Évaluation des incidences sur la vie privée du projet de regroupement ajusté selon les risques de la population, janvier 2015

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

Notre vision

De meilleures données pour de meilleures décisions : des Canadiens en meilleure santé

Notre mandat

Exercer le leadership visant l'élaboration et le maintien d'une information sur la santé exhaustive et intégrée pour des politiques avisées et une gestion efficace du système de santé qui permettent d'améliorer la santé et les soins de santé

Nos valeurs

Respect, intégrité, collaboration, excellence, innovation

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* :

- Projet de regroupement ajusté selon les risques de la population (RARP), janvier 2015

Approuvé par

Brent Diverty
Vice-président, Programmes

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

Ottawa, janvier 2015

Table des matières

Le projet de regroupement ajusté selon les risques de la population en bref 5

1 Introduction 6

2 Projet RARP de l'ICIS 6

2.1 Contexte 6

2.2 Données et cheminement des données 9

3 Analyse du respect de la vie privée 10

3.1 Textes législatifs régissant l'ICIS et l'utilisation des données dans le cadre du projet RARP 10

3.2 Premier principe : responsabilité à l'égard des renseignements personnels sur la santé 11

3.3 Deuxième principe : Établissement des objectifs de la collecte de renseignements personnels sur la santé 12

3.4 Troisième principe : Consentement pour la collecte, l'utilisation ou la divulgation de renseignements personnels sur la santé 13

3.5 Quatrième principe : Restriction de la collecte de renseignements personnels sur la santé 13

3.6 Cinquième principe : Restriction de l'utilisation, de la divulgation et de la conservation des renseignements personnels sur la santé 14

3.7 Sixième principe : Exactitude des renseignements personnels sur la santé 17

3.8 Septième principe : Mesures de protection des renseignements personnels sur la santé 17

3.9 Huitième principe : Transparence de la gestion des renseignements personnels sur la santé 19

3.10 Neuvième principe : Accès individuel aux renseignements personnels sur la santé et modification de ceux-ci 19

3.11 Dixième principe : Plaintes concernant le traitement par l'ICIS des renseignements personnels sur la santé 19

4 Résumé de l'évaluation des incidences sur la vie privée et conclusion 19

Annexe A : Risque d'identification selon la province ou le territoire 20

Annexe B : Texte de remplacement pour la figure 21

Le projet de regroupement ajusté selon les risques de la population en bref

1. L'ICIS a mis sur pied le projet de regroupement ajusté selon les risques de la population (projet RARP) afin d'élaborer une méthodologie et un logiciel de regroupement de la population, à l'aide des données et de l'expertise de l'ICIS.
2. Le logiciel de regroupement
   - aidera l'Institut canadien d'information sur la santé (ICIS) et ses clients à faire un suivi de la santé de la population, à prévoir les tendances liées à l'utilisation des soins de santé, à surveiller et à faire le suivi des maladies et à expliquer les variations en matière d'utilisation des ressources;
   - jettera les bases de l'élaboration des modèles de financement;
   - facilitera les comparaisons interprovinciales et territoriales des intrants;
   - fournira aux clients un fondement complet à la normalisation des populations dans le cadre des analyses interprovinciales et interterritoriales.
3. Le projet d'élaboration a commencé le 1er avril 2013 et devrait prendre fin le 31 mars 2016.
4. Les principaux produits livrables de ce projet sont la méthodologie de regroupement ajusté selon les risques de la population, le logiciel SAS qui appliquera la méthodologie de regroupement de la population et les documents connexes.
5. Ce système de classification clinique sera créé à l'aide de 6 ans de données provenant de l'Ontario, de la Saskatchewan, de l'Alberta et de la Colombie-Britannique. Ces 4 provinces ont été choisies parce qu'elles disposent d'une couverture presque complète dans une vaste gamme de banques de données de l'ICIS qui contiennent des données à l'échelle du patient.
6. La méthodologie de RARP couplera et utilisera des données à l'échelle des patients provenant de sources existantes de l'ICIS, ainsi que des données recueillies devant être utilisées précisément dans le cadre du projet RARP.

1 Introduction

L'Institut canadien d'information sur la santé (ICIS) recueille et analyse de l'information sur la santé et les soins de santé au Canada. Son mandat consiste à exercer le leadership visant l'élaboration et le maintien d'une information sur la santé exhaustive et intégrée, pour des politiques avisées et une gestion efficace du système de santé qui permettent d'améliorer la santé et les soins de santé. L'ICIS obtient les données directement des hôpitaux et d'autres établissements de santé, des établissements de soins de longue durée, des régies régionales de la santé, des praticiens et des gouvernements. Ces données comprennent des renseignements sur la santé concernant les services dispensés aux patients, aux résidents et aux clients, de l'information relative à l'inscription et à la pratique des professionnels de la santé, ainsi que de l'information sur les dépenses de santé.

La présente évaluation des incidences sur la vie privée a pour but d'examiner les risques de violation de la vie privée, de la confidentialité et de la sécurité associés au projet de regroupement ajusté selon les risques de la population (projet RARP). L'évaluation est principalement axée sur les risques associés aux données recueillies par l'ICIS dans le cadre du nouveau projet RARP, ainsi que sur le risque accru d'identification des personnes que pose l'ensemble des données de RARP, lorsqu'elles sont rassemblées (c.-à-d. couplées) dans le cadre d'un programme d'activités de l'ICIS. Les risques de violation de la vie privée associés à la gestion des sources de données existantes de l'ICIS sont abordés dans les évaluations des incidences sur la vie privée déjà réalisées pour chaque base de données, qui sont publiées au www.icis.ca.

L'évaluation comprend l'examen des 10 principes énoncés dans le Code type sur la protection des renseignements personnels de l'Association canadienne de normalisation qui s'appliquent à l'élaboration de la méthodologie de RARP.

La présente évaluation des incidences sur la vie privée repose surtout sur le respect de la *Politique d'évaluation des incidences sur la vie privée* de l'ICIS.

2 Projet RARP de l'ICIS

2.1 Contexte

Une méthodologie de regroupement de la population permet de créer le profil clinique des personnes et d'établir des indicateurs de ressources qui décrivent leurs besoins actuels et futurs en matière de services de santé. Ces méthodologies s'appliquent à plusieurs domaines ayant trait à la gestion, à l'évaluation et à la réalisation de recherches sur système de santé. D'ordre clinique, la méthodologie regroupe toute la population et repose sur un ensemble de groupes ou de cellules qui décrivent l'état clinique des personnes et la gravité de leurs problèmes de santé, en mettant l'accent sur les affections chroniques. Les groupes cliniques et les modèles prévisionnels connexes utiliseront 6 années de données à l'échelle des patients provenant de plusieurs sources de données. Les données seront couplées de sorte qu'on puisse observer la population entre les secteurs de la santé et longitudinalement sur les 6 années de données.

Depuis de nombreuses années, les provinces et les territoires demandent à l'ICIS d'envisager la création d'une méthodologie de regroupement de la population. En 2010, l'ICIS a mandaté le Hay Group pour l'évaluation des besoins des clients et de la valeur d'un programme de l'ICIS qui offre une méthodologie de regroupement de la population. Dans son rapport, le Hay Group a recommandé à l'ICIS de mettre en œuvre un programme national. L'ICIS a entrepris depuis lors d'évaluer la faisabilité d'un programme de RARP et a examiné les options d'élaboration d'une telle méthodologie. L'ICIS a considéré l'acquisition de la licence d'une des méthodologies de regroupement de la population offertes sur le marché, ainsi que l'option de créer une méthodologie interne. En janvier 2013, l'ICIS a décidé d'élaborer sa propre méthodologie en raison du coût élevé des méthodologies de regroupement commerciales et parce qu'aucune d'elles n'utilisait des données canadiennes.

Cette décision permet à l'ICIS d'offrir à ses clients une méthodologie canadienne établie en fonction de la population et du système de santé du pays, de sorte qu'elle répondra aux besoins des administrateurs cliniques et chercheurs dans le domaine de la santé et de tirer profit de tous les avantages qui découlent de la précieuse information sur les soins de santé produite à l'ICIS et ailleurs au Canada. De plus, cette décision assurera la transparence de la méthodologie et permettra aux clients de comprendre la logique utilisée pour attribuer une cellule et des indicateurs de ressources précis à une personne donnée.

Grâce à la méthodologie de regroupement de la population, les intervenants seront en mesure d'identifier les grands utilisateurs potentiels du système de santé, à faire un suivi de la santé de la population, à comprendre les tendances liées à l'utilisation des soins de santé, à expliquer les variations en matière d'utilisation des ressources et à jeter les bases de l'élaboration des modèles de financement. Toute cette information fournira un fondement complet à la normalisation dans le cadre des analyses interprovinciales et interterritoriales.

Les méthodologies de regroupement de la population utilisent l'information clinique à l'échelle des personnes produite à partir des données administratives recueillies au cours des hospitalisations, des visites chez le médecin, des services de soins communautaires, entre autres. Les données administratives de tout secteur de la santé peuvent servir lorsque leur qualité est convenable et qu'elles permettent de dresser un profil représentatif de la morbidité, du niveau de fonctionnement et des risques cliniques liés à une personne.

La richesse des banques de données cliniques de l'ICIS permet le regroupement de la population, ce qui n'est pas possible pour la plupart des entités administratives à l'échelle internationale. L'ICIS a sélectionné les sources de données du RARP en fonction, en partie, de la couverture des données à l'échelle des personnes pour l'ensemble du Canada et de la capacité à coupler les données au fil du temps et entre les secteurs de la santé.

Le RARP utilisera des données provenant de sources de données existantes de l'ICIS :

- Base de données sur les congés des patients (BDCP);
- Système national d'information sur les soins ambulatoires (SNISA);
- Système d'information sur les soins de longue durée (SISLD);
- Base de données canadienne sur les coûts par patient (BDCCP);
- Répertoire sur la facturation des médecins à l'échelle des patients (FMEP) (comprend les données de l'Alberta et de la Saskatchewan au moment de l'évaluation).

En plus des données à l'échelle du patient provenant des banques de données de l'ICIS, les provinces participantes ont accepté de fournir à l'ICIS d'autres données à l'échelle du patient pour le projet RARP en particulier, notamment :

- des données sur la facturation des médecins à l'échelle des patients de l'Ontario et de la Colombie-Britannique qui ont été fournies à l'ICIS dans le cadre particulier du projet RARP, mais qui n'ont pas encore été intégrées au processus habituel de cheminement des données du Répertoire sur la FMEP de l'ICIS;
- des données sur les personnes inscrites de l'Ontario, de la Saskatchewan, de l'Alberta et de la Colombie-Britannique;
- le fichier de données sur les patients et le fichier de données sur les coûts par patient des Services de santé de l'Alberta.

La création de la méthodologie de RARP nécessitera le couplage des données énoncées ci-dessus, à l'échelle du patient, au fil du temps et entre les divers secteurs de la santé.

Les principaux produits livrables de ce projet sont la méthodologie de RARP, le logiciel SAS qui appliquera la méthodologie de regroupement de la population et les documents connexes. Le logiciel SAS sera offert aux organismes responsables de l'administration du système de santé et de la recherche sur les politiques de santé. Un rapport technique décrivant la méthodologie sera publié. Le tableau 1 présente les étapes clés du projet.

Tableau 1 : Étapes clés du projet

Étape clé	Date
Approbation du plan de projet par le comité exécutif de l'ICIS	Avril 2013
Approbation de la collecte de données dans le cadre du projet RARP par le comité exécutif de l'ICIS	Juin 2014
Diffusion d'un prototype de modèle de classification clinique au comité d'experts et aux intervenants du projet	Octobre 2014
Diffusion de la deuxième version de la classification et première ébauche du modèle prévisionnel	Mars 2015
Diffusion de la version définitive de la classification et du modèle prévisionnel avec la documentation	Septembre 2015
Achèvement de la version 1.0 du logiciel SAS pour la méthodologie de regroupement de la population et du guide de l'utilisateur	Février 2016
Production d'un rapport sur la méthodologie (en anglais seulement, diffusion en 2015-2016)	Mars 2016
Diffusion de la version définitive de la classification, du modèle prévisionnel et du logiciel de regroupement SAS ainsi que de la documentation et du guide de l'utilisateur	Mars 2016

2.2 Données et cheminement des données

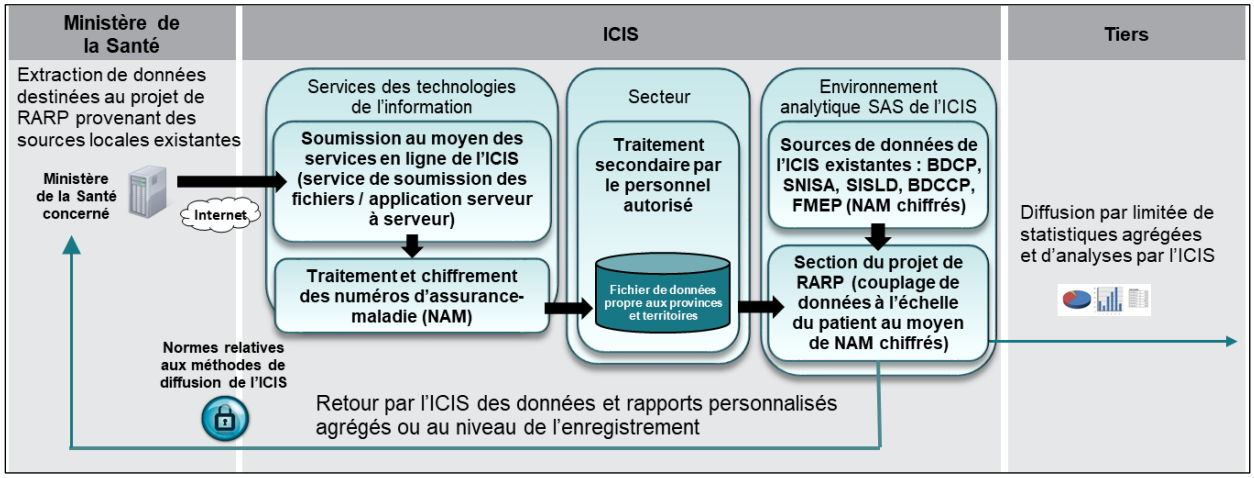
La figure illustre le cheminement général des données du projet RARP. La plupart des données utilisées dans le cadre du projet RARP proviennent directement des sources existantes internes de l'ICIS, notamment le Répertoire sur la FMEP, la BDCP, le SNISA, le SISLD et la BDCCP. Les données au niveau de l'enregistrement des sources existantes de l'ICIS, dont les numéros d'assurance maladie originaux ont été supprimés et remplacés par des numéros d'assurance maladie systématiquement chiffrés, sont mises à la disposition du personnel autorisé de l'environnement analytique SAS de l'ICIS. Il a aussi fallu recueillir des données additionnelles destinées précisément au RARP.

Ces données additionnelles sont acheminées directement à l'ICIS par les ministères de la Santé provinciaux et territoriaux. Les données soumises à l'ICIS sont systématiquement recueillies et conservées par les ministères de la Santé afin de répondre aux exigences de chaque province ou territoire (p. ex. pour la rémunération des médecins et pour améliorer la qualité de la planification et de la gestion de la prestation des services de soins de santé à la population canadienne). En raison du calendrier du projet, les fournisseurs de données n'auront pas à se conformer aux spécifications de l'ICIS relatives à la soumission de données. Chacun d'eux devra plutôt extraire les données à partir de ses sources de données existantes et les préparer pour la soumission selon les spécifications relatives à la soumission négociées par chaque province avec l'ICIS. Les données seront soumises à l'ICIS à l'aide d'applications Web sécurisées ou serveur à serveur.

Les fichiers de données destinés au projet RARP sont traités immédiatement après leur réception et le numéro d'assurance maladie provinciale ou territoriale de chaque fichier est chiffré. Une fois ce chiffrement effectué, un nombre limité d'employés autorisés procèdent au traitement secondaire des fichiers avant qu'ils soient transférés à la section du projet RARP dans l'environnement analytique SAS de l'ICIS.

Les analystes autorisés accèdent aux données utilisées dans le cadre du projet RARP dans l'environnement analytique SAS de l'ICIS. Toutes les demandes d'accès à la section du projet RARP sont traitées par le centre de services centralisé de l'ICIS. Ce processus permet d'assurer que toutes les demandes d'accès aux données du projet RARP sont vérifiables et autorisées.

Figure : Cheminement des données, Projet de regroupement ajusté selon les risques de la population



3 Analyse du respect de la vie privée

3.1 Textes législatifs régissant l'ICIS et l'utilisation des données dans le cadre du projet RARP

Généralités

L'ICIS se conforme à sa *Politique de respect de la vie privée de 2010* ainsi qu'à toute législation ou entente applicable dans ce domaine.

Législation

L'ICIS est un collecteur secondaire de renseignements personnels sur la santé, plus particulièrement à des fins de planification et de gestion du système de santé, y compris d'analyse statistique et de 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.

L'ensemble des provinces et territoires ont des lois sur la protection des renseignements personnels. Ces lois prévoient des mécanismes qui permettent aux organismes publics visés par la loi de divulguer des données identifiables, sans le consentement de la personne, à des fins statistiques. Terre-Neuve-et-Labrador, la Nouvelle-Écosse, le Nouveau-Brunswick, l'Ontario, le Manitoba, la Saskatchewan et l'Alberta disposent aussi de lois sur la protection des renseignements personnels sur la santé octroyant l'autorité légale expresse d'utiliser et de divulguer des renseignements personnels sur la santé sans le consentement de la personne à des fins de gestion du système de santé, y compris d'analyse statistique et de production de rapports.

L'ICIS est par exemple reconnu comme une entité désignée en vertu de la *Loi sur la protection des renseignements personnels sur la santé* de l'Ontario. Les dépositaires de renseignements en Ontario peuvent divulguer des renseignements personnels sur la santé à l'ICIS sans le consentement du patient conformément à l'article 29, comme le prévoit l'alinéa 45 (1) de la Loi.

Ententes

Comme l'indique l'article 2.2, les données sont transmises directement à l'ICIS par les ministères de la Santé responsables des régimes provinciaux et territoriaux d'assurance maladie. Le processus de cheminement de données, y compris certaines données recueillies uniquement aux fins de l'élaboration de la méthodologie de regroupement de la population, est régi par la *Politique de respect de la vie privée de 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 à l'ICIS, ainsi que toute divulgation subséquemment permise.

Les ententes décrivent aussi l'autorité législative selon laquelle les renseignements personnels sur la santé sont divulgués à l'ICIS. Le cas échéant, les ententes de partage de données existantes sont mises à jour ou des ententes distinctes sont conclues pour inclure la prestation de données utilisées dans le cadre du projet RARP à l'ICIS, et ce, avant la date de la soumission des données.

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

Le président-directeur général de l'ICIS est responsable de l'observation de la *Politique de respect de la vie privée de 2010* de l'ICIS. À cet égard, l'ICIS compte sur une chef de la protection des renseignements personnels et avocate générale, une équipe du respect de la vie privée, de la confidentialité et de la sécurité, un comité du Conseil d'administration sur le respect de la vie privée et la protection des données et un conseiller principal externe à la protection des renseignements personnels.

Organisation et gouvernance

La Division des groupes clients de l'ICIS détient la responsabilité complète des objectifs du projet et de ses produits livrables. D'autres divisions de l'ICIS contribueront à ce projet en

- facilitant le couplage de données à partir de multiples banques de données et de façon longitudinale;
- fournissant une expertise en matière d'utilisation et d'interprétation des données du projet qui sont déjà dans les banques de données de l'ICIS;
- participant aux efforts de collaboration avec les intervenants de l'ICIS afin d'obtenir des données additionnelles de manière à combler les lacunes en matière de données.

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

Poste	Rôles et responsabilités
Vice-président, Programmes	Responsable du fonctionnement général et de l'orientation stratégique du projet RARP
Directeur, Méthodologies et Soins spécialisés	Responsable de la prise de décisions stratégiques et opérationnelles concernant le projet RARP.
Gestionnaire, Groupes clients	Responsable de la gestion continue et de la mise en place du projet RARP, ainsi que de la prise de décisions opérationnelles quotidiennes relatives au projet RARP.
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

Groupe d'experts

Le groupe d'experts du RARP est composé de cadres supérieurs des ministères de la Santé et de chercheurs du domaine de la santé qui possèdent de l'expérience dans le domaine de l'élaboration ou de l'application de méthodologies de regroupement de la population. Le groupe formulera des commentaires sur l'élaboration de la méthodologie et veillera à ce qu'elle réponde aux besoins des organismes responsables de l'administration du système de santé et de l'analyse des politiques de santé. De plus, le groupe d'experts du projet RARP, composé de médecins et d'autres cliniciens, donnera des conseils sur la classification clinique.

3.3 Deuxième principe : Établissement des objectifs de la collecte de renseignements personnels sur la santé

Le projet RARP a pour but d'élaborer une méthodologie et un logiciel de regroupement de la population à l'aide des données et de l'expertise de l'ICIS. Le logiciel de regroupement aidera l'ICIS et ses clients à surveiller la santé de la population, à prévoir les tendances liées à l'utilisation des soins, à surveiller et à faire le suivi des maladies et à expliquer les variations en matière d'utilisation des ressources, en plus d'offrir un fondement aux modèles de financement. Il permettra également d'effectuer des comparaisons entre les provinces et territoires et fournira aux clients les fondements d'une normalisation exhaustive des populations dans le cadre d'analyses interprovinciales et interterritoriales.

Afin de faciliter le couplage des données à l'échelle des personnes entre de multiples banques de données et au fil du temps, le projet d'élaboration de la méthodologie de RARP regroupera des renseignements personnels sur la santé, notamment des identificateurs des patients comme les numéros d'assurance maladie provinciaux et les territoriaux. La collecte des identificateurs des patients, par exemple, permet à l'ICIS d'ajouter (c.-à-d. de coupler) l'information sur le projet RARP aux données déjà recueillies sur les interactions du patient avec le système de santé (p. ex. les données sur les séjours à l'hôpital recueillies dans la Base de données sur les congés des patients et le Système national d'information sur les soins ambulatoires).

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

Les ministères de la Santé fourniront les données destinées au projet RARP à l'ICIS afin d'élaborer la méthodologie de RARP. À titre de collecteur secondaire de données, l'ICIS ne communiquera pas directement avec les patients, les fournisseurs de services de santé ou les établissements qui fournissent aux ministères de la Santé des données destinées au RARP dans le cadre de ce projet. L'ICIS s'attend à ce que les fournisseurs de données respectent leurs rôles et responsabilités en matière de collecte, d'utilisation et de divulgation de données, y compris en ce qui concerne le consentement et les avis, tel que le prévoient les lois, les règlements et les politiques en vigueur dans les provinces et territoires.

3.5 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 de 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 du système de santé.

L'ICIS ne recueille que les renseignements personnels sur la santé nécessaires aux activités autorisées liées à l'analyse et à la qualité des données.

En plus de la collecte continue de données sur la santé ayant lieu à l'ICIS, l'ICIS peut de temps à autre entreprendre de nouvelles collectes de données sur la santé, soit pour un programme de travail continu, soit pour un projet particulier d'une durée limitée. Toute nouvelle collecte, dans l'un ou l'autre des cas, exige l'approbation du comité exécutif avant que ne commence la collecte.

En juin 2014, le Comité exécutif a approuvé la collecte de données destinées au RARP dans le cadre de ce projet (voir le tableau 1).

Le RARP est un projet de durée limitée qui nécessite la collecte de certaines données qui ne sont pas déjà intégrées dans le processus habituel de cheminement des données à l'ICIS. Les données destinées au RARP ont été déterminées et fournies à l'ICIS à la suite de négociations avec chaque province et territoire participant. Voici quelques exemples des renseignements personnels sur la santé et d'autres données qui peuvent être considérés comme étant de nature délicate du point de vue d'un patient pour chaque type de données destinées au RARP recueillies par l'ICIS.

- Les données sur la facturation des médecins à l'échelle des patients qui ne sont pas encore intégrées au processus habituel de cheminement des données vers le Répertoire sur la FMEP — L'Ontario et la Colombie-Britannique fourniront des données de leur province respective à l'échelle des patients sur les demandes de remboursement pour des services rémunérés à l'acte et sur les autres modes de paiement, à des fins d'utilisation dans le cadre

du projet RARP. Les données comprennent le numéro d'assurance maladie du patient, la date d'admission, les renseignements sur le service prodigué par le fournisseur et la demande de remboursement, la date d'évaluation, la date de service, le code de diagnostic, le code postal résidentiel, la date de naissance et le sexe.

- Les données des personnes inscrites de l'Ontario, de la Saskatchewan, de l'Alberta et de la Colombie-Britannique — Les données des personnes inscrites comprennent le numéro d'assurance maladie du patient, les dates de début et de fin de l'admissibilité, le code postal de la résidence, la date de naissance, le sexe et la date de décès pour toutes les personnes inscrites au régime d'assurance maladie de leur province respective.
- Le fichier de données longitudinales sur les patients et le fichier de données sur les coûts par patient des Services de santé de l'Alberta — Ces fichiers contiennent des données longitudinales sur les hôpitaux, les soins ambulatoires et les demandes de remboursement des médecins pour toutes les personnes inscrites au régime d'assurance maladie de l'Alberta, ainsi que les données sur les coûts pour chaque personne figurant dans le fichier de données longitudinales. Les données comprennent le numéro d'assurance maladie du patient, les dates de début et de fin de l'admissibilité, la date de naissance, le sexe et la date de décès.

L'annexe fait état de la justification de la collecte de certains éléments de données destinées au RARP qui pourrait présenter un risque accru d'identification directe ou indirecte d'une personne.

3.6 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 recueillies dans le cadre du projet RARP aux objectifs autorisés décrits à l'article 3.3, en vertu des ententes applicables. 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 et des produits livrables du projet. 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.

Comme indiqué à l'article 2.2, les numéros d'assurance maladie d'origine soumis à l'ICIS sont supprimés et remplacés par des numéros d'assurance maladie systématiquement chiffrés, et ce pour les données déjà détenues par l'ICIS et celles destinées précisément au RARP (les numéros d'assurance maladie d'origine sont supprimés et remplacés dès la réception des données). Depuis 2009, les fichiers de données utilisés à l'interne par l'ICIS à des fins d'analyse ne contiennent aucun identificateur, comme les numéros d'assurance maladie non chiffrés. Le personnel 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 et la *politique de respect de la vie privée de 2010* de l'ICIS.

Couplage de données

Les données destinées au RARP sont couplées à celles d'autres sources de données de l'ICIS. Afin d'atténuer les risques potentiels d'identification des personnes qui découlent du couplage des données, l'ICIS prendra les mesures qui suivent.

Les articles 14 à 31 de la *Politique de respect de la vie privée de 2010* de l'ICIS régissent le couplage des enregistrements contenant des renseignements personnels sur la santé. En vertu de cette politique, l'ICIS permet le couplage des renseignements personnels sur la santé dans certaines circonstances. Il est généralement permis de coupler des données au sein d'une seule banque de données pour l'usage exclusif de l'ICIS. Le couplage de données à partir de multiples banques de données pour l'usage exclusif de l'ICIS et toutes les demandes de couplage de données formulées par des tiers sont soumis à un processus d'examen et d'approbation interne. Lors du couplage de données, 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 de 2010*.

Les critères d'approbation du couplage de données sont énoncés comme suit à l'article 24 de la *Politique de respect de la vie privée de 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.

L'article 28 de la *Politique de respect de la vie privée de 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 de 2010* de l'ICIS prévoit également que la destruction sécuritaire des données couplées ait 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. Dans le cas des données couplées dans le cadre d'un programme de travail continu de l'ICIS, 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.

En avril 2013, l'équipe chargée du respect de la vie privée, de la confidentialité et de la sécurité de l'ICIS a autorisé, dans le contexte du projet RARP, le couplage de données à l'aide de numéros d'assurance maladie chiffrés dans le cadre d'un programme de travail continu.

Renvoi des données au fournisseur de données

L'article 34 de la *Politique de respect de la vie privée de 2010* de l'ICIS stipule que le renvoi des données au ministère de la Santé qui les avait fournies à l'ICIS ne constitue pas un acte de divulgation, mais bien une utilisation de données. L'ICIS peut renvoyer les données utilisées dans le cadre du projet RARP au moyen des services électroniques en ligne ou d'une autre méthode approuvée par l'ICIS.

Restriction de la divulgation

Diffusion publique des données du projet RARP

Puisque le projet RARP a pour but l'élaboration de la méthodologie de regroupement, du logiciel SAS qui appliquera la méthodologie de regroupement de la population et de la documentation connexe, la publication des données utilisées pour l'élaboration de la méthodologie dans le cadre du projet RARP est peu probable. Si l'ICIS devait diffuser des données, il s'agirait de données agrégées afin de réduire au minimum le risque d'identification et de divulgation par recoupements conformément à la *Politique de respect de la vie privée de 2010* de l'ICIS. En général, il faut un regroupement d'au moins 5 observations par cellule.

Restriction de la conservation

L'ICIS conservera les données destinées au RARP aussi longtemps que nécessaire pour la réalisation des fins déterminées, conformément aux ententes et aux échéances de conservation, après quoi elles seront détruites dans le respect des règles énoncées aux articles 28 et 29.

3.7 Sixième principe : Exactitude des renseignements personnels sur la santé

Conformément à la politique d'évaluation du cadre de la qualité des données de l'ICIS, les sources de données internes de l'ICIS utilisées pour le RARP sont soumises à une évaluation régulière de la qualité des données, comme l'exige le *Cadre de la qualité de l'information de l'ICIS* de l'ICIS. Ce processus comprend de nombreuses activités visant à évaluer les diverses dimensions de la qualité, dont l'exactitude des données de l'ICIS.

Compte tenu de la durée limitée du projet, les données destinées au RARP utilisées par l'ICIS seront acceptées telles que fournies par chaque fournisseur de données et feront l'objet d'une évaluation limitée de la qualité selon les exigences du projet.

3.8 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* en vue d'offrir une approche globale de gestion du respect de la vie privée et de la sécurité. Fondé sur les pratiques exemplaires qui prévalent 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 principaux aspects de la sécurité des systèmes de l'ICIS qui revêtent une importance particulière au regard du projet RARP.

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 un ensemble complet de politiques qui précise 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. 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 effectue ses analyses à l'aide de données dépersonnalisées au niveau de l'enregistrement, où le numéro d'assurance maladie a été supprimé ou chiffré. Exceptionnellement, le personnel doit avoir accès aux numéros d'assurance maladie d'origine. L'article 10 des procédures et de la *politique de respect de la vie privée de 2010* de l'ICIS prévoit des contrôles stricts qui garantissent que l'accès est approuvé 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 renseignements personnels sur la santé :

- 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 autorisations 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 renseignements de nature délicate 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 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 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.

3.9 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 de 2010* de l'ICIS sont accessibles au public sur son site Web (*www.icis.ca*).

3.10 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 à la santé au sujet des 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 de 2010* de l'ICIS.

3.11 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 de 2010* de l'ICIS, les plaintes concernant le traitement par l'ICIS des renseignements personnels sur la santé sont examinées par la chef de la protection des renseignements personnels. Cette dernière 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 Résumé de l'évaluation des incidences sur la vie privée et conclusion

Aucune recommandation n'a été formulée jusqu'ici. Les risques de violation de la vie privée décelés dans le cadre de la présente évaluation des incidences sur la vie privée ont été atténués. L'évaluation sera mise à jour ou révisée conformément à la *Politique d'évaluation des incidences sur la vie privée de l'ICIS*.

Annexe A : Risque d'identification selon la province ou le territoire

Les tableaux qui suivent décrivent les éléments de données provinciaux ou territoriaux qui pourraient présenter un risque accru d'identification directe ou indirecte d'une personne. Ils présentent également la définition de ces éléments de données et la justification de leur collecte.

Tableau A1: Données sur la facturation des médecins à l'échelle des patients qui ne sont pas encore incluses dans le Répertoire sur la FMEP de l'ICIS

Élément de données et justification de la collecte/commentaires	Ontario	Colombie-Britannique
Identificateur du patient : Numéro d'assurance maladie du patient **Justification :** Utilisé pour le couplage des données avec d'autres bases de données de l'ICIS, afin de brosser un portrait global du profil clinique de chaque patient	X	X
Code postal du patient : Code postal complet du domicile du patient **Justification :** Utilisé pour l'analyse géographique du lieu de prestation des services par rapport au lieu de résidence du patient et pour associer des mesures spatiales tirées du recensement ou d'autres sources	X	X
Sexe : Sexe du patient **Justification :** Utilisé pour la répartition des patients selon le sexe dans les analyses	X	X
Indicateur du lieu de prestation des services : Le code postal complet n'est indiqué que si le lieu de prestation des services est le domicile du patient **Justification :** Utilisé pour l'analyse géographique du lieu de prestation des services en comparaison du lieu de résidence du patient	X	X

Remarque

X L'élément de données est recueilli par la province.

Tableau A2: Données des personnes inscrites

Élément de données et justification de la collecte/commentaires	Ontario	Saskatchewan	Alberta	Colombie-Britannique
Identificateur du patient : Numéro d'assurance maladie du patient **Justification :** Utilisé pour le couplage des données avec d'autres bases de données de l'ICIS, afin de brosser un portrait global du profil clinique de chaque patient	X	X	X	X
Code postal du domicile du patient : Code postal complet du domicile du patient **Justification :** Utilisé pour l'analyse géographique du lieu de prestation des services par rapport au lieu de résidence du patient et pour associer des mesures spatiales tirées du recensement ou d'autres sources	X	X	X	X
Sexe : Sexe du patient **Justification :** Utilisé pour la répartition selon le sexe dans les analyses	X	X	X	X

Élément de données et justification de la collecte/commentaires	Ontario	Saskatchewan	Alberta	Colombie-Britannique
Date de décès du patient : Date de décès (le cas échéant) **Justification :** La date de décès du patient (le cas échéant) sert à établir un modèle de coûts au cours de la dernière année de vie. Comme la dernière année de vie est souvent très coûteuse, il est important de connaître la date du décès. La date exacte du décès permet d'établir un modèle de coûts à partir du nombre de mois de vie dans un exercice donné.	X	X	X	X

Remarque

X L'élément de données est recueilli par la province.

Tableau A3: Fichier de données longitudinales sur les patients et fichier de données sur les coûts par patient de l'Alberta Health Services

Élément de données et justification de la collecte/commentaires
Identificateur du patient : Numéro d'assurance maladie du patient **Justification :** Utilisé pour le couplage des données avec d'autres bases de données de l'ICIS, afin de brosser un portrait global du profil clinique de chaque patient
Code postal du domicile du patient : Code postal complet du domicile du patient **Justification :** Utilisé pour l'analyse géographique du lieu de prestation des services par rapport au lieu de résidence du patient et pour associer des mesures spatiales tirées du recensement ou d'autres sources
Sexe : Sexe du patient **Justification :** Utilisé pour la répartition des patients selon le sexe dans les analyses

Annexe B : Texte de remplacement pour la figure

Texte de remplacement pour la figure Cheminement des données, Projet de regroupement ajusté selon les risques de la population

Cette figure montre le cheminement général des données du projet RARP.

La plupart des données utilisées dans le cadre du projet RARP proviennent directement des banques de données internes de l'ICIS (Répertoire sur la FMEP, BDCP, SNISA, SISLD et BDCCP). D'autres données destinées au RARP sont soumises directement à l'ICIS par les ministères de la Santé provinciaux et territoriaux à l'aide d'applications Web sécurisées ou serveur à serveur.

Les numéros d'assurance maladie originaux contenus dans les données au niveau de l'enregistrement des 2 sources sont chiffrés et versés dans l'environnement analytique SAS de l'ICIS. Le personnel autorisé de l'ICIS peut y accéder en cas de nécessité.

L'équipe du projet RARP transmet des rapports personnalisés agrégés ou au niveau de l'enregistrement aux ministères de la Santé, et diffuse certaines statistiques agrégées et analyses à des tiers.

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

Tous droits réservés.

Le contenu de cette publication peut être reproduit tel quel, en tout ou en partie et par quelque moyen que ce soit, uniquement à des fins non commerciales pourvu que l'Institut canadien d'information sur la santé soit clairement identifié comme le titulaire du droit d'auteur. Toute reproduction ou utilisation de cette publication et de son contenu à des fins commerciales requiert l'autorisation écrite préalable de l'Institut canadien d'information sur la santé. La reproduction ou l'utilisation de cette publication ou de son contenu qui sous-entend le consentement de l'Institut canadien d'information sur la santé, ou toute affiliation avec celui-ci, est interdite.

Pour obtenir une autorisation ou des renseignements, veuillez contacter l'ICIS :

Institut canadien d'information sur la santé
495, chemin Richmond, bureau 600
Ottawa (Ontario) K2A 4H6

Téléphone : 613-241-7860
Télécopieur : 613-241-8120
www.icis.ca
droitdauteur@icis.ca

© 2015 Institut canadien d'information sur la santé

This publication is also available in English under the title *Population Risk Adjustment Grouping Project Privacy Impact Assessment, January 2015*.

Parlez-nous

ICIS Ottawa
495, rue Richmond, bureau 600
Ottawa (Ontario) K2A 4H6
Téléphone : 613-241-7860

ICIS Toronto
4110, rue Yonge, bureau 300
Toronto (Ontario) M2P 2B7
Téléphone : 416-481-2002

ICIS Victoria
880, rue Douglas, bureau 600
Victoria (Colombie-Britannique) V8W 2B7
Téléphone : 250-220-4100

ICIS Montréal
1010, rue Sherbrooke Ouest, bureau 300
Montréal (Québec) H3A 2R7
Téléphone : 514-842-2226

ICIS St. John's
140, rue Water, bureau 701
St. John's (Terre-Neuve-et-Labrador) A1C 6H6
Téléphone : 709-576-7006

23436-1220

www.icis.ca
Au cœur des données

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