



Évaluation des incidences sur la vie privée du Système de déclaration de l'expérience des patients canadiens

Août 2020



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

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

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

© 2020 Institut canadien d'information sur la santé

Comment citer ce document :

Institut canadien d'information sur la santé. *Évaluation des incidences sur la vie privée du Système de déclaration de l'expérience des patients canadiens, août 2020.* Ottawa, ON : ICIS; 2020.

This publication is also available in English under the title *Canadian Patient Experiences Reporting System Privacy Impact Assessment, August 2020.*

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

- *Évaluation des incidences sur la vie privée du Système de déclaration de l'expérience des patients canadiens, août 2020*

Approuvé par

Brent Diverty

Vice-président, Stratégies de données et Statistiques

Rhonda Wing

Chef de la protection des renseignements personnels et avocate générale

Ottawa, août 2020

Table des matières

Le Système de déclaration de l'expérience des patients canadiens en bref	5
1 Introduction	6
2 Renseignements contextuels	6
2.1 Présentation du SDEPC	6
2.2 Collecte de données	7
2.3 Gestion de l'accès, soumission des données et cheminement des données : SDEPC	10
3 Analyse du respect de la vie privée	13
3.1 Programme de gestion des risques liés au respect de la vie privée et à la sécurité	13
3.2 Textes législatifs et juridiques régissant les données du SDEPC	14
3.3 Premier principe : responsabilité à l'égard des renseignements personnels sur la santé	15
3.4 Deuxième principe : établissement des objectifs de la collecte de renseignements personnels sur la santé	16
3.5 Troisième principe : consentement pour la collecte, l'utilisation ou la divulgation de renseignements personnels sur la santé	16
3.6 Quatrième principe : restriction de la collecte de renseignements personnels sur la santé	17
3.7 Cinquième principe : restriction de l'utilisation, de la divulgation et de la conservation des renseignements personnels sur la santé	18
3.8 Sixième principe : exactitude des renseignements personnels sur la santé	22
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	24
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	25
4 Conclusion	25
Annexe : Texte de remplacement pour la figure	26

Le Système de déclaration de l'expérience des patients canadiens en bref

1. Lancé en avril 2015, le Système de déclaration de l'expérience des patients canadiens (SDEPC) recueille et déclare des données sur l'expérience des patients dans les systèmes de santé au Canada, en commençant par les patients hospitalisés dans les établissements de soins de courte durée. Le SDEPC a pour objectif de produire de l'information normalisée sur l'expérience des patients de partout au pays, dans le but d'orienter et d'améliorer les soins axés sur le patient et les résultats pour le patient.

Les dispensateurs de soins, les gestionnaires des systèmes de santé, les responsables des politiques et les patients utilisent l'information provenant du SDEPC pour
 - analyser l'aspect de la qualité des soins qui touche l'expérience du patient aux fins d'établissement de rapports, de surveillance et de comparaison de la performance;
 - déterminer et orienter les améliorations en matière de qualité et d'efficacité, et évaluer les interventions en santé pour mieux appuyer l'intégration des soins de manière à offrir des soins qui soient davantage axés sur le patient.
2. Avec l'apport d'un vaste éventail d'experts, l'Institut canadien d'information sur la santé (ICIS) a piloté l'élaboration d'un outil de sondage normalisé, le Sondage sur les expériences d'hospitalisation des patients canadiens (SEHPC). Les données du SEHPC soumises au SDEPC portent sur les expériences des patients hospitalisés en soins de courte durée.
3. Le SDEPC contient des renseignements personnels sur la santé (numéro d'assurance maladie et date de naissance), ainsi que les réponses aux questions du SEHPC et des données démographiques. Les champs de projets spéciaux servent à recueillir de l'information supplémentaire qui répond aux besoins particuliers de l'ICIS, des autorités compétentes ou des établissements.
4. Les hôpitaux, régions sanitaires, conseils de la qualité en santé et ministères de la Santé participants, ou leurs mandataires, communiquent avec les patients après leur sortie de l'hôpital pour recueillir des données au sujet de leurs expériences à titre de patients hospitalisés. Ils transmettent ensuite ces données au SDEPC conformément aux spécifications du fichier minimal et prédéterminées du SEHPC. Les méthodes de sondage (p. ex. le mode de collecte) ainsi que la fréquence et la durée du sondage varient selon l'autorité compétente.
5. En date de juin 2020, le SDEPC contenait plus de 320 000 enregistrements de sondage sur l'expérience d'hospitalisation des patients soumis par 6 autorités compétentes (Nouvelle-Écosse, Nouveau-Brunswick, Ontario, Manitoba, Alberta et Colombie-Britannique).

6. Les données du SDEPC sont utilisées à des fins de production de rapports normalisés et d'analyse ainsi que pour le couplage des données à l'échelle de la personne entre les banques de données et au fil du temps. À l'heure actuelle, les autorités compétentes participantes ont accès aux données comparatives sur les hôpitaux versées au SDEPC au moyen de l'outil SEHPC : résultats comparatifs de l'ICIS. L'ICIS travaille à la diffusion publique, prévue pour 2022, d'un ensemble d'indicateurs de base (3 à 5) sur l'expérience des patients dans l'outil Web [Votre système de santé : En détail](#).

1 Introduction

L'Institut canadien d'information sur la santé (ICIS) recueille de l'information sur la santé et les soins de santé au Canada et l'analyse. 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 but d'examiner les risques liés au respect de la vie privée, à la confidentialité et à la sécurité associés au Système de déclaration de l'expérience des patients canadiens (SDEPC). Elle remplace la version de janvier 2015 et comprend un examen des 10 principes énoncés dans le *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation et de leur application au SDEPC. Elle passe également en revue l'application du [Cadre de gestion des risques liés au respect de la vie privée et à la sécurité](#) de l'ICIS.

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

2 Renseignements contextuels

2.1 Présentation du SDEPC

Pour que les soins offerts soient axés sur le patient, il est essentiel de comprendre et d'améliorer l'expérience des personnes qui reçoivent des services et des soins de santé ou subissent une intervention.

Afin de combler les lacunes en matière d'information et le manque d'uniformité des données sur l'expérience des patients, l'ICIS a piloté l'élaboration d'un outil de sondage normalisé, le Sondage sur les expériences d'hospitalisation des patients canadiens (SEHPC). Le Système de déclaration

de l'expérience des patients canadiens (SDEPC) vise donc à produire de l'information normalisée et comparable sur l'expérience des patients, à commencer par ceux qui sont hospitalisés en soins de courte durée au Canada, à partir du SEHPC.

L'information provenant du SDEPC nous aide à mieux comprendre et comparer les points de vue des patients sur les services, les interventions et les soins, afin d'orienter et d'améliorer les soins axés sur les patients, de même que les résultats pour les patients au Canada. Les dispensateurs de soins, les gestionnaires des systèmes de santé et les responsables des politiques utilisent l'information provenant du SDEPC pour

- produire des données comparables sur l'aspect de la qualité des soins qui touche l'expérience du patient aux fins d'établissement de rapports, de surveillance et de comparaison de la performance;
- produire des données qui permettront de déterminer et d'orienter les améliorations en matière de qualité et d'efficacité, et d'évaluer les interventions en santé pour mieux appuyer l'intégration des soins de manière à offrir des soins qui soient davantage axés sur le patient.

Les données recueillies dans le système pourraient ensuite s'étendre à d'autres secteurs de soins.

2.2 Collecte de données

Les données recueillies dans le SDEPC au moyen du SEHPC portent sur 3 gammes de services hospitaliers (médicaux, chirurgicaux et obstétricaux). Le SDEPC recueille

- les réponses des patients aux questions du SEHPC;
- l'information relative aux méthodes du sondage et aux processus d'administration du sondage;
- les données administratives pouvant servir à la soumission et à la production d'analyses et de rapports.

Les hôpitaux, régions sanitaires, conseils de la qualité en santé et ministères de la Santé participants, ou leurs mandataires, communiquent avec les patients après leur sortie de l'hôpital pour recueillir des données au sujet de leurs expériences à titre de patients hospitalisés. Ils transmettent ensuite ces données au SDEPC conformément aux spécifications du fichier minimal et prédéterminées du SEHPC. Les méthodes de sondage (p. ex. le mode de collecte) ainsi que la fréquence et la durée du sondage varient selon l'autorité compétente.

En date de juin 2020, le SDEPC contenait plus de 320 000 enregistrements de sondage sur l'expérience d'hospitalisation des patients soumis par 6 autorités compétentes (Nouvelle-Écosse, Nouveau-Brunswick, Ontario, Manitoba, Alberta et Colombie-Britannique). La soumission de données au SDEPC est volontaire. Elle est coordonnée à l'échelle provinciale

(p. ex. par le ministère de la Santé ou le conseil de la santé) dans 5 des autorités compétentes participantes. En Ontario, la décision de soumettre des données dans le cadre d'un contrat de service établi par l'Association des hôpitaux de l'Ontario ou directement à l'ICIS relève plutôt de l'établissement.

Le SDEPC comprend des éléments de données qui, seuls ou jumelés à d'autres renseignements, permettent d'identifier une personne. Les éléments de données particulièrement sensibles du SDEPC sont énumérés ci-dessous. Le tableau 1 décrit les raisons qui motivent la collecte de renseignements personnels sur la santé dans le SDEPC.

Identificateurs directs (renseignements personnels sur la santé)

Le SDEPC recueille les identificateurs directs suivants :

- Date de naissance complète
- Numéro d'assurance maladie
- Autorité émettrice du numéro d'assurance maladie

Autres identificateurs uniques

Le SDEPC recueille les autres identificateurs uniques suivants :

- Identificateur du patient au sein de l'organisme (p. ex. numéro de dossier)
- Sexe
- Origine ethnique
- Niveau de scolarité

Identificateur de l'établissement de santé

Le SDEPC recueille l'identificateur de l'établissement de santé suivant :

- Identificateur de l'organisme

Tableau 1 Raisons qui motivent la collecte de données sensibles dans le SDEPC

Élément/définition	Moment de la collecte	Raison de la collecte et commentaires
<p>Numéro d'assurance maladie</p> <p>Numéro unique attribué par une autorité compétente à un patient qui a reçu ou qui reçoit des biens ou des services liés aux soins de santé; ceci comprend le code de l'autorité compétente qui a émis le numéro d'assurance maladie</p>	Élément provenant du système administratif de l'hôpital, requis au moment de la soumission à l'ICIS	<p>Pour identifier chaque patient au sein d'une autorité compétente</p> <p>Pour permettre le couplage avec d'autres banques de données de l'ICIS et constituer une riche source de données pour les analyses et les rapports</p>
<p>Identificateur du patient au sein de l'organisme</p> <p>Identificateur unique (p. ex. un numéro de dossier) attribué par l'organisme à un patient qui a reçu ou qui reçoit des biens ou des services liés aux soins de santé</p>	Élément provenant du système administratif de l'hôpital, requis au moment de la soumission à l'ICIS	<p>Pour permettre le couplage d'un enregistrement du SEHPC avec la visite correspondante à l'hôpital (p. ex. un enregistrement de la Base de données sur les congés des patients) quand un identificateur du patient au sein de l'organisme identifiable est fourni (parallèlement à la date de sortie)</p> <p>Pour identifier de façon unique une personne au sein d'un organisme source en l'absence du numéro d'assurance maladie</p>
<p>Date de naissance</p> <p>L'année, le mois et le jour correspondant à la date de naissance officielle ou présumée du patient</p>	Élément provenant du système administratif de l'hôpital ou fourni par le patient lors du sondage; peut être utilisé au moment de la détermination de l'échantillon du sondage (p. ex. les patients qui ont 18 ans et plus) et au moment de la soumission à l'ICIS	Pour déterminer l'âge des patients, un élément nécessaire pour effectuer des analyses selon l'âge et améliorer le couplage avec d'autres banques de données de l'ICIS
<p>Sexe</p> <p>Code utilisé pour indiquer le sexe du patient</p>	Élément provenant du système administratif de l'hôpital ou fourni par le patient lors du sondage	Pour permettre l'analyse des différences dans les expériences des patients selon le sexe
<p>Origine ethnique</p> <p>Appartenance déclarée par le patient à un groupe ou plusieurs groupes sociaux dont les membres ont une tradition nationale ou culturelle commune</p>	Élément fourni par le patient lors du sondage	Pour permettre l'analyse des différences dans les expériences des patients selon les divers groupes ethniques

2.3 Gestion de l'accès, soumission des données et cheminement des données : SDEPC

L'accès aux applications sécurisées de l'ICIS est soumis au processus de gestion de l'accès en fonction du type d'utilisateur de l'ICIS, qui est géré par la direction des Applications de soutien aux clients (ASC). Les ASC gèrent 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).

Les fournisseurs de données du SDEPC, une fois authentifiés dans le SGA, soumettent à l'ICIS des données au niveau de l'enregistrement obtenues des établissements. Ces données sont saisies électroniquement, au moyen d'un logiciel spécialisé, et transmises par l'intermédiaire du Service de soumission électronique de données (eDSS) ou du service de soumission de données sécurisé de l'ICIS aux fins de traitement, à savoir les 2 méthodes de transmission de données sécurisées privilégiées par l'ICIS. Les données sont soumises au SDEPC conformément aux normes de collecte de données ci-dessous :

Normes relatives au sondage

- [Sondage sur les expériences d'hospitalisation des patients canadiens](#)
- [Manuel de procédure du Sondage sur les expériences d'hospitalisation des patients canadiens](#)

Normes de soumission de données

- [Dictionnaire de données du Sondage sur les expériences d'hospitalisation des patients canadiens](#)
- Spécifications à l'intention des fournisseurs, accessibles une fois le contrat de licence à l'usage des fournisseurs signé

Au moment du traitement, toutes les données soumises au SDEPC font automatiquement l'objet de validations et de contrôles de la qualité qui permettent de repérer les erreurs et les incohérences par rapport aux spécifications énoncées dans le *Dictionnaire de données du Sondage sur les expériences d'hospitalisation des patients canadiens* et la trousse de spécifications à l'intention des fournisseurs. Le système de traitement des données est un processus interne; aucun accès n'y est possible à l'extérieur de l'ICIS.

Les fournisseurs de données ont accès aux rapports d'erreurs et de validation générés au moment du traitement par l'intermédiaire de l'application Rapports opérationnels, conformément à la norme sur le transfert sécuritaire de l'information (*Secure Information Transfer Standard*) de l'ICIS. Ces rapports de soumission détaillés indiquent les

enregistrements qui contiennent des erreurs (en précisant l'organisme qui a soumis les données et l'organisme source, le nom du fichier et l'identificateur du sondage, du cycle de sondage et de l'élément de données), le nombre d'enregistrements soumis qui ont été acceptés, ainsi que les motifs des rejets ou de tout message d'avertissement pertinent; ils permettent en outre au fournisseur de données de corriger les enregistrements pour les soumettre de nouveau au SDEPC.

Une fois le processus itératif de correction des erreurs terminé, les rapports sommaires finaux des résultats du traitement des fichiers sont renvoyés au fournisseur de données par l'intermédiaire de l'application Rapports opérationnels. Une copie complète du fichier de données soumis au SDEPC est alors téléchargée dans l'environnement analytique SAS de l'ICIS et mise à la disposition du personnel autorisé pour les besoins de l'ICIS.

Sur demande, l'ICIS renvoie les données du SDEPC au fournisseur de données qui a d'abord fourni les données ainsi qu'au ministère de la Santé concerné. À l'heure actuelle, les autorités compétentes participantes ont accès aux données agrégées comparatives sur les hôpitaux du SDEPC au moyen de l'outil SEHPC : résultats comparatifs de l'ICIS. Cet outil en ligne sécurisé permet aux utilisateurs autorisés de consulter leurs résultats aux mesures des expériences des patients et de les comparer à ceux d'autres hôpitaux participants. L'ICIS diffuse par ailleurs des statistiques agrégées et des analyses à l'intention du grand public. Il projette de présenter les résultats de l'expérience des patients (pour un ensemble de mesures de base) dans son outil [Votre système de santé](#) de l'ICIS. La figure ci-dessous illustre le cheminement général des données du SDEPC.

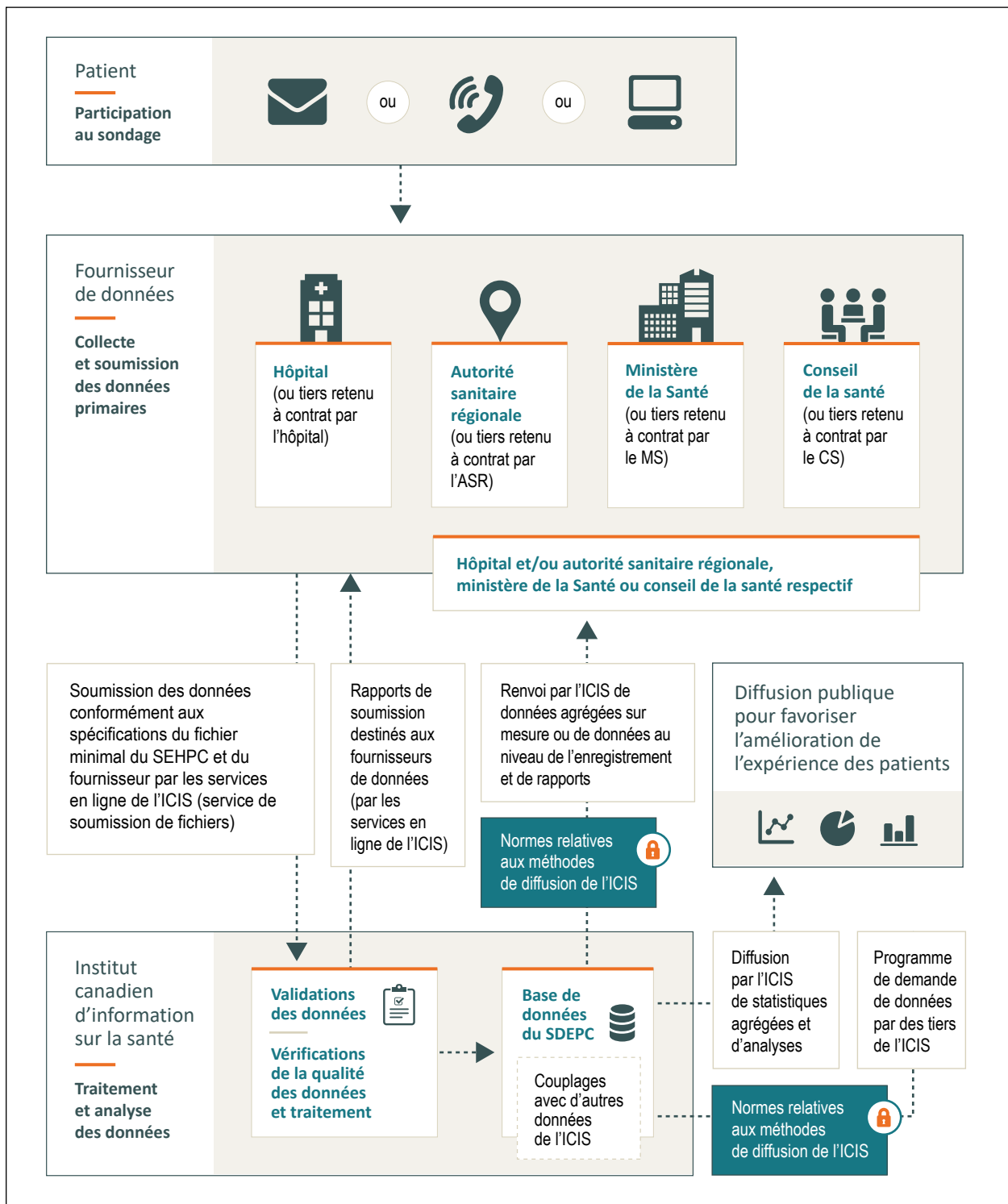
Accès du personnel de l'ICIS aux données du SDEPC

L'accès du personnel à l'environnement analytique SAS est géré au moyen du processus centralisé d'accès aux données SAS de l'ICIS. Ce processus garantit que toutes les demandes d'accès, y compris aux données du SDEPC, sont vérifiables et autorisées. Le système d'accès aux données SAS fait l'objet d'une vérification annuelle qui permet de confirmer que les employés accèdent aux données seulement en cas de nécessité. La section 3.9 explique comment les différentes mesures procédurales et techniques sont mises en place en vue de prévenir l'accès non autorisé aux données du SDEPC et de sécuriser les données de toute autre manière.

Cheminement des données

L'ICIS reçoit et transmet les données du SDEPC à l'aide d'une application Web sécurisée (voir la figure).

Figure Aperçu du cheminement des données pour le SDEPC



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 pouvant être reproduit. Elle 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 incidence possible. En 2015, l'ICIS a approuvé son [Cadre de gestion des risques liés au respect de la vie privée et à la sécurité](#) et mis en œuvre la [Politique sur la gestion des risques liés au respect de la vie privée et à la sécurité](#) connexe. La chef de la protection des renseignements personnels et le chef de la sécurité de l'information de l'ICIS, en collaboration avec les membres de la direction, ont la responsabilité de détecter, d'évaluer, de prendre en charge, de surveiller et d'examiner les risques en matière de respect de la vie privée et de sécurité.

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

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

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

3.2 Textes législatifs et juridiques régissant les données du SDEPC

Renseignements généraux

L'ICIS se conforme à sa [Politique de respect de la vie privée, 2010](#) ainsi qu'à toute législation ou entente applicable.

Lois sur la protection de la vie privée

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

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

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

Ententes

À l'ICIS, les données du SDEPC 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 divulgation, à la conservation et à la destruction des renseignements personnels sur la santé soumis à l'ICIS, ainsi qu'à toute divulgation pouvant être permise subséquemment. Les ententes décrivent aussi l'autorité législative en vertu de laquelle les renseignements personnels sur la santé sont divulgués à l'ICIS.

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

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

Organisation et gouvernance

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

Tableau 2 Principaux postes et responsabilités

Poste, groupe	Rôles et responsabilités
Vice-président, Stratégies de données et Statistiques	Responsable de l'orientation stratégique générale du SDEPC
Directeur, Services d'information sur les soins ambulatoires et de courte durée	Responsable du fonctionnement général du SDEPC et des décisions administratives stratégiques connexes ainsi que de la gestion des relations stratégiques
Gestionnaire, Registres des remplacements articulaires, Résultats et expériences déclarés par les patients	Responsable de la gestion continue et de la mise en place du SDEPC; prend les décisions opérationnelles quotidiennes relatives au SDEPC et soutient les groupes de travail et comités du SDEPC
Chef de la sécurité de l'information	Responsable de l'orientation stratégique et de la mise en œuvre générale du programme de sécurité de l'information de l'ICIS
Chef de la protection des renseignements personnels	Responsable de l'orientation stratégique et de la mise en œuvre générale du programme de respect de la vie privée de l'ICIS
Gestionnaire, Acquisition de données	Responsable du respect des exigences techniques permettant l'exploitation et l'amélioration continues du SDEPC; agit à titre d'administrateur de système pour le SDEPC
Gestionnaire, Soutien et engagement des clients	Responsable de la gestion de l'accès des clients externes aux services Web à accès restreint

Groupes de travail et comités

L'ICIS sollicite les conseils de 2 groupes de travail externes pour orienter les activités du SDEPC, dont le groupe consultatif interprovincial sur les mesures axées sur les patients qui guide l'ICIS dans l'élaboration d'une stratégie commune pour les mesures et rapports axés sur les patients au Canada. Il favorise l'apprentissage entre pairs et la mise en commun de pratiques exemplaires, et formule des conseils et des recommandations pour renforcer l'utilisation des résultats des mesures axées sur les patients.

Le deuxième groupe de travail, soit celui sur la mise en œuvre du SDEPC, réunit les autorités compétentes qui participent au SDEPC. Il recueille de l'information et des observations touchant la collecte de données sur les expériences des patients au sein de chaque autorité compétente dans le but d'éclairer la prise de décisions relatives à la mise en œuvre du SEHPC et à la soumission de données au SDEPC, et facilite la mise en commun des leçons tirées des activités de mise en œuvre.

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

L'ICIS ne recueille que les renseignements personnels sur la santé nécessaires à l'atteinte des objectifs du SDEPC (voir la [section 2.1](#)). Un manuel d'instructions à l'intention des fournisseurs de données du SDEPC ([Dictionnaire de données du SEHPC](#)) présente une liste des éléments de données et décrit leur raison d'être. Ce document, qui est mis à jour au besoin, est accessible au public sur le site Web de l'ICIS.

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

À titre de collecteur secondaire de données, l'ICIS n'a pas de contact direct avec les patients. Il 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 autorités compétentes.

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. 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 du système de santé, dont l'analyse statistique et la production de rapports, à des fins de gestion, d'évaluation ou de surveillance des systèmes de santé.

Conformément à ce principe, le SDEPC ne recueille que les renseignements nécessaires à la réalisation de ses objectifs, tels que ceux-ci sont décrits à la [section 3.4](#) ci-dessus.

Le fichier minimal de données recueillies dans le cadre du SEHPC renferme de l'information relative au sondage sur les expériences des patients et d'autres renseignements. Il s'agit là de l'information minimale nécessaire aux activités du SDEPC.

L'ICIS a élaboré le SEHPC avec l'apport d'un large éventail d'intervenants, en s'inspirant du sondage Hospital Consumer Assessment of Healthcare Providers and Systems (HCAHPS). Ces intervenants comprenaient le groupe interprovincial sur la satisfaction des patients (Inter-Jurisdictional Patient Satisfaction Group), Agrément Canada, l'Institut canadien pour la sécurité des patients, la Change Foundation et le groupe de travail chargé du développement du SDEPC.

La partie du fichier minimal du SEHPC qui concerne la soumission renferme des éléments de données qui facilitent le processus de soumission à l'ICIS (p. ex. identificateur de l'organisme qui soumet les données) et des éléments de données se rapportant à la méthodologie du sondage qui sont nécessaires à l'analyse et à la production de rapports (p. ex. taille de l'échantillon, nombre de sorties admissibles, méthode d'échantillonnage).

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 SDEPC aux objectifs autorisés décrits à la section 3.4 ci-dessus. Cela comprend les analyses comparatives à l'échelle des provinces et territoires ainsi que d'une province ou d'un territoire à l'autre, les analyses des tendances visant à évaluer ou à surveiller l'incidence de tout changement en matière de politiques, de pratiques et de prestation de services, ainsi que la production de statistiques pour appuyer la planification, la gestion et l'amélioration de la qualité.

ICIS

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

Les fichiers de données utilisés à l'interne par l'ICIS à des fins d'analyse ne contiennent aucun nom ni identificateur direct, comme des numéros d'assurance maladie non chiffrés. Ces renseignements sont supprimés avant le versement des enregistrements dans l'environnement analytique du SDEPC (voir la section 2.3 ci-dessus). 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 assujéti aux processus internes d'approbation, comme précisé dans la politique de respect de la vie privée de 2010 de l'ICIS.

Couplage des données

Les données du SDEPC sont couplées avec les données d'autres sources de l'ICIS. Les données sur les expériences des patients prennent davantage de valeur lorsqu'elles sont couplées à l'enregistrement de l'épisode de services en soins de courte durée auquel elles se rapportent. Un tel couplage fournit de l'information sur la complexité et d'autres aspects pertinents de l'expérience, comme les événements indésirables. Il permet également

l'élaboration et la mise en application de méthodologies (p. ex. pondération et ajustements) qui contribuent à renforcer la comparabilité des résultats. Étant donné que le couplage des données peut accroître les risques d'identification de la personne, l'ICIS prend des mesures d'atténuation des risques.

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

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

- Article 23 Les personnes dont les renseignements personnels sur la santé sont utilisés pour le couplage de données y consentent au préalable. OU
- Article 24 Tous les critères suivants sont respectés :
- a) l'objectif du couplage de données s'inscrit dans le mandat de l'ICIS;
 - b) les avantages pour le public sont considérablement plus importants que les risques de violation de la vie privée des personnes;
 - c) les résultats du couplage de données ne porteront pas préjudice aux personnes concernées;
 - d) le couplage de données s'inscrit dans un projet précis et ponctuel, et les données couplées seront par la suite détruites dans le respect des règles énoncées aux articles 28 et 29;
 - e) le couplage de données est effectué dans le cadre d'un programme de travail continu et approuvé de l'ICIS; les données sont conservées aussi longtemps que nécessaire pour la réalisation des fins déterminées, après quoi elles sont détruites dans le respect des règles énoncées aux articles 28 et 29;
 - f) le couplage de données permet de réaliser des économies évidentes par rapport à d'autres méthodes ou est l'unique méthode envisageable.

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 depuis 2010-2011 et qui contiennent 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.

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

Renvoi des données au fournisseur de données

L'article 34 de la [Politique de respect de la vie privée, 2010](#) stipule que l'ICIS, en plus de renvoyer les données aux organismes déclarants, peut également remettre les enregistrements au ministère de la Santé concerné, pour des motifs de qualité des données ou à d'autres fins inscrites dans son mandat (p. ex. la gestion des services de santé et de la santé de la population, qui comprend la planification, l'évaluation et l'affectation des ressources). Le renvoi des données au fournisseur de données est considéré comme une utilisation et non comme une divulgation.

Restriction de la divulgation

Comme il est mentionné à la section 2.3 du présent document, les autorités compétentes participantes peuvent consulter les données du SDEPC au moyen de l'outil SEHPC : résultats comparatifs.

Pour accéder à cet outil, les utilisateurs doivent au préalable signer une entente de service assortie d'exigences relatives aux renseignements identifiant un établissement de santé et à la suppression des cellules de faible valeur.

Demandes de données 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 SDEPC. L'ICIS administre le programme de demandes de données par des tiers qui établit les mesures de contrôle appropriées 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 tout en répondant aux exigences de recherche ou d'analyse du demandeur. Cela signifie que les données sont agrégées dans la mesure du possible. Si les données agrégées ne sont pas suffisamment détaillées pour les besoins définis, l'ICIS peut 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 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 de surveillance continue de la conformité qui fait partie intégrante de ce cycle de vie. Dans le cadre de ce processus, dont il est responsable, tous les fichiers de données qui sont divulgués à des 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 tiers demandeurs 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 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 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 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.

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.

Dans le cadre de sa démarche progressive de diffusion publique des données sur l'expérience des patients, l'ICIS travaille à la publication d'un ensemble d'indicateurs de base (3 à 5) sur l'expérience des patients dans l'outil Web [Votre système de santé : En détail](#). Une fois en ligne, les données de ces indicateurs permettront d'effectuer des comparaisons à l'échelle du pays, des provinces et des territoires, des régions et des établissements. Ces indicateurs devraient être publiés en 2022.

Restriction de la conservation

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

3.8 Sixième principe : exactitude des renseignements personnels sur la santé

L'ICIS est doté d'un programme 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 SDEPC doit régulièrement subir une évaluation de la qualité des données fondée sur le [Cadre de la qualité de l'information de l'ICIS](#). Ce processus comprend de nombreuses activités visant à évaluer les diverses dimensions de la qualité, dont l'exactitude des données du SDEPC.

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

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

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

Sécurité des systèmes

L'ICIS reconnaît que l'information ne peut être considérée comme sécurisée que si elle est protégée pendant tout son cycle de vie, c'est-à-dire à chaque étape des processus de création, de collecte, d'accès, de conservation, de stockage, d'utilisation, de divulgation et de destruction. Par conséquent, l'ICIS a adopté un ensemble exhaustif de politiques qui précisent les contrôles nécessaires à la protection de l'information en format physique et électronique jusqu'à l'étape du chiffrement et de la destruction sécurisée. Ces politiques ainsi que les normes, lignes directrices et procédures opérationnelles qui s'y rattachent sont conformes aux pratiques exemplaires en matière de respect de la vie privée, de sécurité de l'information et de gestion des 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. Ces registres sont par ailleurs immuables. En général, l'ICIS utilise des données dépersonnalisées au niveau de l'enregistrement (où le numéro d'assurance maladie a été supprimé ou chiffré) pour réaliser ses analyses. Il arrive dans des circonstances exceptionnelles que le personnel doive avoir accès aux numéros d'assurance maladie d'origine. La politique de respect de la vie privée de 2010 de l'ICIS prévoit des contrôles stricts qui garantissent que l'accès est autorisé dans les circonstances et au niveau appropriés, et que le principe de minimisation des données est respecté en tout temps. L'ICIS consigne dans ses registres les activités suivantes ayant trait à l'accès aux données :

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

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

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

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

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

L'ICIS publie de l'information concernant ses politiques sur la 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 sur son site Web (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, questions et préoccupations concernant le traitement des renseignements par l'ICIS sont examinées par la chef de la protection des renseignements personnels, qui peut acheminer une demande ou une plainte au commissaire au respect de la vie privée de la province ou du territoire de l'auteur de la demande ou de la plainte.

4 Conclusion

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

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

Annexe : Texte de remplacement pour la figure

Figure : Aperçu du cheminement des données pour le SDEPC

Cette figure illustre le cheminement des données lors de leur entrée dans le programme du SDEPC, de leur traitement au sein de l'ICIS et de leur sortie du programme.

Après leur séjour à l'hôpital, les patients qui ont reçu des soins médicaux, chirurgicaux ou obstétricaux répondent à un questionnaire papier (par la poste), téléphonique ou électronique fondé sur le SEHPC qui permet aux fournisseurs de données (comme les hôpitaux, les régions sanitaires, les ministères de la Santé, les conseils de la santé ou les fournisseurs tiers) de recueillir de l'information sur les expériences d'hospitalisation. Ces données sont soumises à l'ICIS par voie électronique à l'aide du service de soumission de données sécurisé de l'ICIS aux fins de traitement. Elles font entre autres l'objet de validations et de contrôles de la qualité qui permettent de repérer les erreurs et les incohérences. L'ICIS envoie ensuite des rapports de soumission aux fournisseurs de données aux fins d'examen et de correction des erreurs et des incohérences décelées.

Après les validations et les contrôles de la qualité, les données font l'objet d'un traitement et d'un transfert vers la base de données du SDEPC. Le personnel de l'ICIS peut ensuite utiliser le fichier de données à des fins d'analyse et de couplage avec les enregistrements d'autres banques de données de l'ICIS, comme la Base de données sur les congés des patients, afin de produire des données agrégées ou des données au niveau de l'enregistrement sur mesure ainsi que des rapports.



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

22790-1020

