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

Évaluation des incidences sur la vie privée

Janvier 2018

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

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

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

Institut canadien d'information sur la santé
495, chemin Richmond, bureau 600
Ottawa (Ontario) K2A 4H6
Téléphone : 613-241-7860
Télécopieur : 613-241-8120
www.icis.ca
droitdauteur@icis.ca

This publication is also available in English under the title *National Prescription Drug Utilization Information System: Privacy Impact Assessment, January 2018*.

Canadian Institute for Health Information

Institut canadien d'information sur la santé

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

Évaluation des incidences sur la vie privée

Approuvé par :

Brent Diverty
Vice-président, Programmes

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

Ottawa – janvier 2018

Table des matières

Faits saillants sur l'ICIS et le Système national d'information sur l'utilisation des médicaments prescrits

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 recueille des données sur les demandes de remboursement soumises aux régimes publics d'assurance médicaments ou consignées dans un système d'information sur les médicaments. L'ICIS travaille à la collecte de données sur tous les médicaments délivrés dans les pharmacies communautaires, y compris les demandes de remboursement payées par les régimes publics et privés, dans l'ensemble des provinces et territoires.

2. 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.

3. Le SNIUMP recueille 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.

4. Les données contenues dans le SNIUMP sont utilisées pour produire de l'information exacte, actuelle et comparable. Cette information sert ensuite 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.

5. L'information tirée des données du SNIUMP est accessible en différents formats. Les rapports électroniques du SNIUMP donnent aux ministères de la Santé participants un accès aux données agrégées du SNIUMP et permettent au CEPMB de consulter les données agrégées et dépersonnalisées du SNIUMP (au niveau de l'enregistrement). Des tiers peuvent demander des données agrégées ou dépersonnalisées conformément aux règles stipulées dans la Politique de respect de la vie privée, 2010 de l'ICIS. Enfin, l'ICIS divulgue certaines données agrégées au public.

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 dispensent ces services et sur le coût des services de santé.

La présente évaluation des incidences sur la vie privée a pour objet d'examiner les risques de violation de la vie privée, de la confidentialité et de la sécurité associés au SNIUMP. Elle remplace la version de 2011 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, tels qu'ils s'appliquent au SNIUMP, et 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 repose surtout sur le respect de la Politique : Évaluation des incidences sur la vie privée de l'ICIS.

2 Contexte

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 renferme des données pancanadiennes sur les demandes de remboursement de médicaments d'ordonnance. Axé principalement sur les régimes publics d'assurance médicaments, le SNIUMP recueille diverses données afin de produire de l'information exacte, actuelle et comparable servant à

- gérer et orienter les 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.

Information recueillie par le SNIUMP

Le SNIUMP recueille des enregistrements sur les demandes de remboursement soumises aux régimes publics d'assurance médicaments ou consignées dans un système d'information sur les médicaments. Ces enregistrements comprennent de l'information sur

- le médicament prescrit (p. ex. le 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.

Un dictionnaire de données contenant des renseignements détaillés sur les enregistrements recueillis par le SNIUMP est accessible au icis.ca.

Fournisseurs de données

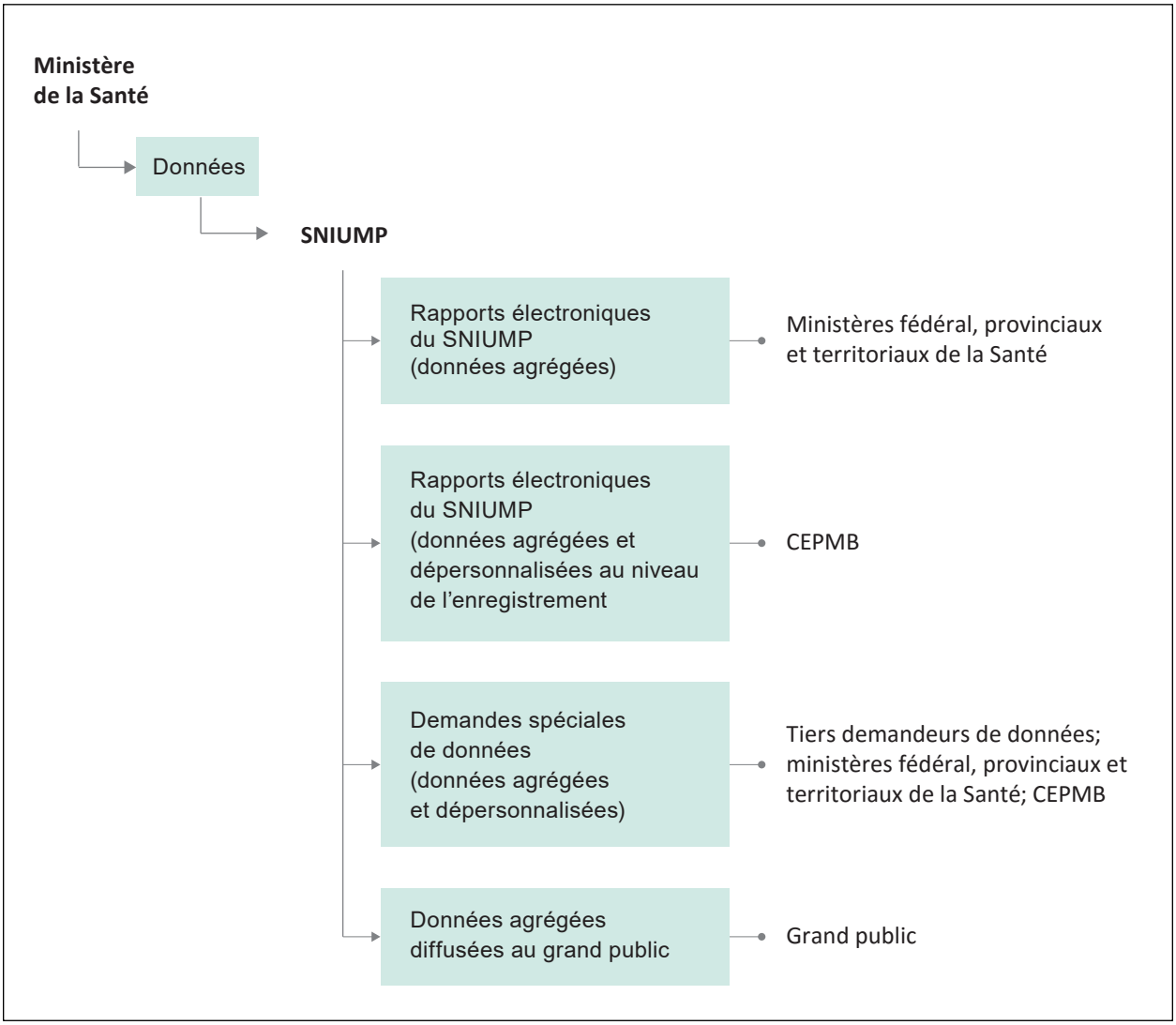
Le SNIUMP recueille des enregistrements sur les demandes de remboursement de médicaments auprès des ministères fédéral, provinciaux et territoriaux de la Santé. Certains ministères fournissent à l'ICIS des enregistrements sur les demandes de remboursement financées par le secteur public seulement. D'autres ministères 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. L'ICIS recueille des données auprès des secteurs public et privé dans l'ensemble des provinces et des territoires.

Acheminement des données

Les ministères soumettent les enregistrements à l'ICIS par l'entremise des applications Web ou de l'application serveur à serveur de l'ICIS.

La figure ci-dessous illustre le cheminement des données du SNIUMP, qui sera abordé plus en profondeur dans la présente évaluation des incidences sur la vie privée.

Figure Cheminement des données du SNIUMP



Information connexe recueillie par le SNIUMP

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.

3 Analyse du respect de la vie privée

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

La gestion des risques liés au respect de la vie privée et à la sécurité est un processus officiel et reproductible qui vise la détection, l'évaluation, la prise en charge et la surveillance des risques dans le but de réduire au minimum la probabilité qu'ils se matérialisent ou leur éventuelle incidence. En 2015, l'ICIS a approuvé son *Cadre de gestion des risques liés au respect de la vie privée et à la sécurité*, puis mis en œuvre un document connexe, à savoir la *Politique sur la gestion des risques liés au respect de la vie privée et à la sécurité*. La chef de la protection des renseignements personnels et le chef de la sécurité de l'information de l'ICIS, de concert avec les cadres supérieurs de l'ICIS, sont responsables de la détection, de l'évaluation, de la prise en charge ainsi que de la surveillance et de l'examen des risques liés au respect de la vie privée et à la 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 saisis dans le registre des risques liés au respect de la vie privée et à la sécurité, puis classés en fonction de leur probabilité et de leur incidence (risque **élevé**, **modéré** ou **faible**).

- **Risque élevé :** il est fort probable que le risque se produise, ou les mesures de contrôle et les stratégies qui ont été mises en place ne sont ni fiables ni efficaces.
- **Risque modéré :** il est modérément probable que le risque se produise, ou les mesures de contrôle et les stratégies qui ont été mises en place sont relativement fiables et efficaces.
- **Risque faible :** il est peu probable que le risque se produise, ou les mesures de contrôle et les stratégies qui ont été mises en place sont fiables et efficaces.

La probabilité et l'incidence du risque détecté permettent d'attribuer une cote (risque faible, modéré ou élevé) à ce risque et d'en déterminer la gravité. Un risque classé comme étant élevé est signe d'une menace grave qu'il est impératif de prendre immédiatement en charge. Une fois la prise en charge initiale effectuée, le risque résiduel (dont la probabilité et l'incidence sont calculées à nouveau à la suite de la prise en charge) est évalué puis comparé à 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 indique que le degré de tolérance de l'organisme à de tels risques est faible. Si la cote du risque résiduel demeure plus élevée que faible, de nouvelles mesures de prise en charge du risque doivent être mises en œuvre jusqu'à l'obtention d'une cote de risque faible, ou jusqu'à ce que le risque non pris en charge ou résiduel soit accepté par le Comité de la haute direction au nom de l'organisme.

3.2 Textes législatifs régissant les enregistrements du SNIUMP

Généralités

L'ICIS se conforme à sa Politique de respect de la vie privée, 2010 et à toute législation ou entente en vigueur.

Législation

L'ICIS est un collecteur secondaire de données sur la santé, 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 de leur territoire, le cas échéant, au moment de la collecte des données.

Terre-Neuve-et-Labrador, l'Île-du-Prince-Édouard, la Nouvelle-Écosse, le Nouveau-Brunswick, l'Ontario, le Manitoba, la Saskatchewan, l'Alberta, le Yukon et les Territoires du Nord-Ouest disposent de lois sur la protection des renseignements personnels sur la santé. Ces lois octroient aux établissements l'autorisation de divulguer des renseignements personnels sur la santé sans le consentement du patient, pour les besoins du système de santé et sous certaines conditions. L'ICIS est par exemple 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 de l'Ontario peuvent divulguer des renseignements personnels sur la santé à l'ICIS sans le consentement du patient en vertu de l'article 29, comme le prévoit l'article 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 enregistrements du SNIUMP sont régis par la Politique de respect de la vie privée, 2010 de l'ICIS, la législation en vigueur dans les provinces et territoires et les ententes de partage des données déjà mises en place avec les provinces et les 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 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 du respect de la Politique de respect de la vie privée, 2010 de l'ICIS. À cet égard, l'ICIS compte sur un chef de la protection des renseignements personnels et avocat général, 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 dont les titulaires sont responsables de la gestion des risques liés au respect de la vie privée et à la sécurité pour le SNIUMP :

Tableau Principaux postes et responsabilités

Poste/groupe	Responsabilités
Vice-président, Programmes	Orientation stratégique du SNIUMP
Directeur, Services d'information sur les produits pharmaceutiques et la main-d'œuvre de la santé	Développement stratégique et opérationnel du SNIUMP
Gestionnaire, Pharmaceutique	Développement et fonctionnement du SNIUMP
Groupe consultatif du SNIUMP	Conseils sur l'amélioration de la base de données, la qualité des données, l'élaboration des rapports et les sujets et méthodes d'analyse
Chef de la sécurité de l'information	Orientation stratégique et mise en œuvre du programme de sécurité de l'information de l'ICIS
Chef de la protection des renseignements personnels	Orientation stratégique et mise en œuvre du programme de respect de la vie privée de l'ICIS
Gestionnaire, Applications de gestion de l'information sur la santé, STI	Assurer la disponibilité des ressources et solutions techniques nécessaires à l'exploitation et à l'amélioration continues du SNIUMP
Gestionnaire, Services centraux à la clientèle	Gérer l'accès aux applications Web d'échange de données du SNIUMP

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

Les enregistrements du SNIUMP se rapportent à des personnes et indiquent les médicaments qui leur sont prescrits. Ces enregistrements sont donc considérés comme des renseignements personnels sur la santé.

Les enregistrements du SNIUMP identifient aussi des membres de la main-d'œuvre en santé (p. ex. les médecins qui prescrivent des médicaments). La Politique de respect de la vie privée des travailleurs de la santé de l'ICIS stipule que pour toute activité de l'ICIS liée à des renseignements personnels sur la santé, la Politique de respect de la vie privée, 2010 de l'ICIS a préséance sur sa *Politique de respect de la vie privée des travailleurs de la santé.*

Comme les enregistrements du SNIUMP sont des renseignements personnels sur la santé, ils sont traités et protégés comme tels conformément à la Politique de respect de la vie privée, 2010 de l'ICIS.

Le SNIUMP recueille des renseignements personnels sur la santé parce qu'ils sont nécessaires à l'atteinte des objectifs de sa base de données, notamment pour produire de l'information exacte, actuelle et comparable sur les médicaments, comme il est décrit à la section 2.

L'information tirée des données du SNIUMP est accessible sous différents formats à un éventail d'intervenants, comme il est décrit à la section Restriction de la divulgation au point 3.7.

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 s'engage à respecter le principe de la minimisation des données. Conformément aux articles 1 et 2 de sa Politique de respect de la vie privée, 2010, l'ICIS ne recueille des fournisseurs de données que les renseignements raisonnablement nécessaires pour les besoins du système de santé, dont l'analyse statistique et la production de rapports, à des fins de gestion, d'évaluation et de surveillance des systèmes de santé. Le SNIUMP ne recueille que les éléments de données que l'ICIS et ses intervenants (p. ex. le Groupe consultatif sur la base de données du SNIUMP) jugent nécessaires à l'atteinte des objectifs de la base de données.

Bien que les enregistrements du SNIUMP ne contiennent pas le nom et l'adresse des patients, ils comprennent d'autres identificateurs des patients tels que le numéro d'assurance maladie, le sexe et la date de naissance. En ce qui a trait à ces données, chaque ministère de la Santé décide s'il envoie

- le numéro d'assurance maladie chiffré ou non chiffré;
- l'année de naissance du patient ou sa date de naissance complète;
- le code postal du patient.

Les ministères de la Santé déterminent l'information que les enregistrements sur les médicaments contiennent pour identifier les prescripteurs et les fournisseurs, puis soumettent l'identificateur et le code postal de chaque prescripteur et de chaque pharmacie, comme il est décrit à la section 2.

L'ICIS considère tous les enregistrements du SNIUMP comme des renseignements personnels sur la santé, quels que soient les éléments de données qu'ils contiennent.

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

Restriction de l'utilisation

L'ICIS restreint l'utilisation des données du SNIUMP aux objectifs autorisés décrits à la section 2, notamment pour produire de l'information exacte, actuelle et comparable sur les médicaments. 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.

Les fichiers de données utilisés à l'interne par l'ICIS à des fins d'analyse ne contiennent aucun identificateur direct, comme les dates de naissance, les codes postaux et les numéros d'assurance maladie non chiffrés. Ces renseignements sont supprimés avant que les enregistrements ne soient versés dans l'environnement analytique du SNIUMP (l'âge est indiqué plutôt que la date de naissance). Le personnel autorisé de l'ICIS a accès aux numéros d'assurance maladie non chiffrés de façon exceptionnelle, uniquement en cas de nécessité. Cet accès est assujetti aux processus internes d'approbation, comme précisé dans les procédures de respect de la vie privée de 2010 de l'ICIS.

Couplage de données

Afin de répondre à de nombreuses questions sur l'utilisation des produits pharmaceutiques, les enregistrements du SNIUMP sont couplés avec les données d'autres sources de l'ICIS. Étant donné que le couplage des données peut accroître les risques que la personne soit identifiée, l'ICIS prend les mesures d'atténuation des risques qui suivent.

Les articles 14 à 31 de la Politique de respect de la vie privée, 2010 de l'ICIS régissent le couplage des enregistrements contenant des renseignements personnels sur la santé. En vertu de cette politique, l'ICIS permet le couplage des renseignements personnels sur la santé dans certaines circonstances. Il est généralement permis de coupler des données au sein d'une seule banque de données pour l'usage exclusif de l'ICIS. Le couplage de données à partir de multiples banques de données pour l'usage exclusif de l'ICIS et 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 exigences relatives au couplage de données sont énoncées comme suit aux articles 23 **et** 24 de la Politique de respect de la vie privée, 2010 de l'ICIS :

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

OU

2. Tous les critères suivants sont respectés :
    a. l'objectif du couplage de données s'inscrit dans le mandat de l'ICIS;
    b. les avantages pour le public sont considérablement plus importants que les risques de violation de la vie privée des personnes;
    c. les résultats du couplage de données ne porteront pas préjudice aux personnes concernées;
    d. le couplage de données s'inscrit dans un projet précis et ponctuel, et les données couplées seront par la suite détruites dans le respect des règles énoncées aux articles 28 et 29;
    e. le couplage de données est effectué dans le cadre d'un programme de travail continu et approuvé de l'ICIS; les données sont conservées aussi longtemps que nécessaire pour la réalisation des fins déterminées, après quoi elles sont détruites dans le respect des règles énoncées aux articles 28 et 29;
    f. le couplage de données permet de réaliser des économies évidentes par rapport à d'autres méthodes ou est l'unique méthode envisageable.

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.

L'article 29 de la Politique de respect de la vie privée, 2010 de l'ICIS prévoit en outre qu'une destruction sécuritaire des données couplées a 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 de l'ICIS, une destruction sécuritaire a lieu lorsque les données ne sont plus nécessaires pour la réalisation des fins déterminées, conformément à la norme de destruction de l'information de l'ICIS. Cette exigence s'applique au couplage de données pour l'usage exclusif de l'ICIS comme aux demandes formulées par des tiers.

Norme de couplage de données sur les clients

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

Renvoi des données au fournisseur de données

Bien que les ministères ne demandent habituellement pas le renvoi des enregistrements soumis au SNIUMP, le renvoi des données au fournisseur de données est permis conformément à l'article 34 de la Politique de respect de la vie privée, 2010 de l'ICIS.

Restriction de la divulgation

Rapports électroniques du SNIUMP

Les rapports électroniques du SNIUMP sont accessibles dans une application en ligne sécurisée qui fournit des données agrégées sur les demandes de remboursement de médicaments. 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.

L'ICIS fournit aux ministères de la Santé participants un accès aux données agrégées du SNIUMP par l'intermédiaire des rapports électroniques du SNIUMP. L'ICIS fournit au CEPBM un accès aux données agrégées et dépersonnalisées (au niveau de l'enregistrement) du SNIUMP par l'intermédiaire d'un environnement de production de rapports électroniques distinct.

Chaque fois qu'un utilisateur accède aux rapports électroniques du SNIUMP, il doit accepter les conditions d'utilisation qui régissent les règles d'utilisation des données. Outre les conditions d'utilisation, les Principes d'exploitation du SNIUMP constituent une politique qui régit l'accès des ministères aux rapports. Ces principes d'exploitation définissent certaines règles, notamment les suivantes :

- Les ministères ne peuvent diffuser publiquement de l'information tirée des rapports électroniques du SNIUMP, à l'exception de leurs propres données.
- Les ministères ne peuvent tenter de coupler de l'information tirée des rapports électroniques du SNIUMP avec de l'information d'autres sources.

Accès du CEPMB

Le CEPMB a accès aux données dépersonnalisées (au niveau de l'enregistrement) afin d'effectuer les couplages et les 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*.

Comme pour les autres utilisateurs des rapports électroniques du SNIUMP, les utilisateurs du CEPMB doivent accepter les conditions d'utilisation chaque fois qu'ils accèdent au service. Le CEPMB a également conclu avec l'ICIS une entente qui régit son accès aux rapports électroniques du SNIUMP et établit certaines règles, notamment les suivantes :

- Le CEPMB ne doit pas divulguer l'information tirée des rapports électroniques du SNIUMP à des tiers, sauf s'il en est tenu par la loi.
- Le CEPMB prendra toutes les mesures nécessaires, y compris la suppression des cellules comprenant moins de 5 observations, afin que ses publications ne contiennent aucune information pouvant servir à identifier une personne.

Risques et mesures d'atténuation

L'évaluation des incidences sur la vie privée du SNIUMP de 2011 recommandait la mise à jour des conditions décrites ci-dessus afin de mieux tenir compte des pratiques actuelles de l'ICIS en matière de respect de la vie privée et de sécurité. Cette mise à jour a été réalisée.

L'évaluation des incidences sur la vie privée de 2011 recommandait aussi à l'ICIS de fournir des documents de formation pour mieux informer les utilisateurs de leurs responsabilités en matière de respect de la vie privée et de sécurité lors de l'utilisation des rapports électroniques du SNIUMP. Cette recommandation n'est plus pertinente, car l'ICIS va remplacer les processus spécialisés de gestion de l'accès associés aux rapports électroniques du SNIUMP par ses propres processus de gestion de l'accès normalisés. Lors de cette transition, la documentation spécialisée des rapports électroniques du SNIUMP, y compris les documents concernant les responsabilités en matière de respect de la vie privée et de sécurité, sera remplacée par la documentation normalisée existante de l'ICIS.

Demandes de données formulées par des tiers

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

L'ICIS administre un programme de demandes de données par des tiers qui contient des mesures de contrôle appropriées de respect de la vie privée et de la sécurité, et s'assure de leur respect par l'organisme demandeur. En outre, comme le stipulent les articles 45 à 47 de sa Politique de respect de la vie privée, 2010, l'ICIS s'efforce de divulguer les données dans le plus grand anonymat possible tout en répondant aux exigences de recherche ou d'analyse du demandeur. C'est pourquoi les données sont agrégées dans la mesure du possible. Si les données agrégées ne sont pas suffisamment détaillées pour les besoins définis, l'ICIS peut décider au cas par cas de divulguer au destinataire des données au niveau de l'enregistrement qui ont été dépersonnalisées. Le destinataire doit avoir signé au préalable une entente de protection des données ou un autre instrument juridiquement contraignant avec l'ICIS. Seuls les éléments de données nécessaires aux fins prévues seront divulgués.

L'ICIS a adopté une approche de gestion axée sur le cycle de vie en ce qui a trait aux demandes de données au niveau de l'enregistrement provenant de tiers. Le Secrétariat à la vie privée et aux services juridiques a élaboré un processus, dont il est responsable, 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 destinataires tiers de données font l'objet d'un suivi et d'une surveillance de façon à garantir leur destruction sécuritaire à la fin de leur cycle de vie. Avant d'avoir accès aux données, les demandeurs tiers doivent signer une entente de protection des données et doivent 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 soumettre une demande par écrit. Ils doivent également signer une entente en vertu de laquelle ils s'engagent à n'utiliser les données qu'aux fins précisées. Toutes les ententes de protection des données conclues avec des tiers précisent que les organismes destinataires doivent veiller à la stricte confidentialité des données dépersonnalisées au niveau de l'enregistrement et qu'ils ne doivent pas divulguer ces données à des personnes à l'extérieur de l'organisme. L'ICIS impose en outre des obligations à ces tiers destinataires, notamment

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

Outre le processus de surveillance de la conformité, qui consiste à s'assurer que les données saisies satisfont aux exigences en matière de destruction des données, le Secrétariat à la vie privée et aux services juridiques communique chaque année avec les tiers destinataires de données pour vérifier qu'ils respectent toujours les obligations énoncées dans le formulaire de demande de données et l'entente de protection des données de l'ICIS qu'ils ont signés.

Restriction de la conservation

Le SNIUMP fait partie des banques de données de l'ICIS et, 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 exhaustif 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 SNIUMP doit subir régulièrement une évaluation de la qualité des données fondée sur le Cadre de la qualité des données de l'ICIS. Ce processus comprend de nombreuses activités visant à évaluer les diverses dimensions de la qualité, dont l'exactitude des enregistrements 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

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. Fondé sur les pratiques exemplaires qui ont cours dans les secteurs public, privé et de la santé, le cadre est conçu de façon à coordonner les politiques de l'ICIS en matière de respect de la vie privée et de sécurité, et à offrir une vision intégrée des pratiques de gestion de l'information adoptées par l'organisme. Les paragraphes qui suivent décrivent les aspects de la sécurité des systèmes de l'ICIS qui revêtent une importance particulière au regard du SNIUMP.

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 d'élimination. Par conséquent, l'ICIS a adopté un ensemble complet de politiques qui précisent les contrôles nécessaires à la protection de l'information en format physique et électronique, y compris à l'étape du chiffrement et de l'élimination 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 dossiers, afin de garantir la confidentialité, l'intégrité et la disponibilité des actifs informationnels de l'ICIS.

Les registres de contrôle et de vérification du système font partie intégrante du programme de sécurité de l'information de l'ICIS et sont immuables. En général, l'ICIS utilise des données dépersonnalisées au niveau de l'enregistrement (où le numéro d'assurance maladie a été supprimé ou chiffré) pour réaliser ses analyses. Dans le cas du SNIUMP, les identificateurs directs, tels que les numéros d'assurance maladie non chiffrés, les dates de naissance et les codes postaux, sont retirés des fichiers analytiques. Le personnel peut, dans des circonstances exceptionnelles, nécessiter un accès aux numéros d'assurance maladie d'origine. Les procédures de respect de la vie privée de 2010 de l'ICIS prévoient des contrôles stricts qui garantissent que l'accès est autorisé au niveau et dans les circonstances appropriés, et que le principe de la minimisation des données est respecté en tout temps. L'ICIS consigne dans ses registres les activités suivantes ayant trait à l'accès aux données :

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

Les employés de l'ICIS sont sensibilisés à l'importance de maintenir la confidentialité des renseignements personnels sur la santé et d'autres types d'information sensible au moyen d'un programme de formation obligatoire sur le respect de la vie privée et la sécurité, et par l'intermédiaire de communications continues concernant les politiques et procédures de l'ICIS à ce sujet. Avant chaque tentative de connexion à un système d'information de l'ICIS, les employés doivent confirmer qu'ils comprennent l'interdiction d'accéder à ce système informatique ou de l'utiliser sans autorisation préalable expresse de l'ICIS ni au-delà de cette autorisation.

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

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

3.10 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 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 il est précisé aux articles 64 et 65 de la Politique de respect de la vie privée, 2010 de l'ICIS, les plaintes concernant le traitement 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 SNIUMP effectuée par l'ICIS n'a décelé aucun risque de violation du respect de la vie privée.

L'évaluation sera mise à jour ou révisée conformément à la Politique : Évaluation des incidences sur la vie privée de l'ICIS.

Annexe : Texte de remplacement de la figure

Figure : Cheminement des données du SNIUMP

Cette figure illustre le cheminement des données du SNIUMP.

Les données sont soumises au SNIUMP par les ministères de la Santé. Plus précisément, les ministères 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.

Les données sont extraites de plusieurs façons :

1. Le SNIUMP fournit aux ministères de la Santé fédéral, provinciaux et territoriaux des rapports qui contiennent des données agrégées.
2. Le SNIUMP fournit au Conseil d’examen du prix des médicaments brevetés des rapports qui contiennent à la fois des données agrégées et des données dépersonnalisées au niveau de l’enregistrement.
3. Le SNIUMP peut en général divulguer des données agrégées et dépersonnalisées au niveau de l’enregistrement aux tiers qui en font la demande. Il divulgue aussi des données aux ministères de la Santé fédéral, provinciaux et territoriaux ainsi qu’au Conseil d’examen du prix des médicaments brevetés.
4. Le SNIUMP divulgue des données agrégées au public.

aide@icis.ca

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

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

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

ICIS Montréal
1010, rue Sherbrooke Ouest
Bureau 602
Montréal (Qc)
H3A 2R7
514-842-2226

icis.ca

17136-0318