Système national d’information sur l’utilisation des médicaments prescrits

Évaluation des incidences sur la vie privée

Avril 2024

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

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

À moins d'indication contraire, les données utilisées proviennent des provinces et territoires du Canada.

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
droitdauteur@icis.ca

© 2024 Institut canadien d'information sur la santé

Comment citer ce document :
Institut canadien d'information sur la santé. *Système national d'information sur l'utilisation des médicaments prescrits : évaluation des incidences sur la vie privée, avril 2024*. Ottawa, ON : ICIS; 2024.

This publication is also available in English under the title *National Prescription Drug Utilization Information System Privacy Impact Assessment, April 2024*.

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 l’utilisation des médicaments prescrits : évaluation des incidences sur la vie privée, avril 2024*

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,
Bureau de la chef de la protection des renseignements personnels et des services juridiques

Ottawa, avril 2024

Table des matières

Le Système national d'information sur l'utilisation des médicaments prescrits en bref 5

1 Introduction. 6

2 Contexte 7

2.1 Présentation du SNIUMP 7

2.2 Collecte de données 7

2.3 Gestion de l'accès et cheminement des données du SNIUMP 8

3 Analyse du respect de la vie privée 11

3.1 Programme de gestion des risques liés au respect de la vie privée et à la sécurité 11

3.2 Textes législatifs régissant les données du SNIUMP 12

3.3 Premier principe : responsabilité à l'égard des renseignements personnels sur la santé 13

3.4 Deuxième principe : établissement des objectifs de la collecte de renseignements personnels sur la santé 14

3.5 Troisième principe : consentement pour la collecte, l'utilisation ou la divulgation de renseignements personnels sur la santé 15

3.6 Quatrième principe : restriction de la collecte de renseignements personnels sur la santé. 15

3.7 Cinquième principe : restriction de l'utilisation, de la divulgation et de la conservation des renseignements personnels sur la santé 16

3.8 Sixième principe : exactitude des renseignements personnels sur la santé 23

3.9 Septième principe : mesures de protection des renseignements personnels sur la santé 23

3.10 Huitième principe : transparence de la gestion des renseignements personnels sur la santé. 25

3.11 Neuvième principe : accès individuel aux renseignements personnels sur la santé et modification de ceux-ci 25

3.12 Dixième principe : plaintes concernant le traitement par l'ICIS des renseignements personnels sur la santé 26

4 Processus d'examen et de mise à jour 26

Le Système national d’information sur l’utilisation des médicaments prescrits en bref

1. Le Système national d’information sur l’utilisation des médicaments prescrits (SNIUMP) est une base de données pancanadienne de l’Institut canadien d’information sur la santé (ICIS) qui contient principalement des données sur les demandes de remboursement soumises aux régimes publics d’assurance médicaments ou consignées dans un système d’information sur les médicaments.
2. L’ICIS a entrepris d’étendre la portée du SNIUMP à tous les médicaments délivrés dans les pharmacies communautaires (y compris les demandes de remboursement payées par les régimes privés), les médicaments administrés dans les hôpitaux et les médicaments fournis par les organismes de lutte contre le cancer dans l’ensemble des provinces et territoires.
3. Le SNIUMP a été créé au début des années 2000 par l’ICIS en consultation avec le Conseil d’examen du prix des médicaments brevetés (CEPMB). Il a été conçu pour répondre aux besoins de ses fournisseurs de données, à savoir les régimes publics d’assurance médicaments fédéral, provinciaux et territoriaux. Sa portée a été élargie au fil du temps, en fonction des besoins en information des provinces et territoires. Par exemple, en 2019, le SNIUMP a commencé à recueillir des données sur les demandes de remboursement du Système de surveillance des stupéfiants et des substances contrôlées de l’Ontario.
4. Le SNIUMP contient des données sur le médicament prescrit, le patient à qui le médicament a été prescrit, le prescripteur du médicament, le fournisseur du médicament, le régime d’assurance médicaments applicable et le coût du médicament. Certaines données connexes sont aussi consignées, comme la couverture des médicaments par les régimes publics d’assurance médicaments.
5. Les données contenues dans le SNIUMP sont utilisées pour produire de l’information comparable et exploitable qui sert à orienter les décisions concernant les régimes publics d’assurance médicaments, à comparer les dépenses en médicaments et leur utilisation au fil du temps, à mesurer l’incidence des modifications de politiques sur les tendances en matière de médicaments, à relever les nouvelles pratiques de prescription et à appuyer les travaux de suivi et de surveillance axés sur l’utilisation problématique des médicaments d’ordonnance. Le SNIUMP ne recueille que les données nécessaires à ces fins.

6. L'information tirée des données du SNIUMP est accessible en différents formats. Les rapports électroniques du SNIUMP donnent aux ministères de la Santé participants, au CEPMB et à l'Agence des médicaments du Canada un accès aux données agrégées et dépersonnalisées du SNIUMP (au niveau de l'enregistrement). Des organismes tiers peuvent demander des données agrégées dépersonnalisées conformément aux modalités stipulées dans la *Politique de respect de la vie privée, 2010* de l'ICIS. Enfin, l'ICIS diffuse certaines données agrégées au public sur son site icis.ca.

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. Son mandat consiste à fournir une information comparable et exploitable qui favorise une amélioration rapide des soins de santé, de la performance des systèmes de santé et de la santé de la population dans l'ensemble du continuum de soins. L'ICIS obtient des données des hôpitaux et d'autres établissements de santé, des établissements de soins de longue durée, des autorités sanitaires régionales, des praticiens et des gouvernements. Ces données comprennent des renseignements sur les services de santé dispensés aux patients, sur les professionnels de la santé qui dispensent ces services et sur le coût des services de santé.

La présente évaluation des incidences sur la vie privée a pour but d'examiner les risques liés au respect de la vie privée, à la confidentialité et à la sécurité associés au Système national d'information sur l'utilisation des médicaments prescrits (SNIUMP). Elle remplace la version de janvier 2018 et consiste en un examen des 10 principes énoncés dans le *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation et de leur rapport avec le SNIUMP. Elle traite en outre de l'application du *Cadre de gestion des risques liés au respect de la vie privée et à la sécurité* de l'ICIS.

Cette évaluation vise avant tout le respect de la *Politique d'évaluation des incidences sur la vie privée* de l'ICIS.

Toutes les politiques mentionnées dans la présente évaluation des incidences sur la vie privée sont accessibles sur le site icis.ca.

2 Contexte

2.1 Présentation du SNIUMP

Le SNIUMP a été créé au début des années 2000 par l'ICIS en consultation avec le Conseil d'examen du prix des médicaments brevetés (CEPMB). Il a été conçu pour répondre aux besoins de ses fournisseurs de données, à savoir les régimes publics d'assurance médicaments fédéral, provinciaux et territoriaux. Le SNIUMP contient des données pancanadiennes sur les demandes de remboursement de médicaments d'ordonnance, principalement celles soumises aux régimes publics d'assurance médicaments ou consignées dans un système d'information sur les médicaments.

Sa portée a été élargie au fil du temps, en fonction des besoins en information des provinces et territoires. Par exemple, en 2019, le SNIUMP a commencé à recueillir des données sur les demandes de remboursement du Système de surveillance des stupéfiants et des substances contrôlées de l'Ontario. Il contient désormais également des données sur tous les médicaments délivrés dans les pharmacies communautaires du Manitoba, de la Saskatchewan et de la Colombie-Britannique, y compris ceux payés par les régimes publics ou privés d'assurance médicaments, ou par les particuliers.

2.2 Collecte de données

Le SNIUMP contient principalement des enregistrements sur les demandes de remboursement soumises aux régimes publics d'assurance médicaments ou consignées dans un système d'information sur les médicaments. Il recueille des enregistrements sur les demandes de remboursement de médicaments auprès des ministères de la Santé fédéral, provinciaux et territoriaux. Certains ministères de la Santé fournissent à l'ICIS des enregistrements sur les demandes de remboursement financées par le secteur public seulement. D'autres lui fournissent des données sur tous les médicaments délivrés dans les pharmacies communautaires, y compris les demandes de remboursement payées par les régimes publics et privés. S'il constate des lacunes en matière de données, l'ICIS déploie des efforts pour les combler.

Chaque enregistrement soumis au SNIUMP respecte les exigences du fichier minimal et comprend de l'information sur

- le médicament prescrit (p. ex. numéro d'identification du médicament);
- le patient à qui le médicament a été prescrit (p. ex. numéro d'assurance maladie, code postal, sexe du patient, date de naissance);
- le prescripteur du médicament (p. ex. identificateur du prescripteur, code postal);

- le fournisseur du médicament (p. ex. identificateur de la pharmacie, code postal);
- le régime d’assurance médicaments applicable (p. ex. régime qui a remboursé le coût du médicament);
- le coût du médicament (p. ex. coût des ingrédients, honoraires, coûts remboursés par le régime d’assurance médicaments, partage des coûts).

Le SNIUMP ne recueille pas d’information sur

- les médicaments prescrits, mais jamais fournis au patient;
- les médicaments qui ont été fournis au patient, mais dont les coûts n’ont pas fait l’objet d’une demande de remboursement auprès d’un régime d’assurance médicaments, et qui n’ont pas été consignés dans un système d’information sur les médicaments;
- les diagnostics des patients ou les affections à l’origine des ordonnances.

Outre des enregistrements de demandes de remboursement, le SNIUMP recueille aussi de l’information connexe pour contextualiser les demandes de remboursement de médicaments, notamment

- de l’information recueillie auprès des ministères de la Santé sur la couverture des médicaments par les régimes publics d’assurance médicaments (renseignements sur la liste des médicaments assurés);
- de l’information sur les médicaments recueillie auprès de Santé Canada.

D’autres renseignements concernant les données recueillies dans le SNIUMP sont accessibles à la page Métadonnées du SNIUMP du site Web de l’ICIS.

2.3 Gestion de l’accès et cheminement des données du SNIUMP

L’accès aux applications sécurisées de l’ICIS est régi par la section Accès et engagement des clients de l’ICIS. Cette section gère l’autorisation et la révocation de l’accès aux applications sécurisées de l’ICIS conformément aux processus établis du système de gestion de l’accès (SGA).

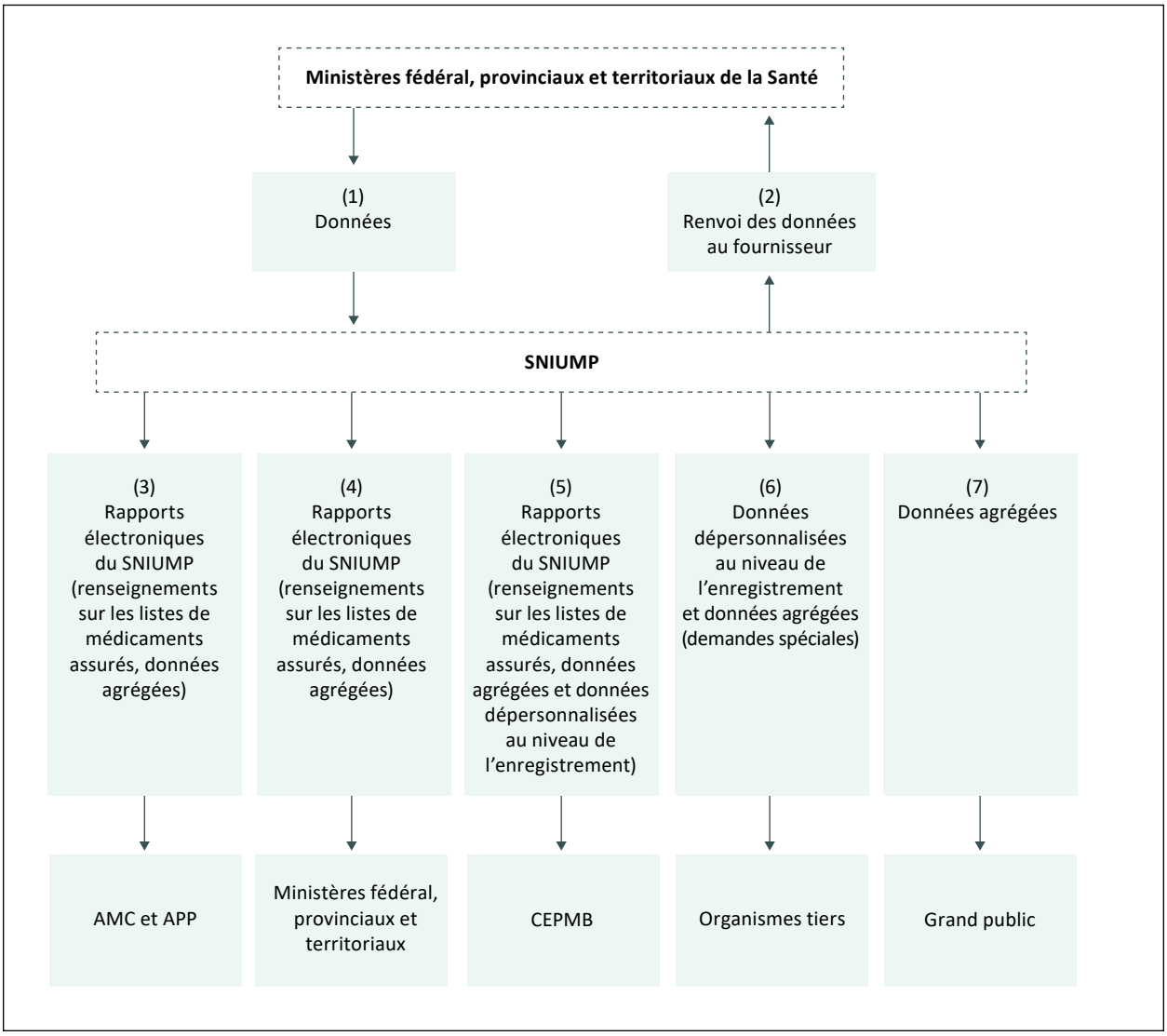
Une fois authentifiés dans le SGA de l’ICIS, les fournisseurs des données du SNIUMP soumettent à l’ICIS des données au niveau de l’enregistrement des établissements saisies électroniquement au moyen d’un logiciel spécialisé. Ils utilisent pour ce faire le Service de soumission électronique de données (eDSS) sécurisé de l’ICIS ou une application serveur à serveur.

Le cheminement des données du SNIUMP sur les demandes de remboursement va comme suit :

1. Les ministères de la Santé fédéral, provinciaux et territoriaux soumettent les données au SNIUMP. Plus précisément, les ministères de la Santé envoient des enregistrements sur les demandes de remboursement soumises aux régimes publics d'assurance médicaments ou consignées dans un système d'information sur les médicaments.
2. Une copie des enregistrements tels qu'ils ont été acceptés par le SNIUMP ainsi que certains rapports qui comprennent des renseignements personnels sur la santé sont mis à la disposition du ministère de la Santé qui a soumis les données à l'ICIS.
3. L'ICIS fournit, au moyen des rapports électroniques du SNIUMP, des renseignements sur les listes de médicaments assurés et des données agrégées à l'Agence des médicaments du Canada (AMC) et à l'Alliance pharmaceutique pancanadienne (APP).
4. L'ICIS fournit, au moyen des rapports électroniques du SNIUMP, des renseignements sur les listes de médicaments assurés et des données agrégées aux ministères de la Santé qui soumettent des données au SNIUMP.
5. L'ICIS fournit, au moyen des rapports électroniques du SNIUMP, des renseignements sur les listes de médicaments assurés ainsi que des données dépersonnalisées au niveau de l'enregistrement et des données agrégées au Conseil d'examen du prix des médicaments brevetés (CEPMB).
6. L'ICIS divulgue des données dépersonnalisées au niveau de l'enregistrement et des données agrégées du SNIUMP aux tiers qui en font la demande, conformément à sa *Politique de respect de la vie privée*.
7. L'ICIS diffuse des données agrégées du SNIUMP au public.

La figure ci-dessous illustre le cheminement des données du SNIUMP.

Figure Cheminement des données du SNIUMP



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. L'ICIS a mis en œuvre son *Cadre de gestion des risques liés au respect de la vie privée et à la sécurité* et 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 avocate générale, ainsi que 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 susceptibles d'avoir une incidence sur les principes décrits aux sections 3.3 à 3.12.

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. La cote de niveau de risque (faible, moyen ou élevé) définit le degré de risque. Une cote de niveau de risque élevé est signe d'une menace grave qu'il est impératif de prendre immédiatement en charge. Une fois le risque initial pris en charge, le risque résiduel (nouveau calcul de la probabilité et de l'incidence du risque par suite du traitement) est évalué en fonction de l'énoncé sur la tolérance à l'égard 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 faible, ou jusqu'à ce que le risque résiduel ou non pris en charge soit accepté par le Comité exécutif de l'ICIS au nom de l'organisme.

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

3.2 Textes législatifs régissant les données du SNIUMP

Généralités

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

Lois sur la protection de la vie privée

L'ICIS est un collecteur secondaire de données sur la santé, particulièrement à des fins de planification et de gestion des systèmes de santé du Canada, ce qui comprend l'analyse statistique et la production de rapports. Il incombe aux fournisseurs de données de respecter les obligations légales de leur autorité compétente, selon le cas, au moment de la collecte des données.

Les provinces et territoires suivants disposent de lois sur la protection des renseignements personnels sur la santé : Terre-Neuve-et-Labrador, Île-du-Prince-Édouard, Nouvelle-Écosse, Nouveau-Brunswick, Ontario, Manitoba, Saskatchewan, Alberta, Yukon et Territoires du Nord-Ouest. 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, sous réserve de certaines conditions. Par exemple, l'ICIS étant 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 le paragraphe 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

À l'ICIS, les données du SNIUMP sont régies par la *Politique de respect de la vie privée, 2010*, la législation en vigueur dans les autorités compétentes et les ententes de partage de données conclues avec les provinces et territoires. Les ententes de partage des données établissent les critères relatifs au but, à l'utilisation, à la conservation et à la destruction des renseignements personnels sur la santé fournis à l'ICIS, ainsi que toute divulgation subséquemment permise. Les ententes décrivent aussi l'autorité législative en vertu de 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, de même qu'un comité de gouvernance et de respect de la vie privée issu du Conseil d'administration.

Organisation et gouvernance

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

Tableau Principaux postes et responsabilités

Poste et groupe	Rôles et responsabilités
Vice-président, Stratégies de données et Statistiques	Responsable de l'orientation stratégique générale du SNIUMP
Directrice, Pharmaceutique	Responsable du fonctionnement général du SNIUMP et des décisions administratives stratégiques connexes
Chef de la sécurité de l'information	Responsable de l'orientation stratégique et de la mise en œuvre générale du programme de sécurité de l'information de l'ICIS
Chef de la protection des renseignements personnels et avocate générale	Responsable de l'orientation stratégique et de la mise en œuvre générale du programme de respect de la vie privée de l'ICIS

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

L’ICIS 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 des soins. L’organisme produit notamment de l’information servant à

- orienter la prise de décisions relatives aux régimes d’assurance médicaments;
- comparer les dépenses en médicaments et leur utilisation au fil du temps;
- mesurer l’incidence des modifications de politiques sur les tendances en matière de médicaments;
- relever les nouvelles pratiques de prescription;
- appuyer les travaux de suivi et de surveillance axés sur l’utilisation problématique des médicaments d’ordonnance.

Pour ce faire, l’ICIS recueille les types de données suivants dans le SNIUMP aux fins indiquées.

Identificateurs personnels du patient

Il peut s’agir, par exemple, du numéro d’assurance maladie ou du numéro d’assurance maladie chiffré par l’autorité compétente. 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 jumeler les enregistrements, l’ICIS doit savoir lesquels se rapportent à la personne. Pour cette raison, tous les enregistrements doivent inclure des identificateurs.

Caractéristiques démographiques du patient

Il peut s’agir, par exemple, de la date de naissance, du code postal, du sexe ou des identificateurs de statut autochtone. L’ICIS utilise l’âge calculé à partir de la date de naissance, l’information géographique dérivée du code postal, le sexe et les identificateurs de statut autochtone pour réaliser des analyses démographiques des services de santé fournis et de leurs résultats.

Identificateurs de l’établissement de santé

Il peut s’agir, par exemple, du numéro attribué à la pharmacie qui a délivré le médicament ou de son code postal. L’ICIS utilise ces informations pour comparer les établissements et les groupes d’établissements.

Identificateurs du fournisseur de services de santé

Il peut s’agir, par exemple, du numéro attribué au prescripteur ou du code postal du lieu d’exercice du prescripteur. L’ICIS utilise ces informations pour déterminer les types de ressources humaines ayant contribué aux soins.

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 assument leurs responsabilités en matière de collecte, d’utilisation et de divulgation de données, y compris en ce qui concerne le consentement et les avis, comme le prévoient les lois, les règlements et les politiques en vigueur dans les provinces et territoires.

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

L’ICIS souscrit au principe de la minimisation des données. En vertu des articles 1 et 2 de sa *Politique de respect de la vie privée, 2010*, l’ICIS ne recueille des fournisseurs de données que les renseignements raisonnablement nécessaires pour les besoins des systèmes 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.

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 des données du SNIUMP aux objectifs autorisés décrits à la section 3.4. Ceux-ci comprennent les analyses comparatives dans et entre les provinces et territoires, les analyses des tendances visant à évaluer et à surveiller l’incidence des différences de politiques, de pratiques et de prestation de services, ainsi que la production de statistiques pour appuyer la planification, la gestion et l’amélioration de la qualité.

Personnel de l’ICIS

Le personnel de l’ICIS est autorisé à accéder aux données et à les utiliser uniquement en cas de nécessité, notamment pour la gestion du traitement et de la qualité des données, la production de statistiques et de fichiers de données, ainsi que la réalisation d’analyses. Tous les membres du personnel de l’ICIS doivent signer une entente de confidentialité au moment de leur embauche, et sont ensuite tenus de renouveler chaque année leur engagement à l’égard du respect de la vie privée.

L’accès du personnel à l’environnement analytique sécurisé de l’ICIS est fourni au moyen du processus centralisé d’accès aux données de l’ICIS. Cet environnement offre un espace distinct et sécurisé pour le stockage des fichiers de données analytiques, où le personnel doit effectuer ses analyses et en stocker les résultats.

Les fichiers de données du SNIUMP utilisés pour les analyses internes de l’ICIS ne comprennent aucun identificateur direct (p. ex. date de naissance, code postal complet, numéro d’assurance maladie non chiffré). Ils contiennent plutôt l’âge, le numéro d’assurance maladie chiffré et le nom de la province ou du territoire. Le personnel autorisé de l’ICIS a accès à de l’information contenant des identificateurs directs de façon exceptionnelle, uniquement en cas de nécessité. Cet accès est assujetti aux processus internes d’approbation, comme précisé dans les procédures et la politique de respect de la vie privée, 2010 de l’ICIS.

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

Couplage des données

Les données du SNIUMP sont couplées avec les données d'autres sources de l'ICIS. Comme le couplage des données peut accroître les risques d'identification d'une 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 entre de multiples banques de données pour l'usage exclusif de l'ICIS et toutes les demandes de couplage de données formulées par des tiers sont soumis à un processus interne d'examen et d'approbation. Lors du couplage, l'ICIS utilise généralement des numéros d'assurance maladie chiffrés. Les données couplées demeurent assujetties aux dispositions en matière d'utilisation et de divulgation de la *Politique de respect de la vie privée, 2010*.

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

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

Article 24 Tous les critères suivants sont respectés :

a) l'objectif du couplage de données s'inscrit dans le mandat de l'ICIS;
b) les avantages pour le public sont considérablement plus importants que les risques de violation de la vie privée des personnes;
c) les résultats du couplage de données ne porteront pas préjudice aux personnes concernées;
d) le couplage de données s'inscrit dans un projet précis et ponctuel, et les données couplées seront par la suite détruites dans le respect des règles énoncées aux articles 28 et 29;

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

Norme de couplage de données sur les clients

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

Destruction des données couplées

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

Pour certains projets ponctuels, l'article 29 de la *Politique de respect de la vie privée, 2010* de l'ICIS prévoit par ailleurs que la destruction sécuritaire des données couplées aura lieu dans l'année suivant la publication de l'analyse ou dans les 3 années suivant le couplage, selon la première éventualité, conformément à la norme de destruction 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.

Renvoi des données au fournisseur

Bien que les ministères de la Santé ne demandent habituellement pas le renvoi des enregistrements soumis au SNIUMP, l'article 34 de la *Politique de respect de la vie privée, 2010* stipule que l'ICIS peut remettre les enregistrements au fournisseur de données (c.-à-d. au ministère de la Santé concerné) ou tel qu'il est indiqué dans l'entente de partage des données ou un autre instrument juridique. Le renvoi des données au fournisseur de données est considéré comme une utilisation et non comme une divulgation.

Restriction de la divulgation

Rapports électroniques du SNIUMP

Les rapports électroniques du SNIUMP sont accessibles dans une application en ligne sécurisée qui, selon le niveau d'accès accordé par l'ICIS, fournit

- de l'information sur les listes de médicaments assurés (c.-à-d. renseignements contextuels comparables associés aux politiques administratives des programmes et des régimes publics d'assurance médicaments des gouvernements fédéral, provinciaux et territoriaux);
- des données agrégées provenant du SNIUMP;
- des données dépersonnalisées au niveau de l'enregistrement provenant du SNIUMP.

L'utilisateur peut produire des rapports sur l'utilisation des médicaments, leur coût et leur couverture par les régimes d'assurance médicaments. Les rapports électroniques du SNIUMP permettent à l'utilisateur de personnaliser les rapports en sélectionnant certains intrants et extrants.

Avant d'obtenir l'accès aux rapports électroniques du SNIUMP, l'organisme doit signer l'Entente de services de rapports électroniques de l'ICIS, laquelle, notamment,

- restreint l'utilisation de l'information à des fins non commerciales aux activités des clients touchant la gestion interne, l'assurance de la qualité des données, la planification, la recherche, l'analyse ou l'appui à la prise de décisions reposant sur des données probantes;
- interdit la divulgation des données à des tiers, sauf s'il s'agit des données du client;
- permet 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;
- interdit la publication de renseignements permettant d'identifier un établissement ou organisme de santé, à moins que l'utilisateur en informe préalablement l'ICIS afin de lui permettre d'aviser le ministère de la Santé concerné.

En vertu de l'Entente de services de rapports électroniques, chaque organisme doit mandater une personne-ressource à l'interne pour désigner les utilisateurs autorisés de l'organisme, lesquels pourront ensuite accéder aux rapports électroniques du SNIUMP, conformément à l'entente de services.

Les rapports électroniques du SNIUMP font partie des services et des applications à accès restreint de l'ICIS. L'utilisateur doit accepter les conditions d'accès et d'utilisation propres aux systèmes et applications des Services à la clientèle de l'ICIS chaque fois qu'il souhaite accéder à ces services à accès restreint. Il doit non seulement accepter les conditions

générales (p. ex. mesures de sécurité relatives au nom d'utilisateur et au mot de passe), mais également les conditions afférentes aux applications de déclaration électronique de l'ICIS, dont les rapports électroniques du SNIUMP (p. ex. « vous devez accéder aux services et les utiliser conformément aux dispositions de l'Entente de services »).

Accès des fournisseurs de données participants

L'ICIS fournit, au moyen des rapports électroniques du SNIUMP, des renseignements sur les listes de médicaments assurés et des données agrégées du SNIUMP aux ministères de la Santé fédéral, provinciaux et territoriaux participants.

L'accès de chaque ministère de la Santé à ces rapports est régi par les conditions d'accès et d'utilisation des systèmes et applications des Services à la clientèle et par l'Entente de services de rapports électroniques de l'ICIS décrites ci-dessus.

Accès de l'Agence des médicaments du Canada (AMC) et de l'Alliance pharmaceutique pancanadienne (APP)

L'ICIS fournit, au moyen des rapports électroniques du SNIUMP, des renseignements sur les listes de médicaments assurés et des données agrégées du SNIUMP à l'AMC et à l'APP.

L'accès de chaque organisme à ces rapports est régi par les conditions d'accès et d'utilisation des systèmes et applications des Services à la clientèle et par l'Entente de services de rapports électroniques de l'ICIS décrites ci-dessus.

Accès du Conseil d'examen du prix des médicaments brevetés (CEPMB)

L'ICIS fournit, au moyen des rapports électroniques du SNIUMP, des renseignements sur les listes de médicaments assurés ainsi que des données agrégées et des données dépersonnalisées au niveau de l'enregistrement au CEPMB, afin que ce dernier puisse effectuer des analyses complexes de données dans le cadre du mandat qui lui a été confié par le ministre fédéral de l'Industrie en vertu de la *Loi sur les brevets*.

L'accès du CEPMB à ces rapports est régi par les conditions d'accès et d'utilisation des systèmes et applications des Services à la clientèle de l'ICIS. Il est également régi par une Entente de services de rapports électroniques qui, en plus des dispositions habituelles décrites ci-dessus, comprend des dispositions supplémentaires visant à protéger les données dépersonnalisées au niveau de l'enregistrement auxquelles le CEPMB accède.

Demandes de données formulées par des tiers

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

L'ICIS administre le programme de demandes de données par des tiers, qui établit les mesures de contrôle de respect de la vie privée et de la sécurité que l'organisme demandeur doit respecter. En outre, comme le stipulent les articles 37 à 57 de sa *Politique de respect de la vie privée, 2010*, l'ICIS divulgue des renseignements sur la santé conformément à son mandat et à ses fonctions de base, et s'efforce de divulguer les données dans le plus grand anonymat possible tout en répondant aux exigences de recherche ou d'analyse du demandeur. Les données sont donc agrégées dans la mesure du possible. Si les données agrégées ne sont pas suffisamment détaillées pour les fins visées, l'ICIS peut décider, au cas par cas, de divulguer au destinataire des données dépersonnalisées au niveau de l'enregistrement ou des renseignements personnels sur la santé (dans des circonstances particulières, par exemple, avec le consentement de la personne). Le destinataire doit avoir signé au préalable une entente de protection des données ou un autre instrument juridiquement contraignant avec l'ICIS. Seuls les éléments de données nécessaires aux fins visées seront divulgués.

L'ICIS offre aux demandeurs de données tiers un environnement d'accès sécurisé (EAS) comme moyen d'accès privilégié aux données au niveau de l'enregistrement. L'EAS est distinct de l'environnement analytique sécurisé à l'intention du personnel de l'ICIS, comme indiqué à la section 3.7. L'EAS est un environnement chiffré et sécurisé hébergé dans le centre des données de l'ICIS. Conformément aux politiques et procédures en vigueur à l'ICIS, les chercheurs autorisés — qui sont liés par de rigoureuses conditions d'utilisation — ont accès à des données extraites, préparées et vérifiées par des membres du personnel de l'ICIS pour un projet de recherche approuvé. Les données au niveau de l'enregistrement ne peuvent pas être copiées ni extraites de l'EAS; seuls des résultats agrégés peuvent être extraits de l'EAS. De plus amples renseignements sur l'EAS sont disponibles sur le site icis.ca à la page Faire une demande de données et dans le document *Évaluation des incidences sur la vie privée de l'environnement d'accès sécurisé*.

L'ICIS a adopté une approche de gestion axée sur le cycle de vie pour les données au niveau de l'enregistrement extraites dans des fichiers transmis aux chercheurs et aux autres utilisateurs autorisés. Le Secrétariat à la vie privée et aux services juridiques a élaboré et gère un processus de surveillance continue de la conformité qui fait partie intégrante de ce cycle de vie. Dans le cadre de ce processus, tous les fichiers de données qui sont divulgués à des demandeurs tiers font l'objet d'un suivi et d'une surveillance de façon à garantir leur destruction sécuritaire à la fin de leur cycle de vie. Avant d'avoir accès aux données, les demandeurs tiers doivent signer une entente de protection des données et accepter de se conformer aux conditions et restrictions de l'ICIS concernant la collecte, le but, l'utilisation, la sécurité, la divulgation et le renvoi ou la destruction des données.

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

- des exigences de destruction sécuritaire;
- le droit de l'ICIS 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, le SNIUMP recueille des identificateurs de statut autochtone. La divulgation de ces données est soumise à la politique de l'ICIS sur la diffusion et la divulgation de données identificatoires sur les Autochtones, en vertu de laquelle toute demande de données identifiant des Autochtones doit être accompagnée d'une preuve de l'approbation des autorités autochtones compétentes. Pour en savoir plus, consultez le document *Tracer la voie vers la gouvernance respectueuse des données de l'ICIS sur les Premières Nations, les Inuits et les Métis*.

Diffusion publique

Dans le cadre de son mandat, l'ICIS publie uniquement des données agrégées en s'assurant de réduire au minimum le risque d'identification et de divulgation par recoupements. En général, il faut au moins 5 observations par cellule conformément à l'article 33 de la *Politique de respect de la vie privée, 2010* de l'ICIS. Des statistiques agrégées et des analyses sont diffusées dans des publications et sur le site icis.ca au moyen d'outils comme Votre système de santé (p. ex. le rapport *Dépenses en médicaments prescrits au Canada*, le rapport *Utilisation des médicaments chez les personnes âgées au Canada*, l'indicateur Médicaments potentiellement contre-indiqués prescrits aux personnes âgées).

Restriction de la conservation

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

3.8 Sixième principe : exactitude des renseignements personnels sur la santé

L'ICIS dispose d'un vaste programme 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 des autres banques de données de l'ICIS, le SNIUMP fait régulièrement 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 SNIUMP.

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

Le *Cadre de respect de la vie privée et de sécurité* de l'ICIS offre 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 SNIUMP.

Sécurité des systèmes

L'ICIS reconnaît que l'information peut être considérée comme sécurisée uniquement 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 d'un ensemble exhaustif de politiques qui définissent les contrôles nécessaires pour garantir la protection de l'information en format

physique et électronique, y compris des mesures rigoureuses de chiffrement et d'élimination. Ces politiques ainsi que les normes, lignes directrices et procédures opérationnelles qui s'y rattachent sont conformes aux pratiques exemplaires en matière de respect de la vie privée, de sécurité de l'information et de gestion des enregistrements, afin de garantir la confidentialité, l'intégrité et la disponibilité des actifs informationnels de l'ICIS.

Les registres de contrôle et de vérification des systèmes 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 à risque réduit au niveau de l'enregistrement (où le numéro d'assurance maladie a été chiffré) pour réaliser ses analyses. Il arrive dans des circonstances exceptionnelles que le personnel doive avoir accès aux numéros d'assurance maladie d'origine. Les procédures et la politique de respect de la vie privée, 2010 de l'ICIS prévoient des contrôles stricts qui garantissent que l'accès est autorisé dans les circonstances et au niveau appropriés, et que le principe de minimisation des données est respecté en tout temps. L'ICIS consigne dans ses registres les activités suivantes ayant trait à l'accès aux données :

- l'accès aux numéros d'assurance maladie et aux noms des patients (rarement recueillis) dans les bases de données de production de l'ICIS;
- l'accès aux fichiers de données contenant des renseignements personnels sur la santé qui sont extraits des bases de données de production de l'ICIS et mis à la disposition des analystes internes dans des circonstances exceptionnelles;
- la modification des privilèges d'accès dans les bases de données de production.

Les employés de l'ICIS sont sensibilisés à l'importance de maintenir la confidentialité des renseignements personnels sur la santé et d'autres types d'information sensible au moyen d'un programme de formation obligatoire sur le respect de la vie privée et la sécurité, et par l'intermédiaire de communications continues concernant les politiques et procédures de l'ICIS à ce sujet. Avant chaque tentative de connexion à un système d'information de l'ICIS, les employés doivent confirmer qu'ils comprennent l'interdiction d'accéder à ce système informatique ou de l'utiliser sans autorisation 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 évaluer la conformité à 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 par rapport 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 les conditions 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 régulièrement par des tiers, constituent une composante importante du programme de vérification de l'ICIS. Toutes les recommandations issues de vérifications par des tiers sont consignées dans le registre des recommandations du plan d'action général de l'ICIS, et des mesures sont prises en conséquence.

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

L'ICIS publie des informations concernant ses politiques de protection de la vie privée, ses pratiques en matière de traitement des données et ses programmes de gestion des renseignements personnels sur la santé. Plus précisément, le *Cadre de respect de la vie privée et de sécurité* et la *Politique de respect de la vie privée, 2010* de l'ICIS sont accessibles au 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 le stipulent 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 et avocate générale, qui peut acheminer une demande ou une plainte au commissaire à l’information et à la protection de la vie privée de la province ou du territoire de l’auteur de la demande ou de la plainte.

4 Processus d’examen et de mise à jour

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

aide@icis.ca

ICIS Ottawa
495, chemin Richmond
Bureau 600
Ottawa (Ont.)
K2A 4H6
613-241-7860

ICIS Toronto
4110, rue Yonge
Bureau 300
Toronto (Ont.)
M2P 2B7
416-481-2002

ICIS Victoria
880, rue Douglas
Bureau 600
Victoria (C.-B.)
V8W 2B7
250-220-4100

ICIS Montréal
1010, rue Sherbrooke Ouest
Bureau 511
Montréal (Qc)
H3A 2R7
514-842-2226

icis.ca

51238-0724