



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

© 2022 Institut canadien d'information sur la santé

RAI-MDS 2.0 © interRAI Corporation, Washington (D.C.), 1995, 1997, 1999.  
Modifié avec permission pour utilisation au Canada en vertu d'une licence accordée à l'Institut canadien d'information sur la santé. Les éléments propres au Canada et leur description © Institut canadien d'information sur la santé, 2022.

Comment citer ce document :

Institut canadien d'information sur la santé. *Système d'information ontarien sur la santé mentale : évaluation des incidences sur la vie privée, juin 2022.*  
Ottawa, ON : ICIS; 2022.

This publication is also available in English under the title *Ontario Mental Health Reporting System Privacy Impact Assessment, June 2022.*

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

- *Système d'information ontarien sur la santé mentale : évaluation des incidences sur la vie privée*

Approuvée par

Brent Diverty

Vice-président, Stratégies de données et Statistiques

Rhonda Wing

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

Ottawa, juin 2022



# Le Systeme d'information ontarien sur la sante mentale en bref

1. Le Systeme d'information ontarien sur la sante mentale (SIOSM) est une base de donnees de l'Institut canadien d'information sur la sante (ICIS) qui sert a recueillir des donnees sur les soins aux patients hospitalises en sante mentale. L'ICIS analyse ces donnees et les utilise pour produire de l'information statistique exacte, actuelle et comparable sur l'accès aux soins, la qualite de ces soins et les ressources consommées pour leur prestation.
2. Les établissements, ministères de la Santé et autorités sanitaires régionales se servent de cette information pour prendre des décisions éclairées sur les soins aux patients hospitalisés en sante mentale.
3. Le SIOSM recueille principalement des données sur les soins de sante mentale offerts aux patients adultes hospitalisés en Ontario. De plus, le SIOSM reçoit actuellement des données de quelques établissements de Terre-Neuve-et-Labrador et du Manitoba.
4. Chaque enregistrement du SIOSM respecte les exigences du fichier minimal du SIOSM et comprend des identificateurs personnels, des renseignements démographiques,

# 1 Introduction

L'Institut canadien d'information sur la sante (ICIS) recueille et analyse de l'information sur la sante et les soins de sante au Canada. Son mandat consiste à fournir une information comparable et exploitable qui favorise une amélioration rapide des soins de sante, de la performance des systemes de sante et de la sante de la population dans l'ensemble du continuum de soins. L'ICIS obtient des donnees des hopitaux et d'autres établissements de sante, des établissements de soins de longue durée, des autorités sanitaires régionales, des praticiens et des gouvernements. Ces données comprennent des renseignements sur les services de sante dispensés aux patients, sur les professionnels de la sante qui dispensent ces services et sur le coût des services de sante.

La présente évaluation des incidences sur la vie privée a pour but d'examiner les





## 2.2 Collecte de données

### Instrument d'évaluation des résidents — santé mentale

Les hôpitaux recueillent l'information sur les patients au cours de la prestation des services aux patients hospitalisés en santé mentale. Les établissements qui déclarent des données au SIOSM utilisent l'instrument d'évaluation des résidents — santé mentale (RAI-MH), ce qui permet de recueillir des données normalisées. L'instrument RAI-MH a été élaboré conjointement par l'ICIS, interRAI (un réseau regroupant des chercheurs et des praticiens dont l'objectif est d'améliorer les soins de santé pour les personnes handicapées ou présentant des besoins médicaux complexes), le ministère de la Santé de l'Ontario, l'Association des hôpitaux de l'Ontario (OHA) et certains hôpitaux ayant participé au projet pilote. Ces collaborateurs ont déterminé les éléments de données à inclure dans le fichier de données initial et participent à la mise à jour de ce fichier de temps à autre afin d'améliorer la qualité ou la pertinence des données recueillies, d'harmoniser le fichier de données aux normes d'interRAI ou de répondre à d'autres besoins du ministère de la Santé de l'Ontario, de l'OHA ou de l'ICIS.

Certaines données recueillies par les établissements au moyen de l'instrument RAI-MH sont incluses dans l'enregistrement du SIOSM soumis à l'ICIS au sujet du patient. Plus précisément, chaque enregistrement du SIOSM respecte les exigences du fichier minimal du SIOSM et comprend des identificateurs du patient, des renseignements démographiques à son sujet, ses caractéristiques de santé, des données administratives, des identificateurs de l'établissement de santé et des champs de texte libre. De plus amples renseignements sur les données incluses dans le fichier minimal du SIOSM sont accessibles sur le [site Web de l'ICIS](#).

## 2.3 Cheminement des données

Le cheminement des données du SIOSM va comme suit :

1. L'établissement soumet les enregistrements à l'ICIS.
2. Le SIOSM transmet des rapports de soumission pour aider l'établissement à corriger les erreurs relevées dans les enregistrements (p. ex. éléments de données manquants).
3. Une copie des enregistrements tels qu'ils ont été acceptés par le SIOSM ainsi que les rapports qui comprennent des renseignements personnels sur la santé sont mis à la disposition de l'établissement et du ministère. Le ministère de la Santé de l'Ontario ne reçoit pas les données soumises par les établissements du Manitoba et de Terre-Neuve-et-Labrador; ce sont les ministères de la Santé du Manitoba et de Terre-Neuve-et-Labrador qui reçoivent les données des établissements déclarants de leur province respective, en plus des données de l'Ontario agrégées à l'échelle de la province, aux fins de comparaison.



4. L'ICIS fournit des donnees agrégées et au niveau de l'enregistrement aux établissements déclarants et au ministère. L'ICIS fournit des données agrégées aux autorités sanitaires.
5. L'ICIS peut fournir des données agrégées et dépersonnalisées au niveau de l'enregistrement aux tiers qui en font la demande (voir la [section 3.7](#)).

La figure ci-dessous illustre le cv

## 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





## Ententes

À l'ICIS, les données du SIOSM sont régies par la [Politique de respect de la vie privée, 2010](#), la législation en vigueur dans les provinces et territoires et les ententes de partage de données conclues avec les provinces et territoires. Les ententes de partage des données établissent les critères relatifs au but, à l'utilisation, à la divulgation, à la conservation et à la destruction des renseignements personnels sur la santé fournis à l'ICIS, ainsi que toute divulgation subséquentement permise. Les ententes décrivent aussi l'autorité législative selon laquelle les renseignements personnels sur la santé sont divulgués à l'ICIS.

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

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

## Organisation et gouvernance

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

### Tableau Principaux postes et responsabilités

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

L'ICIS a pour mandat de fournir une information comparable et exploitable qui favorise une amélioration rapide des soins de santé, de la performance des systèmes de santé et de la santé de la population dans l'ensemble du continuum de soins. L'organisme produit notamment de l'information sur les soins aux patients hospitalisés en santé mentale afin de soutenir la planification et la gestion des services financés par le secteur public au Canada. Pour ce faire, l'ICIS recueille les types suivants de données du SIOSM aux fins indiquées :

### Identificateurs personnels

Il peut s'agir, par exemple, du numéro d'assurance maladie ou d'un identificateur personnel propre au SIOSM. L'ICIS utilise ces informations pour brosser le portrait complet des soins fournis à la personne en regroupant les enregistrements décrivant les divers types de soins qui lui ont été fournis à divers moments par divers établissements. Afin de pouvoir réunir les enregistrements, l'ICIS doit savoir lesquels se rapportent à la personne. Pour cette raison, tous les enregistrements doivent inclure des identificateurs.

### Caractéristiques démographiques

Il peut s'agir, par exemple, de la date de naissance, du code postal, du sexe, de la situation de famille, de la langue, du niveau d'études, du statut d'emploi ou de données identifiantes sur les Autochtones. L'ICIS utilise l'âge (calculé avec la date de naissance), l'information géographique dérivée du code postal, le sexe, la langue, le statut d'emploi et les données identifiantes sur les Autochtones pour réaliser des analyses démographiques des services de santé fournis et de leurs résultats.

### Caractéristiques de santé

Il peut s'agir, par exemple, de la raison de l'admission, des relations familiales, des sévices subis, des dépendances, des diagnostics de santé mentale, des antécédents pharmaceutiques, des traitements récemment fournis, du risque de s'infliger des blessures ou de blesser autrui, et des problèmes de santé physique. L'ICIS se sert de cette information pour évaluer les types de problèmes de santé qui nécessitent des services de santé mentale pour patients hospitalisés, la qualité des soins fournis à la personne et les coûts associés au traitement.

## Données administratives

Il peut s'agir, par exemple, des dates d'admission à l'établissement et de sortie. À l'aide de ces informations, l'ICIS évalue le temps d'attente pour les soins, de même que les ressources consommées pour leur prestation.





L'accès du personnel à l'environnement du système d'analyse statistique (SAS) est fourni au moyen du processus centralisé d'accès aux données SAS de l'ICIS, qui est géré par le Centre de services de l'ICIS. Cet environnement distinct et sécurisé sert au stockage des fichiers de données analytiques, y compris des fichiers pour usage général, où le personnel doit effectuer ses analyses et en stocker les résultats.

Les fichiers de données pour usage général sont des fichiers prétraités conçus expressément pour les besoins des analystes internes. Le prétraitement consiste à supprimer le numéro d'assurance maladie original (et à le remplacer par un numéro d'assurance maladie non chiffré), la date de naissance complète et le code postal complet, et à les remplacer par un ensemble de variables dérivées standards.

Ce processus garantit que toutes les demandes d'accès, y compris aux données du SIOSM, sont vérifiables et autorisées, conformément à l'article 10 de la [Politique de respect de la vie privée, 2010](#) de l'ICIS. Le système d'accès aux données SAS fait l'objet d'une vérification annuelle qui permet de confirmer que les employés accèdent aux données seulement en cas de nécessité. La [section 3.9](#) explique comment les différentes mesures procédurales et techniques sont mises en place en vue de prévenir l'accès non autorisé aux données du SIOSM et de sécuriser les données de toute autre manière.

## Couplage des données

Les données du SIOSM sont couplées à celles d'autres sources de données de l'ICIS. Comme le couplage des données peut accroître les risques d'identification de la personne, l'ICIS prend des mesures d'atténuation des risques.

Les articles 14 à 31 de la [Politique de respect de la vie privée, 2010](#) de l'ICIS régissent le couplage des enregistrements contenant des renseignements personnels sur la santé. En vertu de cette politique, l'ICIS permet le couplage des renseignements personnels sur la santé dans certaines circonstances. Il est généralement permis de coupler des données au sein d'une seule banque de données pour l'usage exclusif de l'ICIS. Le couplage de données à partir de multiples banques de données pour l'usage exclusif de l'ICIS et toutes les demandes de couplage de données formulées par des tiers sont soumis à un processus interne d'examen et d'approbation. Lors du couplage, l'ICIS utilise généralement des numéros d'assurance maladie chiffrés. Les données couplées demeurent assujetties aux dispositions en matière d'utilisation et de divulgation de la [Politique de respect de la vie privée, 2010](#).



Les criteres d'approbation du couplage de donnees sont enonces comme suit aux articles 23 et 24 de la [Politique de respect de la vie privee, 2010](#) de l'ICIS :

Article 23 Les personnes dont les renseignements personnels sur la sante sont utilises pour le couplage de donnees y consentent au prealable; ou

Article 24 Tous les criteres suivants sont respectes :

- a. l'objectif du couplage de donnees s'inscrit dans le mandat de l'ICIS;
- b. les avantages pour le public sont considerablement plus importants que les risques de violation de la vie privee des personnes;
- c. les resultats du couplage de donnees ne porteront pas prejudice aux personnes concernees;
- d. le couplage de donnees s'inscrit dans un projet precis et ponctuel, et les donnees couplees seront par la suite detruites dans le respect des regles enoncees aux articles 28 et 29;
- e. (peut remplacer le critere d.) le couplage de donnees est effectue dans le cadre d'un programme de travail continu et approuve de l'ICIS; les donnees sont conservees aussi longtemps que necessaire pour la realisation des fins determinees, apres quoi elles sont detruites dans le respect des regles enoncees aux articles 28 et 29;
- f. le couplage de donnees permet de realiser des economies evidentes par rapport a d'autres methodes ou est l'unique methode envisageable.

## Norme de couplage de donnees sur les clients

En 2015, l'ICIS a adopte une norme de couplage de donnees sur les clients a l'echelle de l'organisme. Cette norme regit le couplage des enregistrements qui ont ete crees depuis 2010-2011 et qui contiennent les elements de donnees suivants : numero d'assurance maladie chiffre et province ou territoire ayant emis le numero d'assurance maladie. Les enregistrements qui ne satisfont pas a ces criteres sont regis par un mecanisme de couplage defini au cas par cas.

## Destruction des donnees couplees

L'article 28 de la [Politique de respect de la vie privee, 2010](#) de l'ICIS definit l'exigence selon laquelle l'ICIS doit detruire les renseignements personnels sur la sante et les donnees depersonnalisees de facon securitaire, a l'aide de methodes de destruction qui conviennent au format, au support ou au dispositif, de maniere a ce qu'une reconstitution ne soit pas raisonnablement previsible.

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

## Contribution du SIOSM à la BDSMMH

L'ICIS fusionne les enregistrements du SIOSM et de la [Base de données sur les congés des patients \(BDSP\)](#) pour créer une autre base de données de l'ICIS appelée [Base de données sur la santé mentale en milieu hospitalier \(BDSMMH\)](#), qui fournit de l'information sur les soins de santé mentale offerts aux patients hospitalisés partout au pays<sup>i</sup>. Cette activité ne répond pas aux critères du couplage des données définis dans la [Politique de respect de la vie privée, 2010](#) de l'ICIS, car elle ne donne pas lieu à de nouveaux enregistrements mixtes. La [section 3.7](#) présente de l'information générale sur le couplage des données.

## Renvoi des données au fournisseur

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

L'article 34 de la [Politique de respect de la vie privée, 2010](#) stipule que l'ICIS, en plus de renvoyer les données aux établissements déclarants, peut également remettre les enregistrements au ministère concerné, pour des motifs de qualité des données ou à d'autres fins inscrites dans son mandat (p. ex. la gestion des services de santé et de la santé de la population, qui comprend la planification, l'évaluation et l'affectation des ressources) ou tel qu'il est indiqué dans l'entente de partage des données ou un autre instrument juridique. De même, l'ICIS met les données au niveau de l'enregistrement soumise au SIOSM par les établissements de l'Ontario à la disposition des établissements et du ministère de la Santé de l'Ontario. Ces rapports ne présentent pas les données soumise par les

---

i. Aussi, la BDSMMH recueille directement des données auprès d'un seul établissement au Canada.

établissements du Manitoba et de Terre-Neuve-et-Labrador. De plus, l'ICIS met les données au niveau de l'enregistrement soumise au SIOSM par les établissements du Manitoba et de Terre-Neuve-et-Labrador à la disposition de leur ministère de la Santé respectif. Ces rapports présentent les données de l'Ontario agrégées à l'échelle de la province, aux fins de comparaison.

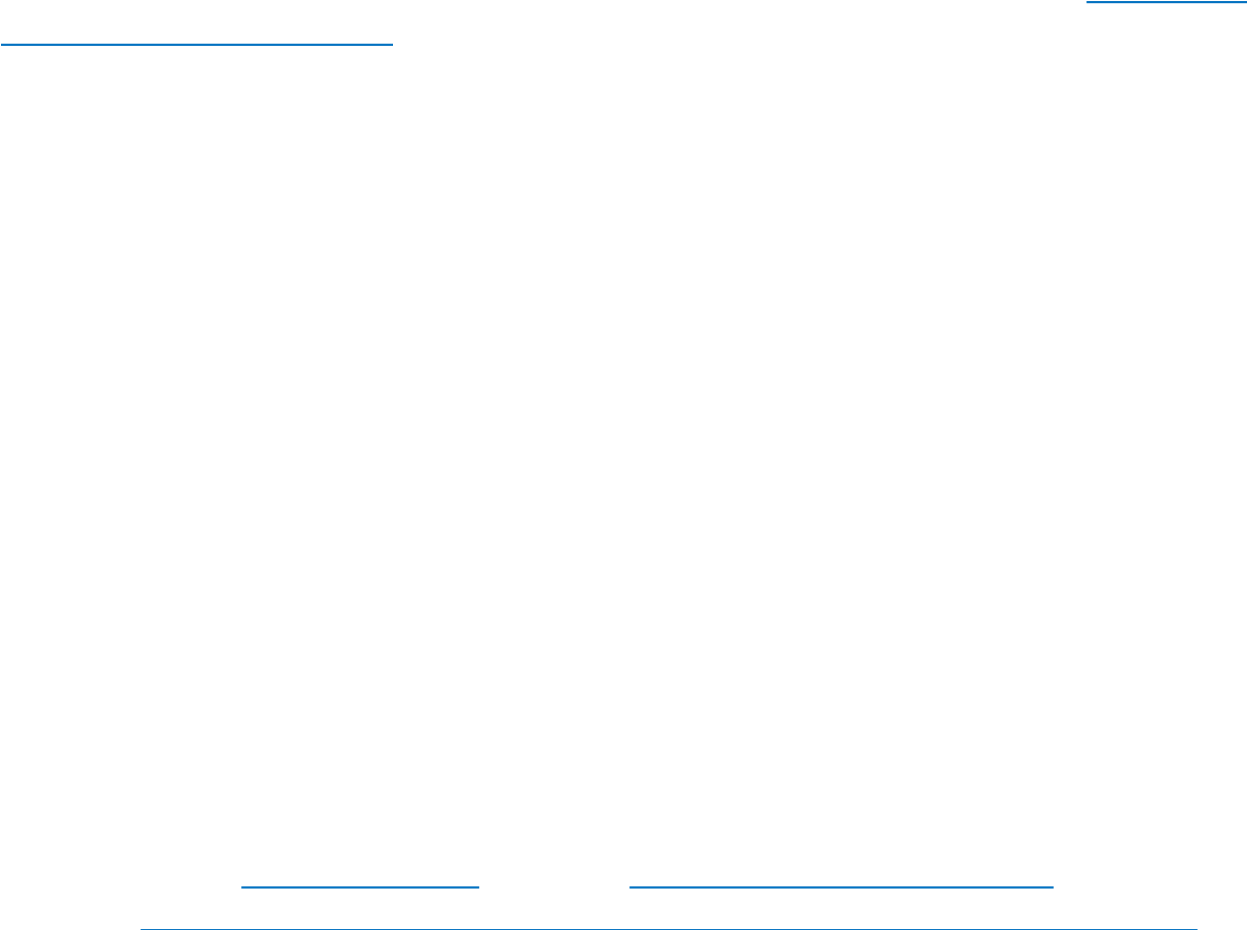
## Restriction de la divulgation

### Divulgation des rapports

Chaque trimestre, l'ICIS fournit des rapports comparatifs à tous les fournisseurs de données. Ces rapports contiennent des données agrégées permettant d'identifier un établissement grâce auxquelles les fournisseurs de données peuvent analyser leurs données au fil du temps et se comparer à d'autres fournisseurs de services semblables. Ces rapports contiennent également, pour chaque établissement, des données au niveau de l'enregistrement tirées des soumissions de l'établissement concerné.

Par mesure de sécurité, avant d'avoir accès aux rapports, l'organisme doit signer une entente de services qui comprend notamment des règles visant à

- restreindre l'utilisation de l'information à des fins non commerciales aux activités de gestion interne, d'assurance de la qualité des données, de planification, de recherche, d'analyse ou d'appui à la prise de décisions reposant sur des données probantes des clients;
- interdire la divulgation des données à des tiers, sauf s'il s'agit des données du client;
- permettre la publication de l'information uniquement lorsque toutes les mesures raisonnables ont été prises pour préserver l'identité des personnes et que les données ne contiennent pas de cellules comprenant moins de 5 observations;
-



tiers font l'objet d'un suivi et d'une surveillance de façon à garantir leur destruction sécuritaire à la fin de leur cycle de vie. Avant d'avoir accès aux données, les demandeurs tiers doivent signer une entente de protection des données et accepter de se conformer aux conditions et restrictions de l'ICIS concernant la collecte, le but, l'utilisation, la sécurité, la divulgation et le renvoi ou la destruction des données.

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

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

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

Comme indiqué à la [section 3.4](#) de la présente évaluation des incidences sur la vie privée, le SIOSM recueille des données identifiantes sur les Autochtones. La divulgation de cet identificateur est soumise à la *politique sur la diffusion et la divulgation de données identifiantes sur les Autochtones* de l'ICIS, en vertu de laquelle toute demande de données identifiant des Autochtones doit être accompagnée d'une preuve de l'approbation des autorités autochtones compétentes. Pour en savoir plus, consultez le document [Tracer la voie vers la gouvernance respectueuse des données de l'ICIS sur les Premières Nations, les Inuits et les Métis](#), et la page [Premières Nations, Inuits et Métis](#) sur le site Web de l'ICIS.

## Restriction de la conservation

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

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

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

À l'instar d'autres banques de données de l'ICIS, le SIOSM doit régulièrement faire l'objet d'une évaluation de la qualité des données fondée sur le [Cadre de la qualité de l'information de l'ICIS](#). Ce processus comprend de nombreuses activités visant à évaluer les diverses dimensions de la qualité, dont l'exactitude des données du SIOSM.

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

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

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

### Sécurité des systèmes

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



Les 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 de vérification par des tiers sont consignées dans le registre des recommandations d'action général de l'ICIS, et les mesures sont prises en conséquence.

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

L'ICIS publie de l'information concernant ses politiques sur le respect de la vie privée, ses pratiques relatives aux données et ses programmes de gestion des renseignements personnels sur la santé. Plus précisément, le [Cadre de respect de la vie privée et de sécurité](#) et la [Politique de respect de la vie privée, 2010](#) de l'ICIS sont accessibles sur son site Web ([icis.ca](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 en sa possession pour prendre des décisions administratives ou relatives aux personnes concernées. Toute personne qui souhaite accéder à ses renseignements personnels sur la santé verra sa demande traitée conformément aux articles 60 à 63 de la [Politique de respect de la vie privée, 2010](#) de l'ICIS.

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

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







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

**ICIS Ottawa**

495, chemin Richmond

Bureau 600

Ottawa (Ont.)

K2A 4H6

**613-241-7860**

**ICIS Toronto**

4110, rue Yonge

Bureau 300

Toronto (Ont.)

M2P 2B7

**416-481-2002**

**ICIS Victoria**

880, rue Douglas

Bureau 600

Victoria (C.-B.)

V8W 2B7