes de services de santé et produit des rapports pertinents à partir de renseignements financiers et statistiques sur les hôpitaux et les autorités sanitaires régionales de partout au pays. Les données sont recueillies selon un cadre normalisé. La BDCS ne contient pas de renseignements permettant d'identifier les patients. Elle contient cependant des renseignements sur les salaires des employés, résumés au niveau du centre d'activité national, des organismes de soins de santé qui soumettent des données; aucun renseignement permettant d'identifier les employés, comme leur nom ou leur numéro d'employé, n'est inclus.

Pour obtenir un complément d'information, consultez l'[EIVP de la BDCS](#).

## Données de référence (données complémentaires)

Les données de référence englobent notamment l'index organisationnel (IO) de l'ICIS, ainsi que des données démographiques et géographiques (GeoDIM), agrégées et non confidentielles, obtenues auprès de Statistique Canada.

### Index organisationnel

L'ICIS a créé l'IO et le tient à jour afin d'atteindre les objectifs suivants :

- Atténuer les variances dans les renseignements sur les organismes, par exemple leur nom;
- Simplifier le couplage des organismes dans plusieurs banques de données;
- Faire le suivi des changements constants dans les organismes et leurs relations hiérarchiques;
- Consigner les changements organisationnels au fil du temps.

Le Portail de l'ICIS se fonde sur les renseignements de l'IO pour regrouper les résultats afin de garantir l'exactitude des rapports à plusieurs niveaux (de l'hôpital, régional, provincial, territorial et national). Par exemple, lorsqu'une province est responsable de plusieurs autorités sanitaires régionales, l'IO permet de veiller à ce que les données puissent être

- regroupées à l'échelle de la province;
- divisées à l'échelle
  - de toute autorité sanitaire régionale qui relève de la province;
  - de toute association qui relève d'une autorité sanitaire régionale;
  - de tout établissement de soins de santé relevant d'une association qui le gère et en est propriétaire.

## Données démographiques

Les estimations de la population sont des ensembles de données créés par l'ICIS à partir des fichiers démographiques de Statistique Canada, selon le recensement et les derniers fichiers des limites. L'ICIS utilise ces estimations pour calculer les indicateurs axés sur la population. Elles peuvent également servir au calcul des taux normalisés selon l'âge ou le sexe ainsi que d'autres statistiques.

## Données géographiques

Les données géographiques (GeoDIM) sont un ensemble de données créé par l'ICIS à partir du Fichier de conversion des codes postaux (FCCP) de Statistique Canada et du document [Régions sociosanitaires : limites et correspondance avec la géographie du recensement](#).

Les produits de production de rapports électroniques de l'ICIS utilisent les données géographiques pour attribuer des renseignements géographiques selon le code postal du patient (ou de l'établissement).

## Statistique Canada : Fichier de conversion des codes postaux

### Revenus (quintiles et déciles)

Les renseignements sur les revenus nationaux et régionaux sont tirés du FCCP de Statistique Canada, qui se fonde sur les données du recensement.

Les éléments de données accessibles dans le Portail de l'ICIS comprennent le quintile et le décile de l'aire de diffusion dans lesquels est classé le patient. Plus précisément, l'ICIS a ajouté 4 éléments de données sur le revenu dans le Portail de l'ICIS :

- **Quintiles de revenus nationaux** : correspond au revenu par équivalent-personne (RPEP) à l'échelle nationale divisé en 5 catégories égales; il s'agit d'une mesure du revenu ajusté selon la taille des ménages, fondée sur les données sommaires du dernier recensement.
- **Déciles de revenus nationaux** : correspond au RPEP à l'échelle nationale divisé en 10 catégories égales; il s'agit d'une mesure du revenu ajusté selon la taille des ménages, fondée sur les données sommaires du dernier recensement.
- **Quintiles de revenus régionaux** : correspond au revenu du quartier par équivalent-personne à l'échelle régionale (quintiles de revenus du quartier) divisé en 5 catégories égales; il s'agit d'une mesure de revenu ajusté selon la taille des ménages, fondée sur les données sommaires du dernier recensement.
- **Déciles de revenus régionaux** : correspond au revenu du quartier par équivalent-personne à l'échelle régionale (déciles de revenus du quartier) divisé en 10 catégories égales; il s'agit d'une mesure de revenu ajusté selon la taille des ménages, fondée sur les données sommaires du dernier recensement.

L'introduction des quintiles et des déciles de revenus nationaux et des quartiers permet d'effectuer des analyses spéciales des populations de patients en fonction du statut socioéconomique.

## 2.3 Gestion de l'accès et cheminement des données du Portail de l'ICIS

Le Portail de l'ICIS est utilisé par 2 types de clients : les fournisseurs de données qui soumettent de l'information à l'ICIS (**organismes soumettant des données**) et les **organismes qui ne soumettent pas de données**. Les organismes de cette dernière catégorie qui souhaitent utiliser le Portail de l'ICIS doivent satisfaire aux critères définis par l'ICIS. Dans le cadre du processus de gestion des accès, les 2 types de clients doivent signer l'Entente de services de l'ICIS et l'annexe relative au Portail propre à chaque type de client (voir la [section 3.2](#) pour obtenir un complément d'information).

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. L'ICIS gère l'autorisation et la révocation de l'accès à ses applications sécurisées conformément aux processus établis du système de gestion de l'accès.

Il existe 3 types de demandes d'accès (nouvel accès, accès existant et révocation d'accès) et 2 types d'utilisateurs désignés (analystes et consommateurs d'information) :

### Types de demandes

#### Accès pour de nouveaux clients

Les organismes qui n'ont pas signé d'entente avec l'ICIS pour utiliser son portail doivent remplir et signer l'Entente de services et l'annexe relative au Portail. Un nouveau client doit notamment définir une personne-ressource de l'organisme (PRO), c.-à-d. la personne désignée par le client pour mettre en œuvre les modalités de l'Entente de services, qui est responsable de déterminer qui sont les utilisateurs désignés et quels sont leurs droits d'accès (voir ci-dessous). Une fois ces documents signés et retournés à l'ICIS, celui-ci accordera l'accès approprié et enverra des notifications aux nouveaux utilisateurs désignés.

#### Demandes d'accès pour des organismes clients

Pour qu'un utilisateur désigné d'un organisme déjà client de l'ICIS soit ajouté, la PRO désignée doit en faire la demande officielle. L'ICIS modifiera l'annexe relative au Portail de l'ICIS et l'enverra à la PRO afin qu'elle confirme la demande d'accès. Une fois l'annexe modifiée signée, l'ICIS accordera l'accès approprié, informera la PRO et enverra une notification au nouvel utilisateur désigné.

## Révocation d'accès

Pour qu'un accès au Portail de l'ICIS soit révoqué, la PRO doit en faire la demande officielle. L'ICIS communiquera avec elle pour confirmer la demande de révocation d'accès et veiller à ce que l'annexe relative au Portail de l'ICIS soit modifiée et signée. Une fois l'annexe signée, l'ICIS révoquera l'accès et enverra une notification à la PRO.

Prenez note que la signature d'une version modifiée de l'annexe relative au Portail de l'ICIS est nécessaire uniquement pour les analystes. Cette étape n'est pas requise pour les consommateurs d'information.

## Accès en fonction du type d'utilisateur désigné

### Analyste

Les analystes jouissent d'une flexibilité et d'un accès maximums pour travailler avec les données accessibles sur le Portail de l'ICIS (p. ex. pour la création de rapports ou le calcul de nouvelles mesures à partir de données existantes).

### Consommateur d'information

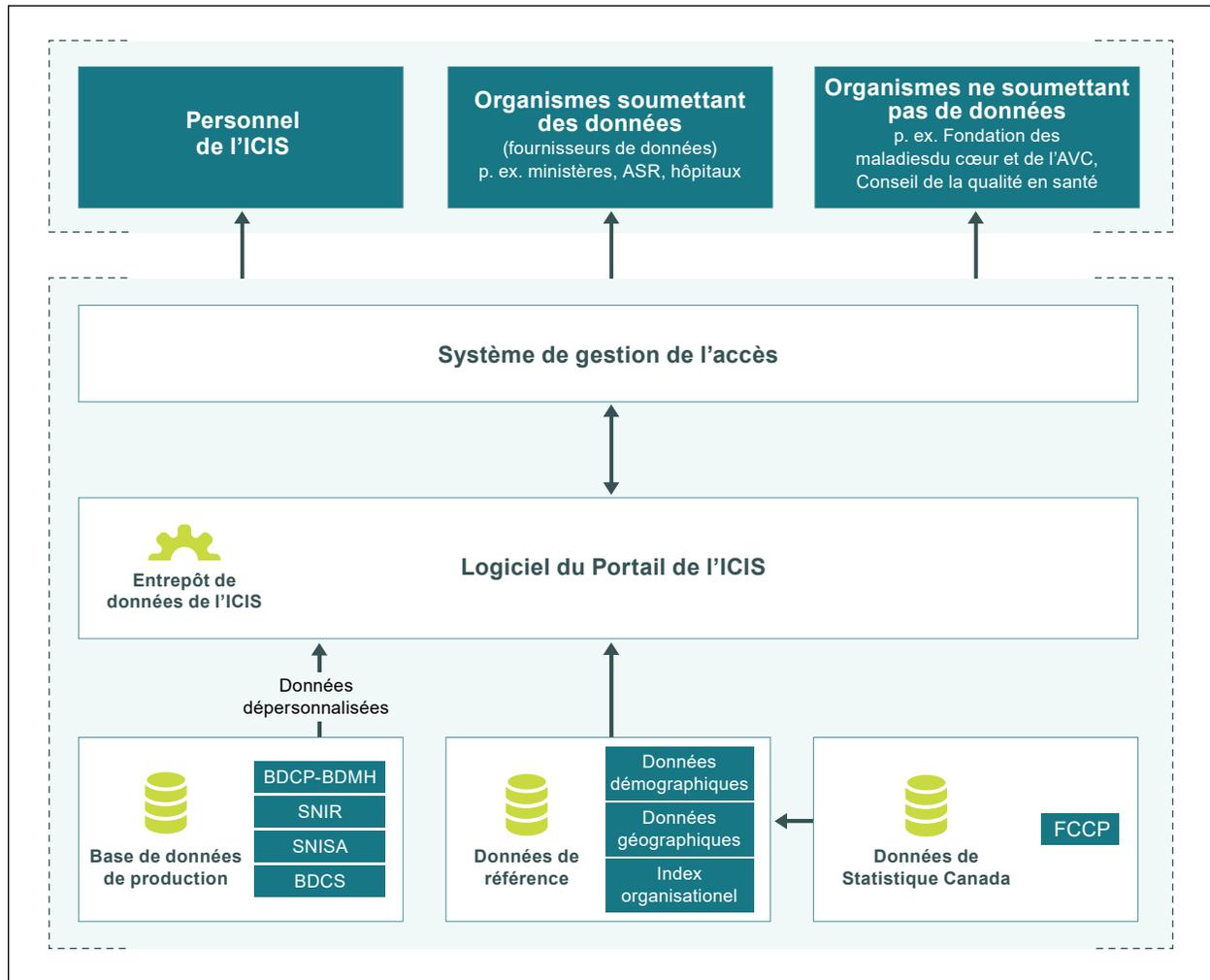
Les consommateurs d'information peuvent afficher, enregistrer et manipuler tous les rapports existants. Les utilisateurs désignés disposant de ce type d'accès ne peuvent pas créer de nouveaux rapports et ont uniquement accès aux données contenues dans les rapports existants. Les résultats de ces interrogations peuvent être publiés dans le Portail de l'ICIS ou être regroupés et exportés vers d'autres formats de fichier (p. ex. MS Excel). Les données au niveau de l'enregistrement dépersonnalisées sous-jacentes ne sont pas exportables.

## Accès des membres du personnel de l'ICIS

L'accès des membres du personnel au Portail de l'ICIS est géré au moyen du processus centralisé d'accès aux données SAS de l'ICIS. Ce processus garantit que toutes les demandes d'accès, y compris aux données du Portail de l'ICIS, 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 Portail de l'ICIS et de sécuriser les données.

La figure ci-dessous donne un aperçu du cheminement des données du Portail de l'ICIS.

**Figure 2** Cheminement des données du Portail de l'ICIS



**Remarques**

ASR : autorités sanitaires régionales.

BDCP-BDMH : Base de données sur les congés des patients-Base de données sur la morbidité hospitalière.

SNISA : Système national d'information sur les soins ambulatoires.

SNIR : Système national d'information sur la réadaptation.

BDCS : Base de données canadienne SIG.

FCCP : Fichier de conversion des codes postaux.

## 3 Analyse du respect de la vie privée

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

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

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

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

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

## 3.2 Autorités régissant les données du Portail de l'ICIS

### Renseignements généraux

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, plus particulièrement à des fins de planification et de gestion des systèmes de santé, ce qui comprend l'analyse statistique et la production de rapports. Il incombe aux fournisseurs de données de respecter les obligations légales de leur province ou territoire, selon le cas, au moment de la collecte des données.

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

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

### Ententes

Les données du Portail de l'ICIS sont régies par la [Politique de respect de la vie privée, 2010](#), les lois en vigueur dans les autorités compétentes et les ententes de partage de données conclues avec les provinces et territoires. Les ententes de partage des données établissent les critères relatifs au but, à l'utilisation, à la divulgation, à la conservation et à la destruction des renseignements personnels sur la santé soumis à l'ICIS, ainsi qu'à toute divulgation pouvant être permise subséquemment. Les ententes décrivent aussi l'autorité législative en vertu de laquelle les renseignements personnels sur la santé sont divulgués à l'ICIS.

## Entente de services de rapports électroniques sécurisés de l'ICIS

Les clients (qu'ils soumettent ou non des données) sont tenus de signer l'Entente de service de l'ICIS. Cette entente limite les clients du Portail de l'ICIS quant à l'utilisation et à la divulgation de données dépersonnalisées et de renseignements permettant d'identifier un établissement de santé obtenus par l'intermédiaire du portail. Plus précisément, les clients et leurs utilisateurs désignés peuvent se servir de ces données uniquement à des fins d'utilisation interne non commerciale liée à des activités de gestion, de qualité des données, de planification, de recherche, d'analyse ou de prise de décisions reposant sur des données probantes. Les clients ne sont pas autorisés à divulguer à des tiers les données du Portail de l'ICIS, sauf s'il s'agit de leurs propres données. La publication ou la divulgation à l'extérieur de l'organisme client est autorisée uniquement lorsque toutes les mesures raisonnables sont prises pour préserver l'identité des personnes et que les données ne contiennent pas de cellules contenant moins de 5 observations. Les renseignements permettant d'identifier un établissement de santé ne peuvent pas être divulgués à moins que le client en informe préalablement l'ICIS afin de lui permettre d'informer le ministère concerné.

Les clients sont responsables de veiller à ce que leurs utilisateurs désignés du Portail de l'ICIS soient informés des modalités de l'Entente de services et les respectent. Ces modalités sont notamment les suivantes :

- Assurer la confidentialité des données dépersonnalisées obtenues sur le Portail de l'ICIS, y compris tous les rapports, avec la même diligence raisonnable dont ils font preuve pour protéger leurs propres données confidentielles, pour éviter le vol, la perte, l'utilisation, la divulgation, la copie, la modification ou la suppression de données, ou encore l'accès non autorisé à ces données, sauf dans les cas expressément prévus dans l'Entente de services ou requis par la loi;
- Dans la mesure du possible, accéder au Portail de l'ICIS uniquement à partir du réseau du client ou de son établissement. Sinon, le client doit veiller à accéder à Internet à partir d'un environnement sûr.

Les clients acceptent d'informer immédiatement l'ICIS de toute utilisation non autorisée de tout mode d'accès d'un utilisateur désigné ou de toute autre violation de la confidentialité ou de la sécurité dont ils ont connaissance.

De plus, l'Entente de services définit les exigences et les responsabilités suivantes en matière de gestion des accès :

- Les clients doivent veiller en tout temps à ce que l'ICIS dispose de données d'inscription exactes pour tous leurs utilisateurs désignés.
- Les clients et leurs utilisateurs désignés sont responsables d'assurer la confidentialité des modes d'accès (p. ex. veiller à la stricte confidentialité des noms d'utilisateurs et des mots de passe). Les modes d'accès ne peuvent pas être partagés avec une autre personne ou une autre entité pour quelque raison que ce soit ni divulgués à de telles personnes. Ils ne sont pas transférables et ne peuvent pas être attribués à un particulier ou à un poste non nommément désigné.
- Les clients ont l'entière responsabilité de toutes les activités menées lors d'un accès obtenu avec les modes d'accès de leurs utilisateurs désignés.
- Les clients et leurs utilisateurs désignés ne doivent pas permettre à des tiers ou à des utilisateurs non autorisés d'accéder au Portail de l'ICIS.

L'ICIS a mis sur pied un programme de formation obligatoire à l'intention des utilisateurs désignés du Portail de l'ICIS; le programme couvre chacun de ces éléments.

L'ICIS rappelle aux utilisateurs désignés qu'avant d'accéder aux données, ils doivent accepter les conditions d'utilisation, qui résument les modalités d'accès et d'utilisation, chaque fois qu'ils ouvrent une session dans le Portail de 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 formé de membres du Conseil d'administration et un conseiller principal externe à la protection des renseignements personnels.

Les clients du Portail de l'ICIS sont responsables du respect de l'Entente de services au sein de leur organisme. Ils sont également soumis aux lois sur la protection des données en vigueur dans leur province ou territoire et au contrôle indépendant des commissaires à la protection de la vie privée ou de leur équivalent.

## Organisation et gouvernance

Le tableau ci-dessous présente les principaux postes de direction internes responsables de la gestion des risques liés au respect de la vie privée et à la sécurité pour les données du Portail de l'ICIS :

**Tableau** Principaux postes et responsabilités

Poste, groupe	Rôles et responsabilités
<b>Vice-présidente, Communications et Expérience client</b>	Responsable de l'orientation stratégique générale des produits numériques de l'ICIS, y compris du Portail de l'ICIS
<b>Directrice, Innovation numérique</b>	Responsable des recommandations et des décisions stratégiques sur l'orientation des produits numériques de l'ICIS (y compris le Portail) et des initiatives de gestion de l'information
<b>Directrice, Stratégie, Architecture et Normes</b>	Responsable des recommandations et des décisions stratégiques sur les principales technologies de l'information afin de contribuer à l'harmonisation ou à l'intégration des initiatives clés avec l'ensemble des priorités et des plans de l'ICIS
<b>Chef de la sécurité de l'information</b>	Responsable de l'orientation stratégique et de la mise en œuvre générale du programme de sécurité de l'information de l'ICIS
<b>Chef de la protection des renseignements personnels</b>	Responsable de l'orientation stratégique et de la mise en œuvre générale du programme de respect de la vie privée de l'ICIS
<b>Gestionnaire, Gestion du contenu et des canaux numériques</b>	Responsable du fonctionnement quotidien des produits numériques de l'ICIS (y compris le Portail de l'ICIS)
<b>Gestionnaire, Renseignements et Intégration de l'information</b>	Responsable du respect des exigences techniques pour le développement, la mise en œuvre et le maintien continus des produits numériques de l'ICIS ainsi que pour l'administration des systèmes

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

Le Portail de l'ICIS est un service fourni par l'ICIS pour répondre aux besoins de ses clients d'accéder en ligne aux données dépersonnalisées pancanadiennes des BDCA, du SNIR et de la BDCS. L'Entente de services limite les droits des clients d'utiliser et de divulguer l'information sur la santé dépersonnalisée et les renseignements permettant d'identifier un établissement de santé obtenus sur le Portail de l'ICIS. Plus précisément, les clients et leurs utilisateurs désignés peuvent se servir de ces données uniquement à des fins d'utilisation interne non commerciale liée à des activités de gestion interne, de qualité des données, de planification, de recherche, d'analyse ou de prise de décisions reposant sur des données probantes. La portée et les objectifs prévus du Portail de l'ICIS sont indiqués clairement dans la présente EIVP et sur le [site Web de la page du Portail de l'ICIS](#).

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

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

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

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

Le Portail de l'ICIS est une façon sûre d'accéder à certaines données déjà détenues par l'ICIS dans les BDCA, le SNIR et la BDCS.

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

### Restriction de l'utilisation

#### Clients

L'ICIS restreint l'utilisation par les clients des données de son portail aux objectifs autorisés décrits à la [section 2.1](#). Cela comprend les analyses comparatives au sein des autorités compétentes et entre celles-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.

#### 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. Des autorisations sont accordées une fois réussis les cours d'apprentissage en ligne sur le Portail de l'ICIS. Un cours est offert pour chaque banque de données qui alimente le Portail de l'ICIS. Les membres du personnel de l'ICIS qui utilisent son portail demeurent liés par l'entente de confidentialité qu'ils doivent tous signer au moment de leur entrée en fonction et qu'ils doivent ensuite renouveler chaque année.

Les données du Portail de l'ICIS utilisées par l'ICIS à des fins d'analyses internes ne contiennent aucun nom ni identificateur direct, comme les numéros d'assurance maladie non chiffrés, les dates de naissance complètes et les codes postaux complets. Ces identificateurs sont supprimés des enregistrements de toutes les banques de données de l'ICIS avant qu'ils soient versés dans le Portail de l'ICIS (consultez la [section 2.2](#)).

### Couplage des données

Le couplage des données est effectué par l'ICIS. Étant donné que les risques d'identification de la personne sont accrus, l'ICIS prend des mesures d'atténuation pertinentes (p. ex. la dépersonnalisation en retirant les identificateurs des patients et en attribuant à ces derniers des numéros de transaction sans signification).

Le couplage de données effectué par le Portail de l'ICIS est un processus automatisé conçu pour rendre possible la fonction relative aux données des patients (réadmission, admissions antérieures, nouvelles visites et visites antérieures), qui permet aux utilisateurs désignés d'analyser plusieurs admissions ou visites (c.-à-d. les admissions antérieures ou ultérieures des patients d'une cohorte dans le même établissement ou d'autres établissements). Ce couplage des données est effectué en arrière-plan, sans l'intervention des clients. Ainsi, les utilisateurs désignés n'ont pas accès aux 4 variables (numéro d'assurance maladie chiffré, province émettrice de la carte d'assurance maladie, date de naissance et genre) utilisées par l'ICIS pour procéder au couplage. Les données peuvent uniquement être couplées à *l'intérieur* d'une même banque de données (soit la BDCP ou le SNISA), et non *entre* les banques.

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 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.

## 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.

## Restriction de la divulgation

Conformément à la [section 3.2](#), avant d'avoir accès au Portail de l'ICIS, les clients doivent signer une Entente de services qui impose des restrictions et des obligations en matière de confidentialité et de sécurité. Les clients ne sont pas autorisés à divulguer à des tiers les données du Portail de l'ICIS, sauf s'il s'agit de leurs propres données.

Les clients sont également soumis aux exigences des lois de protection des données de leurs autorités compétentes respectives.

## Restriction de la conservation

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

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

L'ICIS est doté 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 Portail de l'ICIS 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 Portail de l'ICIS.

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

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

L'ICIS a élaboré un [Cadre de respect de la vie privée et de sécurité](#) visant à offrir une approche globale de la gestion du respect de la vie privée et de la sécurité. Ce cadre est fondé sur des pratiques exemplaires des secteurs public et privé ainsi que du secteur de la santé. Il est conçu de façon à coordonner les politiques de l'ICIS en matière de respect de la vie privée et de sécurité, et à offrir une vision intégrée des pratiques de gestion de l'information adoptées par l'organisme. Les paragraphes qui suivent décrivent les aspects de la sécurité des systèmes de l'ICIS qui revêtent une importance particulière au regard des données du Portail de l'ICIS.

### Sécurité des systèmes

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

Les registres de contrôle et de vérification du système font partie intégrante du programme de sécurité de l'information de l'ICIS. Ces registres sont par ailleurs immuables. En général, l'ICIS utilise des données dépersonnalisées au niveau de l'enregistrement (où le numéro d'assurance maladie a été supprimé ou chiffré) pour réaliser ses analyses. Il arrive dans des circonstances exceptionnelles que le personnel doive avoir accès aux numéros d'assurance maladie d'origine. Les procédures et la politique de respect de la vie privée de 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 préalable expresse de l'ICIS ni au-delà de cette autorisation.

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

Les évaluations de la vulnérabilité et des tests d'intrusion de l'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 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 de protection de la vie privée, ses pratiques en matière de traitement des données et ses programmes de gestion des renseignements personnels sur la santé. Ainsi, 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](http://icis.ca)).

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

L'ICIS n'utilise pas les renseignements personnels sur la santé qu'il détient pour prendre des décisions administratives ou relatives 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 précisé aux articles 64 et 65 de la [Politique de respect de la vie privée, 2010](#) de l'ICIS, les plaintes, questions et préoccupations concernant le traitement des renseignements par l'ICIS sont examinées par la chef de la protection des renseignements personnels, qui peut acheminer une demande ou une plainte au commissaire au respect de la vie privée de la province ou du territoire de l'auteur de la demande ou de la plainte.

## 4 Conclusion

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

La présente EIVP sera mise à jour ou révisée conformément à la [Politique d'évaluation des incidences sur la vie privée](#) de l'ICIS.

## Annexe

### Texte de remplacement pour les figures

#### Figure 1 : Services du Portail de l'ICIS

##### **Suite d'exploitation de données**

Un environnement analytique Web dynamique est au cœur du Portail de l'ICIS. Pour la première fois, obtenez un accès sûr à des données sur la santé à jour qui permettent d'identifier les établissements et qui proviennent des banques de données de l'ICIS. Effectuez des analyses approfondies et partagez des rapports prêts à être publiés avec des pairs à l'interne ou à l'externe.

##### **Programme de formation**

Cette série de modules d'apprentissage en ligne et d'ateliers en classe vous offre l'information nécessaire pour utiliser efficacement le Portail de l'ICIS. Apprenez comment mieux utiliser les données et les méthodologies de l'ICIS. Le niveau d'utilisateur que vous souhaitez obtenir détermine la quantité de formations à suivre.

##### **Solutions personnalisées**

L'ICIS vous aidera à trouver des solutions adaptées à vos besoins uniques en matière d'analyse et d'exploitation de données. Profitez de nos services directs et optimisez les avantages du Portail de l'ICIS pour votre établissement. Nous travaillerons avec vous pour ajouter des fonctions et du contenu personnalisés qui vous conviennent.

##### **Communautés de pratique**

À la base du Portail de l'ICIS se trouve une communauté d'utilisateurs qui sont tous dévoués à la gestion des soins de santé. Profitez de cette communauté pour favoriser la collaboration à l'interne et à l'externe. Utilisez des outils interactifs pour établir de nouvelles relations. Interagissez avec vos pairs, échangez des idées et faites progresser les initiatives conjointes.

## **Figure 2 : Cheminement des données du Portail de l'ICIS**

Le Portail de l'ICIS contient des sous-ensembles de données tirés des bases de données de production existantes de l'ICIS (Base de données sur les congés des patients-Base de données sur la morbidité hospitalière, Système national d'information sur les soins ambulatoires, Système national d'information sur la réadaptation, Base de données canadienne SIG), des données de référence (index organisationnel, données démographiques et géographiques) et les données du Fichier de conversion des codes postaux de Statistique Canada.

Les données dépersonnalisées des bases de données de l'ICIS, les données de référence et les données du Fichier de conversion des codes postaux sont versées dans le Portail de l'ICIS, qui fait partie de l'entrepôt de données de l'ICIS.

Le système de gestion de l'accès de l'ICIS authentifie les utilisateurs autorisés du Portail de l'ICIS, soit les membres du personnel de l'ICIS, les organismes soumettant des données (aussi connus sous le nom de fournisseurs de données, comme les ministères, les autorités sanitaires régionales et les hôpitaux) et les organismes qui ne soumettent pas de données (comme la Fondation des maladies du cœur et de l'AVC et le Conseil de la qualité en santé). Les utilisateurs peuvent accéder au Portail de l'ICIS pour partager et consulter des rapports préétablis, rechercher des données en fonction de leurs propres critères et créer des rapports personnalisés aux fins d'évaluation, de prise de décisions et de transfert de connaissances.



**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

23607-0121

