



Registre canadien des insuffisances et des transplantations d'organes

Évaluation des incidences
sur la vie privée

Septembre 2023



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

© 2023 Institut canadien d'information sur la santé

Comment citer ce document :

Institut canadien d'information sur la santé. *Registre canadien des insuffisances et des transplantations d'organes : évaluation des incidences sur la vie privée, septembre 2023*. Ottawa, ON : ICIS; 2023.

This publication is also available in English under the title *Canadian Organ Replacement Register Privacy Impact Assessment, September 2023*

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*](#) :

- *Registre canadien des insuffisances et des transplantations d'organes : évaluation des incidences sur la vie privée, septembre 2023*

Approuvé par

Brent Diverty
Vice-président, Stratégies de données et Statistiques

Rhonda Wing
Directrice exécutive, chef de la protection des renseignements personnels et avocate générale, Bureau de la chef de la protection des renseignements personnels et des services juridiques

Ottawa, septembre 2023

Table des matières

Le Registre canadien des insuffisances et des transplantations d'organes en bref	5
Définitions	6
1. Introduction	7
2 Contexte.	7
2.1 Présentation du RCITO.	7
2.2 Collecte de données	8
2.3 Gestion de l'accès et cheminement des données du RCITO	10
3 Analyse du respect de la vie privée	14
3.1 Programme de gestion des risques liés au respect de la vie privée et à la sécurité	14
3.2 Autorités régissant les données du RCITO	15
3.3 Premier principe : responsabilité à l'égard des renseignements personnels sur la santé	16
3.4 Deuxième principe : établissement des objectifs de la collecte de renseignements personnels sur la santé	17
3.5 Troisième principe : consentement pour la collecte, l'utilisation ou la divulgence de renseignements personnels sur la santé	20
3.6 Quatrième principe : restriction de la collecte de renseignements personnels sur la santé	20
3.7 Cinquième principe : restriction de l'utilisation, de la divulgation et de la conservation des renseignements personnels sur la santé	21
3.8 Sixième principe : exactitude des renseignements personnels sur la santé	27
3.9 Septième principe : mesures de protection des renseignements personnels sur la santé	28
3.10 Huitième principe : transparence de la gestion des renseignements personnels sur la santé	29
3.11 Neuvième principe : accès individuel aux renseignements personnels sur la santé et modification de ceux-ci	30
3.12 Dixième principe : plaintes concernant le traitement par l'ICIS des renseignements personnels sur la santé.	30
4 Conclusion	30

Le Registre canadien des insuffisances et des transplantations d'organes en bref

- Le Registre canadien des insuffisances et des transplantations d'organes (RCITO), administré par l'Institut canadien d'information sur la santé (ICIS), est un registre pancanadien qui recueille des données sur les patients qui reçoivent des traitements au stade terminal de l'insuffisance organique (dialyse ou transplantation) et sur les donneurs vivants et décédés au Canada. À ses débuts en 1972, le RCITO était un registre des insuffisances rénales; son premier rapport a été produit en 1974. La portée de ses données a été étendue aux transplantations autres que rénales en 1988. Il s'agit d'une base de données longitudinale qui suit les patients de leur premier traitement pour insuffisance organique au stade terminal jusqu'à leur décès ou, rarement, jusqu'à l'arrêt des suivis.
- L'objectif du RCITO est de fournir des données pancanadiennes sur les remplacements d'organes vitaux au Canada, en vue d'améliorer les traitements et les soins aux patients ainsi que de faciliter la recherche.
- Le RCITO contient des données au niveau de l'enregistrement — y compris des identificateurs personnels et des renseignements personnels sur la santé — sur 4 types de personnes : les patients en dialyse au stade terminal de l'insuffisance rénale, les receveurs d'une transplantation (rein, foie, cœur, poumon/cœur-poumon, pancréas et îlots pancréatiques, intestins), les donneurs vivants et les donneurs décédés.
- Le RCITO reçoit des données provenant directement de 335 centres de dialyse, 25 centres de transplantation et 12 organismes de don d'organes participants (en date d'août 2022).
- Le RCITO est administré par l'ICIS, qui reçoit des conseils stratégiques et des directives du conseil d'administration du RCITO, une entité externe indépendante, directement ou par l'intermédiaire de groupes de travail. Le conseil d'administration compte des représentants de la Société canadienne de transplantation, de la Société canadienne de néphrologie, de la Société canadienne du sang et de la Fondation canadienne du rein.

Définitions

Les définitions suivantes s'appliquent aux termes utilisés dans la présente évaluation des incidences sur la vie privée :

Données agrégées : données compilées à partir des enregistrements et agrégées à un niveau qui garantit que l'identité des personnes ne pourra pas être établie selon des méthodes raisonnablement prévisibles. Les données agrégées dont la valeur des cellules est inférieure à 5 peuvent être considérées comme des données dépersonnalisées ou des renseignements personnels sur la santé.

Données au niveau de l'enregistrement : données dont chaque enregistrement est relié à une seule personne (parfois appelées microdonnées).

Données des fournisseurs : données du RCITO qui ont été initialement soumises à l'ICIS par un fournisseur de données.

Données du Registre canadien des insuffisances et des transplantations d'organes : toutes les données agrégées et au niveau de l'enregistrement recueillies à l'aide du système du RCITO et enregistrées dans ce système.

Fournisseur de données : tout ministère ou organisme gouvernemental, autorité sanitaire régionale, établissement de soins de santé, établissement public ou privé ou organisme qui soumet des données.

Renseignements identifiant un établissement de santé : toute information qui identifie directement un établissement de santé par son nom.

1 Introduction

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

La présente évaluation des incidences sur la vie privée a pour objet d'examiner les risques liés au respect de la vie privée, à la confidentialité et à la sécurité associés au Registre canadien des insuffisances et des transplantations d'organes (RCITO). Elle remplace la version de juillet 2017 et consiste en un examen des 10 principes énoncés dans le *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation et de la façon dont ils s'appliquent au RCITO. Elle se penche également sur l'application du [*Cadre de gestion des risques liés au respect de la vie privée et à la sécurité*](#) de l'ICIS.

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

2 Contexte

2.1 Présentation du RCITO

Administré par l'ICIS, le RCITO est une base de données pancanadienne sur les patients qui reçoivent des traitements au stade terminal de l'insuffisance organique (dialyse ou transplantation) et sur les donneurs d'organes vivants et décédés au Canada. Cette base de données longitudinale suit les patients de leur premier traitement pour insuffisance organique au stade terminal jusqu'à leur décès ou, rarement, jusqu'à l'arrêt des suivis. À l'aide du RCITO, l'ICIS fournit de l'information sur les remplacements d'organes vitaux à l'échelle du Canada, en vue d'améliorer les traitements et les soins aux patients ainsi que de faciliter la recherche.

Créé en 1972, le RCITO était alors la première base de données sur les insuffisances rénales au Canada, dirigée par le D^r Arthur Shimizu. En 1973, la gestion de la base de données a été transférée à Statistique Canada, avec la collaboration de la Fondation canadienne du

rein. En 1987, avec le soutien du Comité consultatif fédéral-provincial des services médicaux et des services en établissement, on élargit la base de données dans le but d'intégrer les données sur les transplantations autres que rénales. Cette base de données étendue était à l'origine tenue à jour par le Hospital Medical Records Institute (HMRI). En 1995, le HMRI a été intégré à l'ICIS, qui s'est alors vu confier la responsabilité du RCITO.

Le nombre de transplantations d'organes pleins réalisées au Canada continue de croître, et depuis la création de la base de données, les techniques de transplantation de même que les soins préopératoires et postopératoires ont beaucoup évolué. Les demandes d'accès aux données du RCITO provenant de responsables des politiques, de gestionnaires des systèmes de santé et de chercheurs au Canada augmentent également.

2.2 Collecte de données

Chaque enregistrement soumis au RCITO respecte les exigences du fichier minimal et comprend des identificateurs personnels, des renseignements démographiques, des données sur les caractéristiques de santé, des données administratives et des identificateurs de l'établissement de soins de santé. De plus amples renseignements sur les éléments de données du fichier minimal du RCITO sont accessibles sur le [site Web de l'ICIS](#).

Le RCITO contient des données au niveau de l'enregistrement — y compris des identificateurs personnels et des renseignements personnels sur la santé — sur 4 types de personnes : les patients en dialyse au stade terminal de l'insuffisance rénale, les receveurs d'une transplantation (rein, foie, cœur, poumon/cœur-poumon, pancréas et îlots pancréatiques, intestins), les donneurs vivants et les donneurs décédés.

Actuellement, le RCITO ne reçoit pas de données sur les patients en attente d'une transplantation. Des données agrégées sur les patients en attente d'une transplantation (y compris le nombre de patients décédés pendant l'attente) et le nombre de donneurs sont fournis annuellement par les organismes de dons d'organes. Cette information supplémentaire est conservée séparément du RCITO et sert à bonifier les rapports sur les transplantations et les donneurs.

Le tableau 1 résume les différents éléments de données du RCITO qui concernent l'information sur les personnes. Le but de la collecte de ces données, y compris les identificateurs directs et les renseignements personnels sur la santé, est expliqué à la [section 3.4](#). Le cheminement sécurisé des données jusqu'à l'ICIS et le traitement qui s'ensuit au sein de l'organisme sont décrits à la [section 2.3](#).

Tableau 1 Éléments de données recueillis sur les personnes, selon le type de personnes

Élément de données	Type de personnes			
	Patients en dialyse	Receveurs d'une transplantation d'organe	Donneurs d'organes vivants	Donneurs d'organes décédés
Province de résidence	O	O	O	O
Code postal	O	O	N	N
Date de naissance	O	O	N (âge seulement)	N (âge seulement)
Sexe	O	O	O	O
Nom	O (nom complet)	O (nom complet)	O (nom partiel)	O (nom partiel)
Numéro d'assurance maladie	O	O	N	N
Groupe sanguin	N	O	O	O
Race	O	O	O	O
Taille	O	O	O	O
Poids	O	O	O	O
Décès	• Cause du décès	• Cause du décès	• Sans objet	• Province de décès • Cause du décès
Information clinique	• Information pré-dialyse • Diagnostic • Traitement • Facteurs de risque • Information sur l'arrêt du traitement • Information sur le suivi	• Information sur la transplantation • Diagnostic • Temps d'attente • Facteurs de risque • Statut sérologique • Résultats • Information sur le suivi post-transplantation • Information sur la tumeur (foie seulement)	• Information sur l'hôpital • Sérologie • Facteurs de risque • Information spécifique sur les organes	• Sérologie • Facteurs de risque • Information spécifique sur les organes

Remarques

O : Oui, l'information est recueillie, partiellement recueillie ou convertie.

N : Non, l'information n'est pas recueillie.

2.3 Gestion de l'accès et cheminement des données du RCITO

Les fournisseurs de données peuvent utiliser 2 méthodes pour soumettre des données électroniques au RCITO de façon sécurisée : par le Service de soumission électronique de données (eDSS) de l'ICIS et par l'application de formulaires Web du RCITO. Les 2 systèmes sont hébergés dans l'environnement sécurisé de l'ICIS, et tous les utilisateurs doivent être authentifiés dans le système de gestion de l'accès (SGA) de l'ICIS.

Il y a une exception aux méthodes de soumission de données du RCITO : un établissement en Nouvelle-Écosse a autorisé le personnel du RCITO à créer un profil d'utilisateur afin d'accéder à l'environnement sécurisé de l'établissement. Comme lors de la soumission de données au moyen de l'eDSS de l'ICIS, le personnel du RCITO doit s'authentifier en ouvrant une session à l'aide d'un nom d'utilisateur et d'un mot de passe pour accéder à l'environnement sécurisé de l'établissement, puis extraire les enregistrements du RCITO en format PDF préparés par l'établissement. Ensuite, il entre les données sous forme d'enregistrements uniques selon la méthode décrite au paragraphe sur l'[application de formulaires Web du RCITO](#), ci-dessous.

Gestion de l'accès

L'accès aux applications sécurisées de l'ICIS est régi par la Division de la gestion de produits et de l'expérience client de l'ICIS. Cette division gère l'autorisation et la révocation de l'accès aux applications sécurisées de l'ICIS conformément aux processus établis du SGA.

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

Accès à l'application de formulaires Web du RCITO

La Division de la gestion de produits et de l'expérience client de l'ICIS gère les autorisations d'accès conformément aux processus d'autorisation et de révocation d'accès du SGA. Le processus d'autorisation de l'accès à l'outil Web de saisie de données du RCITO résulte de l'effort coordonné de cette Division, des fournisseurs de données (les « clients ») et de l'équipe du RCITO. Un contrôle d'accès en fonction du type d'utilisateur est utilisé pour limiter l'accès aux utilisateurs autorisés. Le RCITO dispose d'un rôle d'utilisateur externe, qui permet aux utilisateurs de soumettre et de modifier leurs propres données seulement.

Cheminement des données

L'ICIS est un collecteur secondaire de données qui compte sur la soumission de données par les centres de dialyse, les agences provinciales de transplantations rénales, les centres de transplantation et les organismes de dons d'organes (pour obtenir la liste des centres qui participent au RCITO, consultez le [Répertoire du Registre canadien des insuffisances et des transplantations d'organes](#)).

Service de soumission électronique de données

Le RCITO accepte les données soumises électroniquement au moyen de l'eDSS sécurisé de l'ICIS. L'eDSS permet aux fournisseurs de données de soumettre leurs fichiers dans divers formats. Pour le RCITO, les centres participants peuvent soumettre les fichiers de données dans un format conforme aux spécifications techniques de l'application de soumission de fichiers électroniques du RCITO ou dans un format de fichier non conforme (fichier Microsoft Excel). Les fichiers conformes soumis au moyen de l'eDSS sont automatiquement reçus dans l'application, puis transmis au système du RCITO dans l'environnement de production. Les fichiers non conformes sont conservés de façon sécuritaire sur le réseau de l'ICIS conformément à la norme relative au stockage sécuritaire de l'information de l'ICIS; seul le personnel autorisé par le gestionnaire du RCITO et la directrice des Services d'information sur les soins ambulatoires et de courte durée de l'ICIS peut les consulter. Les fichiers non conformes sont entrés manuellement par le personnel autorisé du RCITO dans l'environnement de production du RCITO. Ces fichiers sont conservés 5 ans, puis détruits conformément à la norme de destruction sécuritaire de l'ICIS.

Application de formulaires Web du RCITO

L'application de formulaires Web du RCITO offre un environnement Web sécurisé qui permet aux fournisseurs autorisés d'entrer des données en ligne et de les soumettre directement à l'ICIS. Les fournisseurs de données peuvent saisir et sauvegarder des enregistrements partiels ou complets; au moment de la soumission, ils peuvent aussi imprimer une copie des enregistrements qu'ils ont saisis dans l'outil. Une fois la soumission effectuée, les seuls enregistrements que les fournisseurs de données peuvent consulter sont ceux qui leur sont retournés à des fins de correction. Les utilisateurs autorisés n'ont pas accès aux enregistrements partiels soumis par un autre utilisateur, même si ce dernier provient du même établissement qu'eux.

Dans l'application de formulaires Web du RCITO, les utilisateurs soumettent des enregistrements uniques, et chaque enregistrement fait l'objet d'un contrôle visuel de la qualité des données par le personnel du RCITO à même l'application. **Les enregistrements relatifs aux donneurs et aux transplantations** jugés conformes lors du contrôle visuel de la qualité des données sont entrés par le personnel du RCITO dans l'environnement

de production du RCITO. **Les enregistrements de dialyse** jugés conformes lors du contrôle visuel de la qualité des données sont regroupés, traités dans l'application de soumission de fichiers électroniques du RCITO, puis ajoutés dans l'environnement de production du RCITO.

Traitement dans l'environnement de production

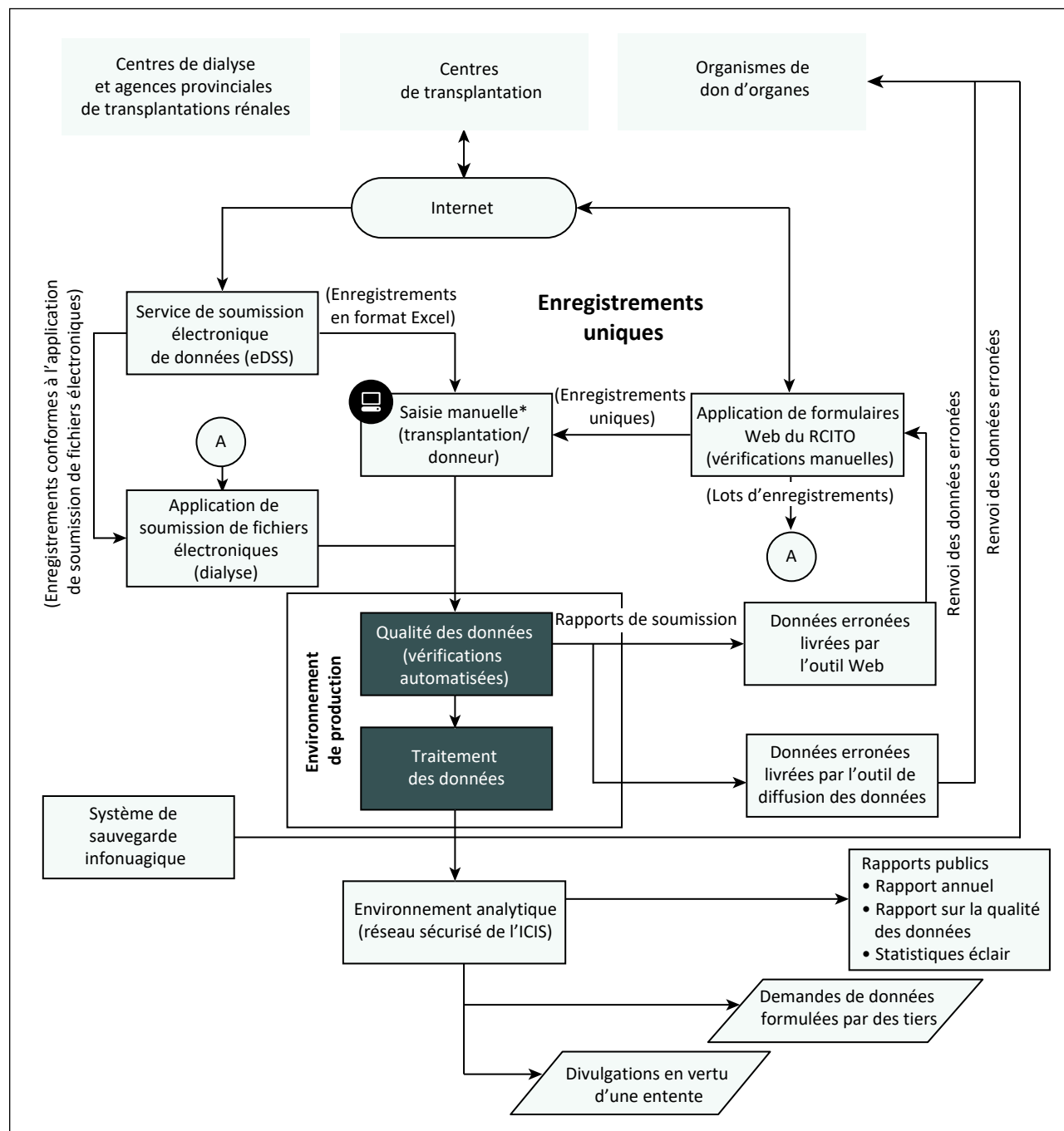
Les enregistrements qui passent par l'environnement de production du RCITO sont soumis à un processus automatisé de traitement des données en 2 étapes avant d'être versés dans l'environnement analytique du RCITO. La première étape consiste à repérer les problèmes de qualité des données; les erreurs, omissions, incohérences ou les enregistrements incomplets sont signalés. Le système du RCITO génère automatiquement un rapport de soumission, et les enregistrements sont retournés aux fournisseurs de données afin d'être corrigés et soumis de nouveau. Si un suivi des corrections est nécessaire, le personnel du RCITO l'effectue conformément à la norme relative au transfert sécuritaire de l'information de l'ICIS (p. ex. par téléphone, par courriel ou au moyen de l'outil sécurisé de diffusion des données de l'ICIS).

La seconde étape du traitement des données consiste à supprimer les identificateurs personnels des enregistrements, notamment les noms et les numéros d'assurance maladie (NAM) non chiffrés. Ces identificateurs sont conservés dans un dossier distinct à accès restreint dans l'environnement analytique du RCITO et non dans sa base de données principale. Le personnel autorisé de l'ICIS peut accéder à la base de données principale et aux dossiers à accès restreint uniquement sur approbation et en cas de nécessité. Cet accès est d'une durée limitée et ne peut être accordé que sur approbation écrite du gestionnaire du RCITO et de la directrice des Services d'information sur les soins ambulatoires et de courte durée.

Des copies des données du RCITO sont conservées dans un système de sauvegarde infonuagique.

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

Figure Cheminement des données du RCITO



Remarques

* Pour un établissement de la Nouvelle-Écosse, un membre du personnel du RCITO doit ouvrir une session dans l'environnement sécurisé de l'établissement, puis extraire les enregistrements en format PDF.

Les enregistrements sont ensuite saisis manuellement dans le système du RCITO.

A : Les enregistrements de dialyse saisis au moyen du formulaire Web du RCITO font l'objet de vérifications manuelles, puis sont regroupés et traités dans l'application de soumission de fichiers électroniques du RCITO.

3 Analyse du respect de la vie privée

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

La gestion des risques en matière de respect de la vie privée et de sécurité est un processus officiel et reproductible qui vise la détection, l'évaluation, la prise en charge et la surveillance des risques dans le but de réduire au minimum la probabilité qu'ils se matérialisent ou leurs éventuelles incidences. L'ICIS a mis en œuvre son [Cadre de gestion des risques liés au respect de la vie privée et à la sécurité](#) et la [Politique sur la gestion des risques liés au respect de la vie privée et à la sécurité](#) connexe. La chef de la protection des renseignements personnels et avocate générale, ainsi que le chef de la sécurité de l'information de l'ICIS, en collaboration avec des membres de la direction, ont la responsabilité de détecter, d'évaluer, de prendre en charge, de surveiller et d'examiner les risques en matière de respect de la vie privée et de sécurité.

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

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

Le niveau de risque est calculé en fonction de la probabilité et de l'incidence du risque détecté. La cote de niveau de risque (faible, moyen ou élevé) définit le degré de risque. Un niveau de risque élevé est signe d'une menace grave qu'il est impératif de prendre immédiatement en charge. Une fois le risque initial pris en charge, le risque résiduel (nouveau calcul de la probabilité et de l'incidence du risque par suite du traitement) est évalué en fonction de l'énoncé sur la tolérance à l'égard des risques liés au respect de la vie privée et à la sécurité de l'ICIS, qui stipule que l'ICIS a une faible tolérance à de tels risques. Si le niveau de risque résiduel demeure plus élevé que faible, de nouvelles mesures de prise en charge doivent être mises en œuvre jusqu'à l'obtention d'un risque faible, ou jusqu'à ce que le risque non pris en charge ou résiduel soit accepté par le Comité exécutif de l'ICIS au nom de l'organisme.

Aucun risque lié au respect de la vie privée et à la sécurité n'a été détecté à la suite de cette évaluation des incidences sur la vie privée.

3.2 Autorités régissant les données du RCITO

Généralités

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

Lois sur la protection de la vie privée

L'ICIS est un collecteur secondaire de données sur la santé, particulièrement à des fins de planification et de gestion des systèmes de santé du Canada, ce qui comprend l'analyse statistique et la production de rapports. Il incombe aux fournisseurs de données de respecter les obligations légales de leur 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, sous réserve de certaines conditions. Par exemple, l'ICIS étant reconnu comme une entité prescrite en vertu de la *Loi sur la protection des renseignements personnels sur la santé* de l'Ontario, les dépositaires de renseignements sur la santé de l'Ontario peuvent divulguer de tels renseignements à l'ICIS sans le consentement des patients en vertu de l'article 29, comme le prévoit le paragraphe 45(1) de la Loi.

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

Ententes

À l'ICIS, les données du RCITO 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 fournis à l'ICIS, ainsi que toute divulgation subséquemment permise. Les ententes décrivent aussi l'autorité législative en vertu de laquelle les renseignements personnels sur la santé sont divulgués à l'ICIS.

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

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

Organisation et gouvernance

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

Tableau 2 Principaux postes et responsabilités

Poste et groupe	Rôles et responsabilités
Vice-président, Stratégies de données et Statistiques	Responsable du leadership et de la supervision en matière d'acquisition, de gestion et de diffusion des données du RCITO.
Directrice, Services d'information sur les soins ambulatoires et de courte durée	Responsable de la prise de décisions stratégiques et opérationnelles concernant le RCITO. Veille au développement continu du RCITO et gère les relations stratégiques avec le conseil d'administration du RCITO et les autres intervenants.
Gestionnaire, RCITO et projet relatif aux dons d'organes et aux transplantations (DOT)	Responsable de la gestion continue, du développement et de la diffusion du RCITO. Prend les décisions opérationnelles concernant le RCITO, appuie le conseil d'administration du RCITO et consulte ses collègues à l'interne ainsi que les clients du RCITO, au besoin.
Chef de section, RCITO	Responsable de la coordination des activités opérationnelles et analytiques liées au fonctionnement du RCITO et agit à titre de personne-ressource principale pour les intervenants. Voit à la livraison rapide des résultats et des services qui répondent aux exigences des utilisateurs et de l'organisme.
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

Poste et groupe	Rôles et responsabilités
Gestionnaire, Applications de gestion de l'information sur la santé, STI	Responsable de la disponibilité des ressources et solutions techniques nécessaires à l'exploitation et à l'amélioration continues des données du RCITO.
Gestionnaire, Gestion de produits et Expérience client	Responsable de la gestion de l'accès aux applications en ligne de l'ICIS, comme le RCITO.

Conseil d'administration du RCITO

L'ICIS gère la banque de données du RCITO et reçoit des conseils stratégiques et des directives du conseil d'administration du RCITO, une entité externe indépendante. Ce conseil d'administration a été constitué dans le but de fournir une orientation et des conseils stratégiques au sujet de la base de données, notamment en ce qui a trait aux éléments de données à recueillir. Il est composé des représentants de la Société canadienne de transplantation, de la Société canadienne de néphrologie, de la Société canadienne du sang et de la Fondation canadienne du rein.

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

L'ICIS a pour mandat de fournir une information comparable et exploitable qui favorise une amélioration rapide des soins de santé, de la performance des systèmes de santé et de la santé de la population dans l'ensemble du continuum des soins. Pour ce faire, l'ICIS recueille les types de données suivants dans le RCITO aux fins indiquées à la [section 2.1](#).

Identificateurs uniques

Le RCITO est une base de données longitudinale qui effectue le couplage des données à l'aide des identificateurs uniques ci-dessous, lesquels sont générés par le système du RCITO ou encore par les systèmes d'information sur la santé des fournisseurs de données, puis soumis au RCITO. Ce couplage sert entre autres à ajouter des enregistrements aux données existantes sur les patients, notamment pour assurer le suivi des patients depuis leur traitement initial au stade terminal de l'insuffisance organique (dialyse ou transplantation) jusqu'à leur décès.

Identificateurs d'enregistrement

Chaque enregistrement soumis au moyen d'un fichier électronique est associé à un identificateur unique généré par les fournisseurs de données. Tout enregistrement soumis par l'application de formulaires Web du RCITO est associé à un identificateur unique généré par l'outil en ligne. Les identificateurs d'enregistrement servent à identifier les enregistrements aux fins de correction. Les patients peuvent être associés à plusieurs identificateurs d'enregistrement.

Identificateurs du receveur

En tant que base de données longitudinale, le RCITO attribue un numéro d'identification du receveur et un numéro d'identification de traitement du receveur au moment de l'inscription. Pour les enregistrements subséquents, le RCITO utilise ces identificateurs uniques comme suit :

- Numéro d'identification du receveur : sert à identifier les receveurs de façon unique en associant le nom, le numéro d'assurance maladie et la date de naissance du patient.
- Numéro d'identification de traitement du receveur : utilisé en conjonction avec le numéro d'identification du receveur pour regrouper les traitements associés à chaque receveur.

Identificateurs personnels du patient

Ces identificateurs permettent à l'ICIS de regrouper les enregistrements décrivant les divers types de soins qui lui ont été fournis à divers moments par divers établissements. Il peut s'agir, par exemple, du numéro d'assurance maladie ou du numéro d'identification du donneur attribué par le programme de prélèvement. En raison du besoin particulier d'effectuer un suivi à long terme des soins aux patients dans le RCITO et de la mobilité des patients au pays, le fait d'utiliser le nom, le numéro d'assurance maladie et la date de naissance du patient maximise les possibilités de couplage des enregistrements associés à la même personne. L'ICIS utilise ces informations pour broser le portrait complet des soins fournis à la personne. Afin de jumeler les enregistrements, l'ICIS doit savoir lesquels se rapportent à la personne. Bien qu'il ne s'agisse pas d'une pratique courante à l'ICIS, le nom (partiel ou complet) de la personne est recueilli à cette fin particulière dans le RCITO, de même que le numéro d'assurance maladie et d'autres identificateurs. Ces éléments de données sont stockés, consultés et utilisés strictement en cas de nécessité par le personnel de l'ICIS, conformément à la [Politique de respect de la vie privée, 2010](#) de l'ICIS. Comme il est indiqué ailleurs dans la présente évaluation, l'accès à ces éléments de données est très restreint à l'ICIS.

Caractéristiques démographiques du patient

Il peut s'agir, par exemple, de la date de naissance, du code postal, du sexe ou des identificateurs de statut autochtone. Comme il est mentionné à la [section 2.3](#), l'accès à ces variables sensibles est d'une durée limitée et ne peut être accordé que sur approbation écrite du gestionnaire du RCITO et de la directrice des Services d'information sur les soins ambulatoires et de courte durée. Dans le RCITO, l'âge du patient correspond à la somme du nombre de mois entre sa date de naissance et la date du début du traitement, divisée par 12. Le résultat est arrondi à un nombre entier, soit un nombre d'années. L'âge des donneurs est indiqué par un code (p. ex. nouveau-né, jours, mois, ans) et un nombre (p. ex. 2, 12, 35), puisque l'information fournie sur les donneurs n'inclut pas la date de naissance. L'ICIS utilise l'information géographique dérivée du code postal et du sexe pour réaliser des analyses démographiques des services de santé fournis et de leurs résultats.

Caractéristiques de santé du patient

Ces éléments comprennent les diagnostics et les comorbidités connexes. Le RCITO utilise ces informations pour analyser les diagnostics et les facteurs de risque.

Données administratives

Il peut s'agir, par exemple, de la date à laquelle le patient a commencé la dialyse, a été placé pour la première fois sur la liste d'attente d'une transplantation, a été placé sur la liste finale et a reçu une transplantation. L'ICIS utilise ces informations pour produire des rapports sur le parcours des patients au stade terminal de l'insuffisance organique et sur celui des donneurs.

Identificateurs de l'établissement de santé

Il peut s'agir, par exemple, du nom de l'hôpital où la transplantation a eu lieu ou de l'établissement où le patient reçoit la dialyse. L'ICIS utilise ces informations pour produire des rapports opérationnels et renvoyer aux établissements de santé les données qui leur sont propres.

Champs de texte libre

Il peut s'agir, par exemple, des champs utilisés dans le RCITO pour rendre compte d'autres caractéristiques des patients telles que la cause du décès ou un autre diagnostic principal. Ces champs servent à saisir de l'information essentielle au registre, mais qui n'est pas transmise à des tiers externes. Il peut arriver que les utilisateurs y indiquent des renseignements personnels sur la santé ou d'autres données sensibles. Le contenu des champs de texte libre considéré par le personnel du RCITO comme pouvant poser un risque lié au respect de la vie privée est conservé dans un dossier à accès restreint dans l'environnement de l'ICIS, séparé des autres données; l'accès à ce contenu n'est accordé

qu'avec autorisation et strictement en cas de nécessité. Périodiquement, le RCITO vérifie la présence de renseignements sur la santé ou d'autres données sensibles dans les champs de texte libre. De plus, chaque année avant la clôture de la base de données, le personnel du RCITO passe en revue les réponses saisies dans ces champs et leur attribue de nouvelles catégories en utilisant les codes de diagnostic et de décès appropriés, dans la mesure du possible. Par exemple, si les diagnostics ou causes de décès sont entrés sous forme de texte libre dans le champ Autre plutôt qu'au moyen des codes numériques inscrits dans les listes, le code numérique approprié est attribué lorsqu'il y a lieu.

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

À titre de collecteur secondaire de données, l'ICIS n'a pas de contact direct avec les patients. L'ICIS s'attend à ce que les fournisseurs de données respectent les règles et assument leurs responsabilités en matière de collecte, d'utilisation et de divulgation de données, y compris en ce qui concerne le consentement et les avis, comme le prévoient les lois, les règlements et les politiques en vigueur dans les provinces et territoires.

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

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

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

Personnel de l'ICIS

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

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

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

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

Couplage des données

Puisque le RCITO est une base de données longitudinale, les données qu'il contient sont systématiquement couplées. Le RCITO suit les patients depuis leur traitement initial au stade terminal de l'insuffisance organique (dialyse ou transplantation) jusqu'à leur décès ou, le cas échéant, jusqu'à l'arrêt des suivis. Cela signifie, par exemple, qu'un enregistrement de transplantation rénale sera ajouté aux enregistrements existants du RCITO si le patient a reçu des traitements de dialyse avant la transplantation. Lorsque des enregistrements de suivi concernant un patient inscrit au RCITO sont ajoutés à la base de données, ils sont couplés aux enregistrements existants au moyen du numéro d'identification unique du receveur, que le RCITO génère automatiquement à l'aide d'un algorithme en associant les nom, numéro d'assurance maladie et date de naissance du patient. L'information de suivi concernant les patients en dialyse est saisie annuellement. Pour les patients ayant reçu une transplantation, l'information sur les résultats de l'intervention est recueillie, y compris le statut du patient (p. ex. transfert, échec de la transplantation, décès ou arrêt des suivis).

Le RCITO effectue également des couplages internes entre les donneurs et les receveurs en mettant en correspondance l'identificateur de l'organisme de don d'organes, l'identificateur du donneur, le nom de famille partiel, l'âge ou la date de naissance du donneur ainsi que la date et l'heure du clampage chez le donneur.

Les données du RCITO sont aussi couplées avec les données d'autres sources de l'ICIS à l'aide du NAM chiffré, de la province émettrice du NAM et de l'année de naissance du patient. Comme le couplage des données peut accroître les risques d'identification d'une personne, l'ICIS prend des mesures d'atténuation des risques (p. ex. en attribuant aux patients des numéros de transaction sans signification).

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

L'ICIS a adopté une norme de couplage de données sur les clients à l'échelle de l'organisme qui régit le couplage des enregistrements créés depuis 2010-2011 et contenant les éléments de données suivants : NAM chiffré et province ou territoire ayant émis le NAM.

Les enregistrements qui ne satisfont pas à ces critères sont régis par un mécanisme de couplage défini au cas par cas.

Destruction des données couplées

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

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

Renvoi des données au fournisseur

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

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

Restriction de la divulgation

Demandes de données formulées par des tiers

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

L'ICIS administre le programme de demandes de données par des tiers, qui établit les mesures de contrôle de respect de la vie privée et de la sécurité que l'organisme demandeur doit respecter. En outre, comme le stipulent les articles 37 à 57 de sa [Politique de respect de la vie privée, 2010](#), l'ICIS divulgue des renseignements sur la santé conformément à son mandat et à ses fonctions de base, et s'efforce de divulguer les données dans le plus

grand anonymat possible tout en répondant aux exigences de recherche ou d'analyse du demandeur. Les données sont donc agrégées dans la mesure du possible. Si les données agrégées ne sont pas suffisamment détaillées pour les fins visées, l'ICIS peut décider, au cas par cas, de divulguer au destinataire des données dépersonnalisées au niveau de l'enregistrement ou des renseignements personnels sur la santé (dans des circonstances particulières, par exemple, avec le consentement de la personne). Le destinataire doit avoir signé au préalable une entente de protection des données ou un autre instrument juridiquement contraignant avec l'ICIS. Seuls les éléments de données nécessaires aux fins visées seront divulgués.

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

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

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

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

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

Comme indiqué à la [section 3.4](#), le RCITO recueille un identificateur de statut autochtone. La divulgation de cet identificateur est soumise à la politique sur la diffusion et la divulgation de données identificatoires sur les Autochtones de l'ICIS, en vertu de laquelle toute demande de données identifiant des Autochtones doit être accompagnée d'une preuve d'approbation des autorités autochtones compétentes. Pour en savoir plus, consultez le document [Tracer la voie vers la gouvernance respectueuse des données de l'ICIS sur les Premières Nations, les Inuits et les Métis](#).

Les divulgations (p. ex. les divulgations de demandes de données par des tiers) des données du RCITO sont dérivées des fichiers annuels d'extraction de données qui ont fait l'objet d'un contrôle de la qualité des données. Comme il est indiqué à la [section 3.4](#), l'ICIS recueille de l'information dans les champs de texte libre; les données qui proviennent de ces champs sont diffusées à l'externe uniquement dans le cadre des demandes de renvoi de données aux fournisseurs de données initiaux.

Diffusion publique des données du RCITO

Dans le cadre de son mandat, l'ICIS publie uniquement des données agrégées en s'assurant de réduire au minimum le risque d'identification et de divulgation par recoupements. En général, il faut au moins 5 observations par cellule conformément à l'article 33 de la [Politique de respect de la vie privée, 2010](#) de l'ICIS. Des statistiques agrégées et des analyses sont diffusées dans des publications et sur le [site Web de l'ICIS](#) au moyen de produits comme les [statistiques annuelles](#) et les [statistiques sommaires](#).

La disponibilité de cellules de faible valeur dans les tableaux générés à partir du RCITO est considérée comme essentielle pour fournir aux centres participants l'information clinique dont ils ont besoin. Par exemple, l'information contenue dans les cellules de faible valeur sur les patients pédiatriques est particulièrement importante puisque les diagnostics, les comorbidités et les résultats sont différents chez ces patients. En outre, les cellules de faible valeur sont présentes dans les cas de transplantations non courantes telles que les transplantations combinées. L'incidence de ces interventions est importante en raison de leur rareté. Si les praticiens canadiens n'obtiennent pas du RCITO l'information sur les interventions pratiquées au pays, ils doivent se tourner vers des sources internationales.

En raison de la nature des données diffusées par le RCITO, il peut arriver que des cellules comprenant moins de 5 observations soient déclarées. Avant toute diffusion publique, les données du RCITO font l'objet d'une évaluation visant à déterminer le risque d'identification et de divulgation par recoupements. Pour les produits de 2022 (statistiques sommaires, statistiques annuelles et rapports propres aux centres), le risque a été jugé négligeable.

Restriction de la conservation

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

3.8 Sixième principe : exactitude des renseignements personnels sur la santé

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

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

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

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

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

Sécurité des systèmes

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

Les registres de contrôle et de vérification des systèmes font partie intégrante du programme de sécurité de l'information de l'ICIS. Ces registres sont par ailleurs immuables. En général, l'ICIS utilise des données à risque réduit au niveau de l'enregistrement (où le NAM a été chiffré) pour réaliser ses analyses. Il arrive dans des circonstances exceptionnelles que le personnel doive avoir accès aux NAM d'origine. Les procédures et la [Politique de respect de la vie privée, 2010](#) de l'ICIS prévoient des contrôles stricts qui garantissent que l'accès est autorisé dans les circonstances et au niveau appropriés, et que le principe de minimisation des données est respecté en tout temps. L'ICIS consigne dans ses registres les activités suivantes ayant trait à l'accès aux données :

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

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

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

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

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

L'ICIS publie des informations concernant ses politiques de protection de la vie privée, ses pratiques en matière de traitement des données et ses programmes de gestion des renseignements personnels sur la santé. Plus précisément, le [*Cadre de respect de la vie privée et de sécurité*](#) et la [*Politique de respect de la vie privée, 2010*](#) de l'ICIS sont accessibles au icis.ca.

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

L'ICIS n'utilise pas les renseignements personnels sur la santé qu'il détient pour prendre des décisions administratives ou relatives aux personnes concernées. Toute personne qui souhaite accéder à ses renseignements personnels sur la santé verra sa demande traitée conformément aux articles 60 à 63 de la [Politique de respect de la vie privée, 2010](#) de l'ICIS.

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

Comme le stipulent les articles 64 et 65 de la [Politique de respect de la vie privée, 2010](#) de l'ICIS, les plaintes, questions et préoccupations concernant le traitement des renseignements par l'ICIS sont examinées par la chef de la protection des renseignements personnels et avocate générale, qui peut acheminer une demande ou une plainte au commissaire à l'information et 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 RCITO effectuée par l'ICIS n'a relevé aucun risque lié au respect de la vie privée et à la sécurité qui ne fait pas déjà l'objet de mesures d'atténuation.

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

**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

43417-1123

