Environnement d’accès sécurisé

Évaluation des incidences sur la vie privée

Juin 2021

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.

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

Comment citer ce document :
Institut canadien d'information sur la santé. *Évaluation des incidences sur la vie privée de l'environnement d'accès sécurisé*. Ottawa, ON : ICIS; 2021.

This publication is also available in English under the title *Secure Access Environment Privacy Impact Assessment*.

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

- *Évaluation des incidences sur la vie privée de l’environnement d’accès sécurisé*

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

Ottawa, juin 2021

Table des matières

L’environnement d’accès sécurisé de l’ICIS en bref

Par le passé, l’Institut canadien d’information sur la santé (ICIS) fournissait aux chercheurs et aux autres utilisateurs approuvés un accès à des données dépersonnalisées de ses banques de données en envoyant aux demandeurs des fichiers contenant les données extraites pertinentes. De nombreux grands instituts de données et de recherche ont délaissé cette approche pour privilégier un environnement d’accès sécurisé (EAS) semblable à celui de l’ICIS, décrit ici.

Voici quelques faits importants au sujet de l’EAS de l’ICIS :

- L’EAS de l’ICIS est un environnement chiffré et sécurisé, hébergé dans le centre de données de l’ICIS.
- Conformément aux politiques et procédures de l’ICIS, seuls les chercheurs ou les analystes approuvés ont accès à l’EAS (tous ces utilisateurs étant appelés ci-après « chercheurs » pour les besoins de la présente évaluation des incidences sur la vie privée).
- L’accès des chercheurs se limite aux dossiers contenant des données extraites, préparées et vérifiées par des membres du personnel de l’ICIS pour un projet de recherche approuvé.
- L’accès est géré au moyen de comptes d’utilisateurs approuvés, sécurisés, chiffrés et protégés par un mot de passe fort et une identification à 2 facteurs.
- Toujours selon les politiques et procédures de l’ICIS, seuls des résultats agrégés peuvent être extraits de l’EAS.
- Les utilisateurs approuvés sont liés par de rigoureuses conditions d’utilisation.

1 Présentation

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 (EIVP) a pour bût d'examiner les risques liés à la vie privée, à la confidentialité et à la sécurité en ce qui concerne l'environnement d'accès sécurisé (EAS) de l'ICIS utilisé par des tierces parties qui demandent des données au niveau de l'enregistrement à des fins de recherche. La présente EIVP a été effectuée conformément à notre *Politique d'évaluation des incidences sur la vie privée* et à notre *Cadre de gestion des risques liés au respect de la vie privée et à la sécurité*.

2 Renseignements contextuels

2.1 Présentation de l'EAS

L'ICIS prépare des fichiers prêts à être analysés et les rend accessibles aux tierces parties qui en font la demande au moyen du processus de demande de données de l'ICIS, sous réserve de ses politiques de respect de la vie privée et des ententes de partage des données conclues avec les provinces et territoires. Avant de créer l'EAS, l'ICIS transmettait les données au niveau de l'enregistrement directement aux tierces parties, soit sur un CD ou un DVD chiffré et protégé par mot de passe ou avec l'outil de diffusion des données. L'EAS de l'ICIS vise à renforcer davantage le processus de divulgation des données de l'ICIS et répond aux besoins suivants :

- Surveiller le respect des exigences en matière de sécurité de l'information et d'accès autorisé.
- Simplifier le long processus de destruction des données et de suivi.
- Faciliter la recherche collaborative (lorsque des chercheurs de plusieurs établissements veulent avoir accès aux mêmes fichiers de données).

Pour améliorer ses processus de divulgation des données et ses infrastructures, l'ICIS a mis en place un projet visant à créer l'EAS. Cet environnement offre aux chercheurs un accès sécurisé et contrôlé à distance aux données de l'ICIS à l'ouverture d'une session chiffrée. L'EAS élimine le risque que des données se perdent pendant le transfert, facilite la surveillance du respect des exigences en matière de sécurité de l'information et favorise la recherche collaborative en permettant à des chercheurs de divers établissements d'avoir accès aux mêmes données.

Depuis de nombreuses années, les chercheurs approuvés, les décideurs et les gestionnaires du système de santé peuvent compter sur l'ICIS pour obtenir des données au niveau de l'enregistrement ou des données agrégées provenant de nos bases de données. La requête se fait au moyen du processus de demande de données par des tiers (voir Faire une demande de données), qui est régi par nos politiques de respect de la vie privée :

- *Politique de respect de la vie privée relative à la collecte, à l'utilisation, à la divulgation et à la conservation des renseignements personnels sur la santé et des données dépersonnalisées*
- *Politique de respect de la vie privée relative à la collecte, à l'utilisation, à la divulgation et à la conservation des renseignements personnels des travailleurs de la santé et des données dépersonnalisées*

Grâce à notre processus de demande de données par des tiers, nous divulguons des données hautement dépersonnalisées tout en répondant au but de la recherche ou de l'analyse approuvée. Une fois que le projet est approuvé, les membres du personnel de l'ICIS travaillent avec les demandeurs pour préparer des fichiers de données dépersonnalisés, sur mesure et prêts à être analysés. Ces fichiers divulguent seulement les éléments de données nécessaires pour les besoins de la recherche ou de l'analyse.

Pendant longtemps, nous avons divulgué les fichiers de données en envoyant des copies sécurisées aux utilisateurs. Grâce aux avancées technologiques comme les services infonuagiques et les solutions de chiffrement, de plus en plus de détenteurs de données créent un EAS pour les activités de recherche et d'analyse. Les utilisateurs peuvent uniquement travailler avec les données à l'intérieur de l'environnement, avec un accès à distance, de sorte que les données ne quittent jamais l'EAS.

L'EAS de l'ICIS, comme dans le cas dans les autres environnements du genre, fournit aux utilisateurs autorisés un accès sécurisé et contrôlé à distance aux fichiers de données au niveau de l'enregistrement et aux outils analytiques. Dans sa première phase de déploiement, l'EAS de l'ICIS donne accès uniquement aux données dépersonnalisées au niveau de l'enregistrement. La plupart des utilisateurs ont uniquement accès aux données dépersonnalisées dans l'EAS, mais certains pourraient avoir accès aux renseignements personnels sur la santé, en vertu de l'article 44 de la *Loi sur la protection des renseignements personnels sur la santé* ou après avoir

obtenu un consentement éclairé. Lorsque l'EAS permettra l'accès autorisé à des renseignements personnels sur la santé ou à des renseignements personnels sur les travailleurs de la santé, la présente EIVP sera mise à jour.

L'EAS est hébergé sur des serveurs situés au Canada et exploité à partir de ces serveurs, ce qui est conforme à toutes les exigences applicables des ententes conclues avec nos fournisseurs de données.

L'accès à l'EAS est contrôlé à l'aide d'une connexion sécurisée et chiffrée et d'une identification à 2 facteurs. Autrement dit, l'accès à l'EAS exige une authentification à facteurs multiples, ce qui protège les connexions et bloque les accès non autorisés. L'EAS est protégé par un pare-feu. Aucun accès à Internet n'est permis depuis l'EAS. L'EAS permet la sauvegarde et le stockage sécurisés des données pour les projets autorisés.

L'intégrité et la sécurité des données consultées dans l'EAS sont aussi garanties par les ententes et les conditions d'utilisation de l'EAS.

Les projets et comptes d'utilisateurs font l'objet d'une administration centralisée dans l'EAS. Les membres autorisés de l'équipe du projet peuvent collaborer et prendre mutuellement connaissance de leurs résultats. L'EAS facilite la recherche en donnant accès à différentes applications analytiques comme SAS, et à Microsoft Office.

Les données au niveau de l'enregistrement ne peuvent pas être copiées ni extraites à partir de l'EAS. Pour prévenir la divulgation accidentelle de renseignements personnels sur la santé ou de renseignements personnels sur les travailleurs de la santé, seules les données agrégées qui ont été examinées par les membres du personnel de l'ICIS peuvent être extraites à partir de l'EAS.

2.2 Aucune nouvelle collecte de données

L'EAS n'implique aucune collecte de données par l'ICIS. Il remplace notre ancienne méthode de divulgation des données de nos banques de données aux tiers qui en faisaient la demande. Il donne accès à des données dépersonnalisées ou à des renseignements personnels sur la santé, si la loi le permet et en vertu de l'article 44 de la *Loi sur la protection des renseignements personnels sur la santé*, ou encore après avoir obtenu un consentement éclairé. Les utilisateurs autorisés pourront toutefois verser leurs propres données dans l'EAS, à des fins d'analyse à même l'EAS avec des fichiers de données de l'ICIS qui ont été préparés et rendus disponibles pour le projet en question. L'ICIS a mis en place des mécanismes de contrôle administratifs et techniques pour s'assurer que seuls les utilisateurs autorisés à téléverser des données pourront le faire. L'ICIS examinera les données avant leur téléversement dans l'EAS.

Puisque l'ICIS ne fera aucune nouvelle collecte de données, la présente EIVP n'a pas le même format standard que les autres EIVP publiées par l'ICIS. L'objectif est d'évaluer la mise en œuvre des mécanismes de contrôle administratifs et techniques requis pour assurer le respect de la vie privée, la confidentialité et la sécurité des données consultées dans l'EAS par les demandeurs tiers.

La section qui suit décrit le programme de gestion des risques liés au respect de la vie privée et à la sécurité de l'ICIS. Ce programme s'est avéré essentiel dans l'élaboration et la mise en œuvre des mesures appuyant le respect de la vie privée et la sécurité dans l'EAS de l'ICIS.

3 Analyse du respect de la vie privée et de la sécurité

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

La gestion des risques en matière de respect de la vie privée et de sécurité est un processus officiel pouvant être reproduit. Elle vise la détection, l'évaluation, la prise en charge et la surveillance des risques dans le but de réduire au minimum la probabilité qu'ils se matérialisent ou leur incidence possible. En 2015, l'ICIS a approuvé son *Cadre de gestion des risques liés au respect de la vie privée et à la sécurité* et mis en œuvre la *Politique sur la gestion des risques liés au respect de la vie privée et à la sécurité* connexe. La chef de la protection des renseignements personnels et le chef de la sécurité de l'information de l'ICIS, en collaboration avec 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. Le niveau de risque (faible, moyen ou élevé) établi pendant l'évaluation 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 qu'un premier traitement du risque est effectué, le risque résiduel (nouveau calcul de la probabilité et de l'incidence du risque par suite du traitement) est évalué et comparé à l'énoncé sur la tolérance des risques liés au respect de la vie privée et à la sécurité de l'ICIS, qui stipule que l'ICIS a une faible tolérance à de tels risques. Si le niveau de risque résiduel demeure plus élevé que faible, de nouvelles mesures de prise en charge doivent être mises en œuvre jusqu'à l'obtention d'un niveau faible, ou jusqu'à ce que le risque non pris en charge ou résiduel soit accepté par le Comité exécutif de l'ICIS au nom de l'organisme.

Au terme du processus de gestion des risques liés au respect de la vie privée et à la sécurité, 13 risques liés au respect de la vie privée et à la sécurité ont été relevés. Ces risques ont été inscrits au registre des risques liés au respect de la vie privée et à la sécurité de l'ICIS. Ils ont été évalués et traités conformément à la méthodologie de gestion des risques liés au respect de la vie privée et à la sécurité. Les risques ont été suffisamment atténués pour respecter la faible tolérance de l'ICIS aux risques liés au respect de la vie privée et à la sécurité.

3.2 Autorités régissant les données de l'EAS

Généralités

Comme mentionné précédemment, l'EAS n'implique aucune nouvelle collecte de données par l'ICIS. L'EAS est un moyen plus sécuritaire de donner aux utilisateurs autorisés un accès à des fichiers de données approuvés. Comme toujours, l'ICIS se conforme à sa *Politique de respect de la vie privée, 2010* ainsi qu'à toute législation ou entente applicable.

Les chercheurs autorisés pourront, dans certaines circonstances approuvées et contrôlées, verser des données pour les coupler à celles de l'ICIS. Lorsqu'il traitera les demandes à ce sujet, l'ICIS évaluera les enjeux de respect de la vie privée associés à la proposition et rejettera la demande ou mettra en œuvre les mesures de protection de la vie privée appropriées.

Responsabilité et gouvernance de l'EAS

Le tableau qui suit présente les principaux postes de direction à l'ICIS responsables de la gestion des risques liés au respect de la vie privée et à la sécurité pour les données de l'EAS.

Tableau Principaux postes et responsabilités

Poste ou groupe	Responsabilités
Vice-président, Stratégies de données et Statistiques	Responsable de l'orientation stratégique générale de l'EAS
Directeur, Services d'information sur les soins ambulatoires et de courte durée	Responsable du fonctionnement général de l'EAS et des décisions administratives stratégiques connexes
Gestionnaire, Aide à la décision, Programme interne de demande de données et Traumatismes	Responsable de la gestion continue, du développement et de la mise en œuvre de l'EAS. Prend les décisions opérationnelles liées à l'EAS et assure la gestion des activités de consultation auprès des intervenants internes et externes de l'EAS
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

Respect de la vie privée et sécurité de l'EAS — processus et mesures de protection connexes

Gestion de l'accès et de l'identité

Seuls les chercheurs dont les projets sont conformes aux politiques et aux procédures de l'ICIS peuvent accéder à l'EAS. Les chercheurs doivent fournir les renseignements suivants dans le cadre du processus de demande d'accès :

- Nom
- Poste
- Organisme
- Adresse
- Adresse électronique de l'organisme
- Preuve d'approbation par un conseil d'éthique de la recherche pour l'étude proposée

Ces renseignements doivent être fournis pour le chercheur principal et tous les chercheurs qui auront besoin d'un accès autorisé à l'EAS dans le cadre de leur projet.

Le secteur de programme de l'ICIS responsable confirmera ensuite le statut des chercheurs au moyen d'une recherche en ligne et fera d'autres recherches au besoin. Toute demande de changement de la part d'un utilisateur de l'EAS déclenche un processus d'engagement renouvelé avec cet utilisateur.

L'entente d'utilisation de l'environnement d'accès sécurisé doit être signée par un signataire autorisé de l'organisme auquel la recherche est affiliée, ainsi que par la personne qui dirige le projet de recherche et qui est responsable de tous les chercheurs qui travaillent sur le projet dans l'EAS. L'entente lie l'organisme et la personne qui dirige le projet à des conditions propres à l'EAS et à son utilisation. De plus, chaque chercheur ayant accès à l'EAS doit accepter les conditions d'utilisation de l'environnement d'accès sécurisé.

Les utilisateurs approuvés doivent aussi suivre les directives énoncées dans le *Guide de l'utilisateur de l'EAS*. Ce guide comprend les instructions sur les mesures de protection techniques et les exigences connexes. Parmi ces exigences, mentionnons que seuls les ordinateurs fournis par l'employeur ou l'établissement de l'utilisateur doivent être utilisés pour accéder à l'EAS, qu'un protocole SFTP doit être installé et utilisé, et que l'accès doit se faire par une identification à 2 facteurs avec l'application Duo de Cisco.

Le *Guide de l'utilisateur de l'EAS* indique la marche à suivre pour accéder à l'EAS et l'utiliser. Il explique aussi comment les utilisateurs peuvent joindre notre équipe technique afin de s'assurer qu'ils se conforment à nos exigences en matière de vie privée et de sécurité.

L'entente d'utilisation stipule notamment qu'il est interdit d'accéder à l'EAS à l'extérieur du Canada.

Projets autorisés

L'utilisation de l'EAS est réservée aux utilisateurs dont les projets sont conformes aux politiques et aux procédures de l'ICIS. À la réception d'une demande, l'ICIS évalue l'utilisation prévue des données et approuve le projet seulement s'il s'inscrit dans le mandat et les fonctions de base de l'ICIS (décrits à l'article 37 de la *Politique de respect de la vie privée, 2010*) et s'il est conforme à toutes les autres lois applicables. De plus, pour tous les projets autorisés, l'ICIS voit à ce que les demandeurs signent les ententes juridiquement contraignantes pour assurer l'usage approprié et la protection des données. L'ICIS ne divulgue que les éléments de données nécessaires à la réalisation des fins déterminées.

Couplage des données

Les projets réalisés par des tiers et approuvés peuvent dans certains cas nécessiter le couplage de données entre les fichiers de données détenus par l'ICIS (p. ex. couplage des fichiers de données de la Base de données sur les congés des patients et du Système national d'information sur les soins ambulatoires) ou le couplage de données entre les fichiers de données de l'ICIS et ceux fournis par le chercheur.

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. Toutes les demandes de couplage de données formulées par des tiers sont soumises à un processus interne d'examen et d'approbation. Lors du processus de couplage, l'ICIS utilise des numéros d'assurance maladie chiffrés. Dans tous les cas, les données couplées demeurent assujetties à la *Politique de respect de la vie privée, 2010* de l'ICIS.

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 :

Les personnes dont les renseignements personnels sur la santé sont utilisés pour le couplage de données y consentent au préalable (article 23), ou les critères suivants sont respectés (article 24) :

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 de la *Politique de respect de la vie privée, 2010* de l'ICIS;
e. le couplage de données est effectué dans le cadre d'un programme de travail continu et approuvé de l'ICIS; les données couplées sont conservées aussi longtemps que nécessaire pour la réalisation des fins déterminées, puis elles sont détruites dans le respect des règles énoncées aux articles 28 et 29 de la *Politique de respect de la vie privée, 2010*;
f. le couplage de données permet de réaliser des économies évidentes par rapport à d'autres méthodes ou est l'unique méthode envisageable.

Divulgation et dépersonnalisation des données dans l'EAS

L'accès aux fichiers de données dans l'EAS est considéré comme une divulgation et doit être autorisé, conformément à la *Politique de respect de la vie privée, 2010*. La plupart des utilisateurs ont uniquement accès aux données dépersonnalisées dans l'EAS, mais certains pourraient avoir accès aux renseignements personnels sur la santé, en vertu de l'article 44 de la *Loi sur la protection des renseignements personnels sur la santé* ou après avoir obtenu un consentement éclairé. Dans la phase initiale, l'EAS donnera uniquement accès aux données dépersonnalisées. La présente EIVP sera mise à jour si l'accès à des renseignements personnels identificatoires devait être permis.

Les fichiers de données dépersonnalisées au niveau de l'enregistrement sont vérifiés au moyen de notre solution de dépersonnalisation Eclipse de Privacy Analytics avant d'être rendus accessibles dans l'EAS, le cas échéant. Un rapport de conformité est inclus dans la documentation approuvant la publication des données dans l'EAS. Les fichiers de données dépersonnalisées au niveau de l'enregistrement qui ne sont pas analysés par la solution de dépersonnalisation Eclipse de Privacy Analytics doivent être revus par un méthodologiste principal dans l'unité de méthodologie de l'ICIS avant d'être publiés dans l'EAS.

Accès à l'EAS à l'extérieur du Canada

L'accès à l'EAS à l'extérieur du Canada est interdit, comme stipulé dans l'entente d'utilisation. L'ICIS a mis en place des mécanismes de contrôle techniques et administratifs pour voir au respect de cette exigence.

Extrants

Pour empêcher la divulgation accidentelle de renseignements personnels sur la santé ou de renseignements personnels sur les travailleurs de la santé, l'ICIS a fait en sorte que seules les données agrégées qui ont été examinées par les membres du personnel peuvent être extraites à partir de l'EAS. Les modalités prévues dans l'entente d'utilisation de l'environnement d'accès sécurisé et les conditions d'utilisation de l'environnement d'accès sécurisé stipulent que l'utilisateur peut seulement exporter les données agrégées qui ont été examinées par l'ICIS. De plus, elles interdisent explicitement la copie, l'exportation ou la reproduction des données de l'ICIS (y compris la prise de photos). L'ICIS a aussi mis en place des mécanismes techniques pour empêcher l'utilisateur de faire une copie des données avec des outils de copier-coller. De plus, le personnel de l'ICIS examine manuellement toutes les demandes d'extraction de fichiers de sortie et de codes sources, détectant par ce processus toute tentative de copie des données dans des applications de gestion des données ou des fichiers.

Vérification et surveillance

L’accès à l’EAS est géré au moyen d’un processus centralisé d’accès des utilisateurs. Ce processus permet à l’ICIS de contrôler l’attribution et le retrait des accès à l’EAS. Les utilisateurs approuvés font l’objet d’une vérification annuelle pour confirmer qu’ils sont actifs. Au terme de cette vérification annuelle, les comptes inactifs sont fermés et leur accès est révoqué.

4 Conclusion

Tous les risques relevés pendant l’évaluation des risques liés au respect de la vie privée et à la sécurité de l’EAS ont été suffisamment atténués pour respecter la faible tolérance de l’ICIS à ces risques.

La présente EIVP sera mise à jour ou révisée conformément à notre *Politique d’évaluation des incidences sur la vie privée*.

aide@icis.ca

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

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

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

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

icis.ca

24695-0721