Cadre de respect de la vie privée et de sécurité

2010

Mise à jour en octobre 2020

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

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

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. *Cadre de respect de la vie privée et de sécurité, 2010 — mise à jour en octobre 2020*. Ottawa, ON : ICIS; 2020.

This publication is also available in English under the title *Privacy and Security Framework, 2010 — Updated October 2020*.

Table des matières

Respect de la vie privée et sécurité de l'information à l'ICIS — introduction

Le Cadre de respect de la vie privée et de sécurité aborde de façon intégrale et cohérente la gestion du respect de la vie privée et de la sécurité de l'information à l'Institut canadien d'information sur la santé (ICIS). Le cadre a pour but de faciliter l'intégration et la coordination efficaces des politiques de l'ICIS en matière de respect de la vie privée et de sécurité de l'information. Il offre en outre aux décideurs, aux responsables du respect de la vie privée et de la sécurité de l'information et à l'ensemble de la structure de gouvernance de l'ICIS une vision holistique des pratiques de l'organisme en matière de respect de la vie privée et de sécurité de l'information. Le cadre est mis à jour à mesure que des changements sont apportés aux programmes de respect de la vie privée et de sécurité de l'information de l'ICIS. Il sert également à informer les organismes de réglementation, les gouvernements fédéral, provinciaux et territoriaux, le public et les autres intervenants au sujet de l'engagement de l'ICIS envers le respect de la vie privée et la sécurité de l'information.

Le cadre est fondé sur les pratiques exemplaires de gestion du respect de la vie privée et de la sécurité de l'information qui prévalent dans les secteurs public, privé et de la santé. Le cadre se veut modulaire et permet à l'ICIS de répartir la responsabilité sur l'ensemble des secteurs d'activité, de cerner les points à améliorer et d'élaborer des plans d'action visant des éléments particuliers.

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

Forces motrices

Jurisprudence et législation	*Loi sur la protection des renseignements personnels sur la santé* (LPRPS) et réglementation de l'Ontario ainsi que toute autre loi fédérale, provinciale ou territoriale s'appliquant en matière de respect de la vie privée
Confiance	Confiance du public canadien ainsi que des gouvernements fédéral, provinciaux et territoriaux, incluant les ministères de la Santé, les dispensateurs de soins de santé et les autres intervenants
Vision et mandat	Vision, mandat et fondements décrits dans le Plan stratégique de l'ICIS et autres priorités et objectifs précis Mandat et fonctions de base définis dans la Politique de respect de la vie privée de l'ICIS

Gouvernance

Structure organisationnelle	Comité de gouvernance et de respect de la vie privée du Conseil d'administration Comité des finances et de la vérification du Conseil d'administration Président-directeur général Chef de la protection des renseignements personnels et avocat général Chef de la sécurité de l'information Divers comités appuyant la vision et les engagements en matière de respect de la vie privée et de sécurité de l'information Conseiller externe en matière de respect de la vie privée
Responsabilisation, responsabilités communes et transparence	Responsabilités individuelles en matière de respect de la vie privée et de sécurité de l'information, et mandats écrits des divers comités

Gestion des risques

Programme de gestion des risques liés au respect de la vie privée et à la sécurité	Programme de gestion des risques liés au respect de la vie privée et à la sécurité harmonisé au Programme de gestion des risques de l'ICIS
Analyses comparatives	Analyses contextuelles et pratiques exemplaires
Conformité	Code de conduite de l'ICIS
Continuité des opérations et reprise après sinistre	Plan de continuité des opérations de l'ICIS Plan de reprise technologique

Contrôles de programme

Politiques	Ensemble complet de politiques en matière de respect de la vie privée et de sécurité de l'information
Normes, procédures et protocoles	Normes, procédures et protocoles en appui aux politiques de respect de la vie privée et de sécurité de l'information
Formation et sensibilisation	Politique en matière de formation sur le respect de la vie privée et la sécurité Orientation obligatoire et vérifiable sur le respect de la vie privée et la sécurité pour tous les nouveaux employés, et formation continue en la matière au moins une fois par année Site Web interne Désignation de janvier comme mois de la sensibilisation au respect de la vie privée et de septembre comme mois de la sensibilisation à la sécurité de l'information, dans le cadre des programmes de sensibilisation en matière de respect de la vie privée et de sécurité Séances de formation continue périodiques afin de tenir les employés au courant des tendances et développements en matière de respect de la vie privée et de sécurité de l'information
Cycle de vie de l'information sécurisée	Ensemble de normes et de lignes directrices concernant la protection de la confidentialité, l'intégrité et la disponibilité de l'information pendant tout son cycle de vie, de la création et la collecte à l'élimination, en passant par la conservation et le stockage, l'accès, l'utilisation et la divulgation
Protocole de gestion des incidents	Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité de l'information
Ententes	Ententes internes, y compris l'entente de confidentialité des employés de l'ICIS, renouvelée annuellement Ententes prévues dans le programme de demandes de données par des tiers de l'ICIS
Gestion des tiers fournisseurs	Questions relatives au respect de la vie privée et à la sécurité de l'information abordées dans les ententes avec les fournisseurs
Communications externes	Cadre de respect de la vie privée et de sécurité de l'ICIS et autres instruments stratégiques clés accessibles au public à icis.ca

Vérifications, conformité et rapports

Programme de vérification du respect de la vie privée	Mandat du programme de vérification du respect de la vie privée
Programme de vérification de la sécurité de l'information	Vérifications obligatoires et ponctuelles
Examen externe de l'ICIS	Examen aux 3 ans par le commissaire à l'information et à la protection de la vie privée de l'Ontario, conformément au paragraphe 45 de la LPRPS Système de gestion de la sécurité de l'information (SGSI), conformément à la norme ISO/IEC 27001:2013
Surveillance de la conformité et rapports	Rapport annuel sur le respect de la vie privée soumis au Conseil d'administration, rapports spéciaux sur des sujets en particulier, au besoin et résultant du programme de vérification

1 Forces motrices

a. Jurisprudence et législation

À titre d'entité prescrite en vertu du paragraphe 45 de la *Loi sur la protection des renseignements personnels sur la santé* (LPRPS) de l'Ontario, l'ICIS est autorisé à recueillir, à utiliser et à divulguer des renseignements personnels sur la santé aux fins prévues. Pour se prévaloir de cette désignation, l'ICIS doit faire approuver tous les 3 ans ses pratiques et procédures en matière de respect de la vie privée et de protection de l'information sur la santé par le commissaire à l'information et à la protection de la vie privée de l'Ontario. Le dernier examen remonte à octobre 2017. Les intervenants de tout le pays considèrent le renouvellement du statut d'entité prescrite de l'ICIS comme une preuve de la validité de ses programmes de respect de la vie privée et de sécurité de l'information.

La LPRPS et tous les codes de respect de la vie privée reposent habituellement sur les 10 principes équitables de traitement de l'information énoncés dans le *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation :

- Principe 1 : Responsabilité
- Principe 2 : Détermination des fins de la collecte des renseignements
- Principe 3 : Consentement
- Principe 4 : Limitation de la collecte
- Principe 5 : Utilisation, communication et conservation
- Principe 6 : Exactitude
- Principe 7 : Mesures de sécurité
- Principe 8 : Transparence
- Principe 9 : Accès aux renseignements personnels
- Principe 10 : Possibilité de porter plainte contre le non-respect des principes

Ces principes forment la pierre angulaire des efforts d'autoréglementation de l'ICIS. L'organisme respecte également les lois provinciales et territoriales s'appliquant à son mandat et à ses fonctions de base.

b. Confiance

Avec plus de 30 bases de données (dont la liste se trouve dans le *Guide des produits et services* de l'ICIS), l'ICIS est une source fondamentale d'information objective, crédible et comparable. Pour atteindre ses objectifs, l'ICIS se doit de préserver la confiance des divers intervenants, incluant les organismes gouvernementaux fédéraux, provinciaux et territoriaux, les dispensateurs et établissements de soins de santé, les ordres et associations de professionnels de la santé et, bien sûr, du grand public. Les activités doivent être menées et les partenariats, créés et entretenus de manière à refléter ces attentes.

c. Vision et mandat

Notre vision

La vision de l'ICIS — De meilleures données pour de meilleures décisions : des Canadiens en meilleure santé — illustre comment de meilleures données peuvent mener à une meilleure prise de décisions et améliorer la santé des Canadiens. La réalisation de ce mandat repose essentiellement sur la mise en œuvre d'un cadre rigoureux et efficace de respect de la vie privée et de sécurité.

Notre mandat

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.

Nos fondements

Le travail de l'ICIS est fondé sur 4 éléments fondamentaux qui sont essentiels à son succès et à la réalisation de ses buts stratégiques :

- personnel
- participation des intervenants et partenariats
- confidentialité et sécurité
- technologies de l'information

La gestion de la confidentialité et de la sécurité de l'information et une solide infrastructure des technologies de l'information constituent 2 de ces 4 éléments fondamentaux, et sont par conséquent intégrées à la culture de l'ICIS. Ils servent de façon stratégique à la prise de décisions lors des interactions quotidiennes avec les employés, clients et intervenants.

2 Gouvernance

a. Structure organisationnelle

La structure de gouvernance de l'ICIS reflète ses pratiques de gestion de l'information. Cette structure permet de s'assurer que les stratégies, politiques, normes, processus et ressources de gestion des risques de violation du respect de la vie privée et de la sécurité de l'information sont conformes aux objectifs de l'ICIS et respectent les lois, les normes ainsi que les pratiques exemplaires en vigueur.

Le Comité de gouvernance et de respect de la vie privée du Conseil d'administration de l'ICIS supervise le programme de respect de la vie privée de l'organisme, tandis que le Comité des finances et de la vérification du Conseil d'administration supervise le programme de sécurité de l'information. La structure de gouvernance comprend, outre le président-directeur général, un chef de la protection des renseignements personnels et avocat général ainsi qu'un chef de la sécurité de l'information.

Le chef de la protection des renseignements personnels et avocat général et le chef de la sécurité de l'information occupent des postes de cadre supérieur au sein de l'organisme et, surtout, représentent leurs fonctions respectives au sein des organes de prise de décision et de surveillance de l'ICIS qui comprennent le Comité de gouvernance et de respect de la vie privée du Conseil d'administration, le Comité des finances et de la vérification du Conseil d'administration, le Comité de la haute direction et le Comité sur le respect de la vie privée, la confidentialité et la sécurité. Le chef de la protection des renseignements personnels et avocat général et le chef de la sécurité de l'information bénéficient du soutien de divers comités fonctionnels.

Voici les principaux comités liés à la question du respect de la vie privée et de la sécurité de l'information :

- Comité exécutif
  - Dirigé par le président-directeur général et composé des vice-présidents, des directeurs exécutifs et du chef de la protection des renseignements personnels et avocat général
- Comité de la haute direction
  - Dirigé par le vice-président, Services administratifs, et composé des vice-présidents, des directeurs exécutifs ainsi que de tous les directeurs, dont le chef de la protection des renseignements personnels et avocat général et le chef de la sécurité de l'information
- Équipe de direction des technologies de l'information
  - Dirigée par le vice-président et dirigeant principal de l'information

- Comité sur le respect de la vie privée, la confidentialité et la sécurité
  - Dirigé par le chef de la protection des renseignements personnels et avocat général
- Comité directeur du Système de gestion de la sécurité de l'information (SGSI)
  - Dirigé par le vice-président et dirigeant principal de l'information et composé de tous les directeurs des Services des technologies de l'information et de membres du personnel clés du SGSI
- Groupe de travail du SGSI
  - Dirigé par le conseiller principal, Sécurité de l'information, et composé de cadres supérieurs des Services des technologies de l'information en appui au SGSI de l'ICIS

Les responsabilités du chef de la protection des renseignements personnels et avocat général et du chef de la sécurité de l'information sont étroitement liées. Des communications ouvertes et constantes entre ces 2 fonctions sont essentielles à l'efficacité du modèle de gouvernance de l'information. Le chef de la protection des renseignements personnels et avocat général et le chef de la sécurité de l'information doivent donc coordonner leurs efforts dans des domaines comme la formation et la sensibilisation ainsi que l'élaboration de politiques.

Pour s'assurer que le programme de respect de la vie privée de l'ICIS tient compte des pratiques exemplaires, l'ICIS fait appel à un conseiller principal externe en matière de respect de la vie privée. Son mandat consiste à fournir à l'ICIS des conseils en temps opportun sur les nouvelles tendances en matière de respect de la vie privée, les pratiques exemplaires, les changements apportés aux lois ainsi que les approches et points de vue des responsables externes du respect de la vie privée.

b. Responsabilisation, responsabilités communes et transparence

Tous les employés de l'ICIS jouent un rôle important dans la confidentialité et la sécurité de l'information contenue dans les banques de données de l'organisme. Les responsabilités définies dans les présentes incombent plus particulièrement aux comités et personnes qui jouent un rôle de direction et sont responsables du respect de la vie privée et de la sécurité de l'information.

Conscient de l'importance des obligations de l'ICIS en matière de respect de la vie privée, le Conseil d'administration a créé un Comité de gouvernance et de respect de la vie privée. Ce comité, qui assume les responsabilités les plus élevées, a pour mandat de superviser le programme de respect de la vie privée et d'examiner les rapports de violation du respect de la vie privée et de vérification, les changements importants apportés à la Politique de respect de la vie privée de l'ICIS et toute question jugée pertinente par le président-directeur général ou le chef de la protection des renseignements personnels et avocat général.

Les responsabilités en matière de respect de la vie privée et de sécurité de l'information incombent en fin de compte au président-directeur général de l'ICIS qui, sur le plan opérationnel, a officiellement délégué ces fonctions au chef de la protection des renseignements personnels et avocat général et au chef de la sécurité de l'information.

Le chef de la protection des renseignements personnels et avocat général dirige le Secrétariat à la vie privée et aux services juridiques; gère le programme de respect de la vie privée; fournit conseils et soutien en matière de respect de la vie privée aux diverses sections; veille à l'intégralité, à l'actualisation et à la communication au personnel, au public et aux autres intervenants des politiques et procédures de respect de la vie privée; offre une formation et de la sensibilisation sur le respect de la vie privée; procède à des évaluations des incidences sur la vie privée et à des vérifications; surveille le respect des politiques; effectue des analyses comparatives. Le chef de la protection des renseignements personnels et avocat général a également pour tâche de s'assurer que des ententes de partage de données et autres sont en vigueur, et de surveiller les développements juridiques et autres dans le secteur du respect de la vie privée.

Le chef de la sécurité de l'information dirige la sécurité de l'information et assume au quotidien la responsabilité de la confidentialité, de l'intégrité et de la disponibilité des banques de données qui sont sous la garde et le contrôle de l'ICIS. Il doit également s'assurer de l'efficacité, de la mise à jour et de la communication au personnel, au public et aux autres intervenants du programme de sécurité de l'information et des politiques connexes. Il est de plus responsable de la formation et de la sensibilisation en matière de sécurité de l'information, de la réalisation des évaluations des risques et des vérifications, de l'exécution des analyses comparatives et de l'observation des pratiques exemplaires relatives à la sécurité de l'information dans l'industrie. Le chef de la sécurité de l'information doit faire part de tous les résultats pertinents des vérifications au Comité des finances et de la vérification du Conseil d'administration.

L'ICIS est résolu à appliquer les principes d'ouverture, de transparence et d'accessibilité en rendant le présent cadre et son ensemble de politiques en matière de respect de la vie privée et de sécurité accessibles au public sur son site Web à icis.ca. D'autres documents sont également accessibles, comme

- des renseignements en lien avec les politiques, les procédures et les pratiques de respect de la vie privée et de sécurité mises en place par l'ICIS;
- une description des bases de données de l'ICIS et des renseignements personnels qu'elles contiennent;
- des évaluations des incidences sur la vie privée;
- des documents relatifs à l'examen des pratiques de respect de la vie privée et de sécurité de l'information de l'ICIS réalisé par le commissaire à l'information et à la protection de la vie privée de l'Ontario;

- les coordonnées du chef de la protection des renseignements personnels et avocat général et du chef de la sécurité de l'information de l'ICIS, auxquels quiconque peut faire part de questions, d'inquiétudes ou de plaintes au sujet du respect des politiques, des procédures et des pratiques en matière de respect de la vie privée et de la sécurité, et du respect de la loi et de ses règlements.

L'information accessible au public comprend également

- une description du statut de l'ICIS en tant qu'entité prescrite sous la LPRPS;
- les responsabilités qui découlent de ce statut et des politiques mises en place;
- l'information liée à la récolte, à l'utilisation et à la divulgation de renseignements personnels sur la santé, et à certaines des mesures de protection administratives, techniques et physiques mises en place en vue de protéger la vie privée des personnes visées par les renseignements personnels sur la santé que l'ICIS recueille et de maintenir la confidentialité de ces renseignements.

3 Gestion des risques

Le chef de la protection des renseignements personnels et avocat général et le chef de la sécurité de l'information gèrent le Programme de gestion des risques liés au respect de la vie privée et à la sécurité. Ce programme permet à l'ICIS de cerner, d'évaluer et de gérer adéquatement les risques liés au respect de la vie privée et à la sécurité de l'information.

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

L'ICIS a mis en place un Programme de gestion des risques liés au respect de la vie privée et à la sécurité qui s'harmonise avec son Programme de gestion des risques. 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.

Le Programme de gestion des risques liés au respect de la vie privée et à la sécurité oriente les activités de gestion des risques de l'ICIS et s'y harmonise :

- il repose sur une méthodologie, une terminologie et une structure de gouvernance semblables;
- il permet de déceler les risques liés au respect de la vie privée et à la sécurité de l'information qui pourraient être inclus au registre des risques.

Dans le cadre du Programme de gestion des risques liés au respect de la vie privée et à la sécurité, l'ICIS utilise divers outils d'identification des risques en matière de respect de la vie privée et de sécurité, notamment des évaluations des incidences sur la vie privée, des évaluations des incidents liés au respect de la vie privée et à la sécurité, des évaluations de la vulnérabilité et des tests d'intrusion. Les évaluations des incidences sur la vie privée ont pour but de s'assurer que les principes de respect de la vie privée et de sécurité sont pris en compte lors de la conception, de la mise en œuvre et de la mise à jour des programmes, initiatives, processus ou systèmes (évaluation de la sécurité et de la protection de la vie privée dès la conception).

L'ICIS a réussi à intégrer les évaluations des incidences sur la vie privée à ses processus opérationnels. À noter que la responsabilité des évaluations, conformément à la *Politique d'évaluation des incidences sur la vie privée* de l'ICIS, est partagée par le personnel de section ou le gestionnaire de projet et le personnel du Secrétariat à la vie privée et aux services juridiques. Les évaluations sont réalisées lors de la conception de nouveaux programmes ou lors de révisions majeures de programmes existants, lorsque ces activités comprennent la collecte, l'utilisation ou la divulgation de renseignements personnels ou encore l'accès à ces renseignements.

L'ICIS procède à des évaluations des risques liés à la sécurité de l'information afin de cerner, d'évaluer et de gérer les risques liés à la sécurité de l'information. Des évaluations de la vulnérabilité et des tests d'intrusion sont aussi réalisés ou commandés régulièrement afin de déceler les risques liés à l'information et aux systèmes d'information de l'ICIS.

b. Analyses comparatives

Le chef de la protection des renseignements personnels et avocat général et le chef de la sécurité de l'information comparent régulièrement les attributs et contrôles des programmes de respect de la vie privée et de sécurité de l'ICIS par rapport à ceux d'organismes homologues, aux nouvelles tendances ainsi qu'aux pratiques exemplaires nationales et internationales en vigueur. Cette façon de faire oriente l'élaboration de plans stratégiques, opérationnels et tactiques en matière de respect de la vie privée et de sécurité de l'information.

c. Conformité

Le chef de la protection des renseignements personnels et avocat général surveille activement l'environnement législatif et réglementaire pour veiller à ce que l'ICIS se conforme en permanence à toutes les lois applicables. De même, le chef de la sécurité de l'information surveille l'environnement de sécurité des technologies de l'information pour cerner les menaces émergentes et les pratiques exemplaires.

L'ICIS a mis en place un SGSI conformément à la norme internationale ISO/IEC 27001:2013 et fait l'objet de vérifications régulières pour confirmer qu'elle s'y conforme.

À l'interne, le Code de conduite de l'ICIS exige que les membres du personnel respectent toutes les politiques, procédures, normes et protocoles en matière de respect de la vie privée et de sécurité, et qu'ils confirment tous les deux ans leur engagement à bien comprendre leurs obligations. Tout manquement au code, aux politiques ou aux pratiques peut entraîner des mesures disciplinaires pouvant aller jusqu'au congédiement.

d. Continuité des opérations et reprise après sinistre

L'ICIS dispose d'un plan complet de continuité des opérations, qui comprend un plan de reprise technologique. Ce plan est nécessaire à la protection des bases de données et des dossiers essentiels de l'ICIS en cas de situation d'urgence ou de perturbation des activités d'exploitation. Le chef de la protection des renseignements personnels et avocat général et le chef de la sécurité de l'information sont membres de l'équipe responsable de la continuité des opérations et s'assurent que les préoccupations relatives au respect de la vie privée et à la sécurité sont prises en compte pendant le processus de reprise.

4 Contrôles de programme

L'ICIS maintient un ensemble complet de politiques, de procédures, de normes et de lignes directrices visant le respect de la vie privée et la sécurité de l'information. Ces instruments stratégiques orientent toutes les pratiques en matière d'information au sein de l'organisme.

a. Politiques

La *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, 2010* de l'ICIS (la « Politique de respect de la vie privée ») et la *Politique sur la sécurité de l'information* orientent les autres politiques, normes et lignes directrices visant le respect de la vie privée et la sécurité de l'information.

La Politique de respect de la vie privée de l'ICIS, qui s'inspire du *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation, constitue le fondement du programme de respect de la vie privée à l'ICIS. Elle englobe les principes internationalement acceptés de respect de la vie privée concernant la collecte minimale, la détermination de l'utilisation, de la divulgation et de la conservation ainsi que le droit d'accès et de modification.

La *Politique de sécurité de l'information* de l'ICIS décrit l'engagement de l'organisme en matière de sécurité de l'information ainsi que les rôles et responsabilités de tous les employés quant à la protection de l'information.

Les politiques de l'ICIS en matière de respect de la vie privée et de sécurité de l'information décrivent de façon globale les objectifs et orientations définis par le Conseil d'administration et la direction. Elles sont conformes aux exigences législatives et aux pratiques exemplaires en matière de protection de l'information, ainsi qu'elles sont accessibles, transparentes et complètes. En 2005, 2008, 2011, 2014 et 2017, le commissaire à l'information et la protection de la vie privée de l'Ontario a conclu que les pratiques et procédures en vigueur à l'ICIS protègent adéquatement la vie privée des personnes visées par les renseignements personnels sur la santé qu'il recueille, et que la confidentialité de cette information est adéquatement assurée. L'ICIS met en œuvre toutes les recommandations formulées par le commissaire dans le cadre de son examen.

Un examen continu des politiques permet de s'assurer que celles-ci demeurent toutes à jour et actuelles. Les mises à jour ou les changements relatifs aux politiques, procédures et pratiques de respect de la vie privée et de sécurité de l'information de l'ICIS tiennent compte de ce qui suit :

- ordonnances, directives, feuillets de documentation et pratiques exemplaires émis par le Commissaire à l'information et à la protection de la vie privée de l'Ontario en vertu de la LPRPS et de ses règlements;
- évolution des normes et pratiques exemplaires du milieu en matière de respect de la vie privée et de sécurité de l'information;
- modifications à la LPRPS et à ses règlements qui touchent le statut d'entité prescrite de l'ICIS;
- recommandations issues de vérifications du respect de la vie privée et de la sécurité de l'information, d'évaluations des incidences sur la vie privée et d'enquêtes sur des plaintes en matière de protection de la vie privée, ou sur des violations et des incidents liés au respect de la vie privée et à la sécurité de l'information;
- application continue et confirmée, par la personne ou l'entité prescrite, des politiques, procédures et pratiques liées au respect de la vie privée;
- harmonisation des politiques, procédures et pratiques liées au respect de la vie privée et la sécurité de l'information qui sont mises en œuvre.

Le chef de la protection des renseignements personnels et avocat général ou le chef de la sécurité de l'information veillera à l'application du processus d'approbation requis. De par son mandat, le comité sur le respect de la vie privée, la confidentialité et la sécurité de l'ICIS est tenu d'examiner les politiques et protocoles de l'ICIS en matière de respect de la vie privée et de recommander les changements qui s'imposent. Le Conseil d'administration de l'ICIS doit approuver au préalable toute modification du contenu de la Politique de respect de la vie privée, 2010. Le processus d'approbation de tout autre changement dépend de la nature du document et pourrait nécessiter l'approbation, par exemple, du Comité exécutif, du Comité de la haute direction ou d'un autre comité interne).

b. Normes, procédures et protocoles

L'ICIS dispose d'un ensemble exhaustif de normes, de procédures et de protocoles qui appuient les objectifs des politiques de respect de la vie privée et de sécurité de l'information, notamment en ce qui concerne le cycle de vie de l'information sécurisée, la gestion des incidents et l'utilisation acceptable des systèmes d'information.

c. Formation et sensibilisation

Le Cadre de respect de la vie privée et de sécurité de l'ICIS s'appuie sur un programme interne de formation et de sensibilisation qui regroupe diverses initiatives clés.

- Le site Web interne de l'ICIS fournit des renseignements complets sur les programmes de respect de la vie privée et de sécurité de l'information de l'organisme ainsi que des liens vers les politiques, normes, lignes directrices et autres instruments connexes.
- La *Politique en matière de formation sur le respect de la vie privée et la sécurité* de l'ICIS exige une formation obligatoire et vérifiable sur le respect de la vie privée et la sécurité, qui comprend
  - une séance d'orientation pour tous les nouveaux employés sur le respect de la vie privée et la sécurité;
  - une formation continue en matière de respect de la vie privée et de sécurité, au moins une fois par année pour les employés actuels;
  - une formation spéciale et des séances d'information régulières sur les nouvelles tendances en matière de respect de la vie privée et de sécurité de l'information.
- Dans le contexte des programmes annuels de sensibilisation de l'ICIS en matière de respect de la vie privée et de sécurité de l'information, septembre est le mois de la sensibilisation à la sécurité de l'information et janvier, le mois de la sensibilisation au respect de la vie privée. Des séances de formation croisée et de l'aiguillage en matière de respect de la vie privée et de sécurité de l'information sont offerts pendant ces 2 mois.

d. Cycle de vie de l'information sécurisée

L'ICIS a mis en place des mesures de protection administratives, techniques et physiques en vue de protéger les renseignements personnels sur la santé tout au long de leur cycle de vie : création et collecte, accès, conservation et stockage, utilisation, divulgation et élimination. Un ensemble complet de politiques, ainsi que les normes, lignes directrices et procédures normalisées connexes, reflètent les pratiques exemplaires en matière de respect de la vie privée et de sécurité de l'information, afin de garantir la confidentialité, l'intégrité et la disponibilité des actifs informationnels de l'ICIS. Mentionnons par exemple la *Politique sur la sécurité de l'information confidentielle et l'utilisation d'appareils mobiles et de supports d'information amovibles*, qui précise les contrôles nécessaires pour garantir la protection de l'information stockée dans des appareils mobiles ou amovibles, ainsi que les exigences rigoureuses relatives au chiffrement des renseignements personnels.

e. Protocole de gestion des incidents

Le *Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité* exige une réaction coordonnée, ordonnée et rapide lorsque des événements et des incidents liés au respect de la vie privée et à la sécurité sont décelés, afin que soient réduits au minimum les éventuels préjudices pour l'ICIS ou les personnes dont les renseignements personnels pourraient être compromis.

Tous les employés de l'ICIS doivent assurer la protection des banques de données de l'organisme et ont l'obligation de signaler les incidents relatifs au respect de la vie privée et à la sécurité, y compris toute lacune apparente au chapitre des procédures et contrôles.

Le programme de formation de l'ICIS sur le respect de la vie privée et la sécurité aborde la sensibilisation au protocole de gestion des incidents à l'échelle de l'organisme.

f. Ententes

L'ICIS est la principale source d'information et de données sur la santé fiables au Canada. Les hôpitaux, les régies régionales de la santé, les professionnels de la santé et les gouvernements confient à l'ICIS des données confidentielles. L'ICIS est donc déterminé à préserver la confiance de ses fournisseurs de données en concluant des ententes d'échange d'information en vertu desquelles il s'engage à garantir la confidentialité et la sécurité de ses banques de données.

L'ICIS est également responsable de l'administration d'un programme de demande de données de clients externes à des fins de recherche ou à d'autres fins qui s'inscrivent dans son mandat. Toute personne qui souhaite recevoir de l'information doit d'abord signer une entente visant le respect des conditions et restrictions relatives à la collecte, au but, à l'utilisation, à la sécurité, à la divulgation et au retour ou à l'élimination des données. Cette entente permet également à l'ICIS de procéder à une vérification de conformité sur préavis raisonnable.

g. Gestion des tiers fournisseurs

Les ententes d'impartition et celles avec les fournisseurs qui portent sur de l'information confidentielle ou des systèmes d'information se présentent sous forme de contrats écrits qui incluent les exigences relatives au respect de la vie privée et de la sécurité de l'information, les obligations en matière de confidentialité et les objectifs de niveau de service.

L'accès aux banques de données ou à toute autre source d'information commerciale par des fournisseurs est régi par les politiques et procédures de l'ICIS en matière de respect de la vie privée et de sécurité de l'information.

h. Communications externes

Les renseignements relatifs aux pratiques et aux programmes de respect de la vie privée et de sécurité de l'information sont accessibles au public sur le site Web de l'ICIS. Ils comprennent un aperçu des programmes de respect de la vie privée et de sécurité de l'information, diverses politiques et normes clés, des rapports et des publications ainsi que les coordonnées du chef de la protection des renseignements personnels et avocat général. Les évaluations des incidences sur la vie privée et l'énoncé des objectifs de chaque banque de données sont également accessibles à icis.ca.

L'ICIS attache de l'importance au rôle des organismes fédéraux, provinciaux et territoriaux de réglementation en matière de vie privée et sollicite activement leur point de vue et leurs commentaires au besoin.

5 Vérifications, conformité et rapports

Le *Code de conduite de l'ICIS* définit les comportements éthiques et professionnels au chapitre des relations de travail, des renseignements — dont les renseignements personnels sur la santé — et du milieu de travail. Les employés sont tenus de respecter le contenu du code ainsi que l'ensemble des politiques, des procédures et des protocoles de l'ICIS, y compris la Politique de respect de la vie privée. La conformité au Programme de respect de la vie privée de l'ICIS fait l'objet d'un contrôle dans le cadre du Programme de vérification du respect de la vie privée de l'ICIS, fondé sur les risques, conformément à un plan de vérification pluriannuel. Les cas de non-conformité sont traités conformément au *Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité de l'information* de l'ICIS. Les manquements au code sont référés aux Ressources humaines, au besoin, et peuvent entraîner des mesures disciplinaires allant jusqu'au congédiement.

a. Programme de vérification du respect de la vie privée

Le chef de la protection des renseignements personnels et avocat général est responsable du Programme de vérification du respect de la vie privée, qui permet de surveiller l'observation des exigences législatives et réglementaires, des politiques internes et des obligations contractuelles visant le respect de la vie privée. Le mandat du Programme de vérification du respect de la vie privée (document intitulé *Privacy Audit Program — Terms of Reference*) définit 2 types de vérifications du respect de la vie privée :

- Les vérifications internes du respect de la vie privée permettent d'évaluer l'observation, par le personnel, des politiques de l'ICIS sur le respect de la vie privée et des pratiques exemplaires en matière de respect de la vie privée, ou portent sur la gestion d'une question particulière au sein de l'organisme. Ces vérifications sont effectuées selon les besoins et souvent dans le contexte des processus internes d'intervention en cas d'incident et de violation du respect de la vie privée. Elles peuvent aussi résulter de demandes externes telles qu'une enquête, une recommandation ou une ordonnance d'un commissaire à la protection de la vie privée ou d'un ombudsman.
- Les vérifications de tiers ciblent les destinataires externes de données de l'ICIS. Elles permettent d'évaluer le respect des conditions de l'entente qui régit l'utilisation des données de l'ICIS. Les vérifications donnent également lieu à des recommandations visant à résoudre les problèmes cernés. Pour déterminer les vérifications qui seront effectuées durant l'année, l'ICIS tient compte de nombreux critères, dont la confidentialité des données, la complexité du plan de gestion des données de recherche et la connaissance éclairée des risques selon les activités permanentes de contrôle de la conformité du Secrétariat à la vie privée et aux services juridiques (p. ex. le processus annuel de certification de conformité des destinataires de données).

b. Programme de vérification de la sécurité de l'information

Le chef de la sécurité de l'information est responsable du programme de vérification de la sécurité de l'information de l'ICIS. Ce programme précise un certain nombre de vérifications obligatoires, notamment les suivantes :

- conformité à la norme ISO/IEC 27001:2013;
- accès aux renseignements personnels sur la santé par les employés à l'interne;
- évaluation de la vulnérabilité et test d'intrusion sur l'infrastructure physique et réseau de l'ICIS.

Outre les vérifications obligatoires, le chef de la sécurité de l'information effectue un certain nombre de vérifications spéciales chaque année.

L'ICIS peut procéder à d'autres vérifications du respect de la vie privée et de la sécurité de l'information dans les circonstances suivantes :

- ordonnance ou décision d'un commissaire à la protection de la vie privée;
- violation ou incident lié au respect de la vie privée ou à la sécurité;
- demande formulée par le Conseil d'administration, l'équipe de haute direction, le chef de la protection des renseignements personnels et avocat général ou le chef de la sécurité de l'information de l'ICIS.

c. Examen externe de l'ICIS

Les programmes de respect de la vie privée et de sécurité de l'information de l'ICIS sont assujettis à un examen tous les 3 ans par le commissaire à l'information et à la protection de la vie privée de l'Ontario. Cet examen assure à l'ICIS et à ses intervenants une vérification objective et neutre qui confirme que les pratiques et procédures en vigueur à l'ICIS protègent adéquatement la vie privée des personnes visées par les renseignements personnels sur la santé qu'il recueille, et que la confidentialité de cette information est adéquatement assurée. Le dernier examen, qui a eu lieu en 2017, a permis à l'ICIS de renouveler son statut d'entité prescrite en vertu du paragraphe 45 de la LPRPS.

d. Surveillance de la conformité et rapports

Les recommandations découlant des vérifications du respect de la vie privée et de la sécurité de l'information effectuées par l'ICIS font l'objet d'un suivi et d'une surveillance par l'équipe de la haute direction au moyen d'un registre de recommandations à l'échelle de l'organisme. La responsabilité de la mise en œuvre des recommandations incombe au directeur ou au vice-président touché.

Le chef de la protection des renseignements personnels et avocat général doit soumettre annuellement au Conseil d'administration un rapport qui fait état des réalisations ayant trait au programme de respect de la vie privée, y compris des évaluations des incidences sur la vie privée, des vérifications du respect de la vie privée, de l'élaboration de politiques, de la formation et des autres développements pertinents.

Dans le cadre de son programme de vérification du respect de la vie privée, l'ICIS prépare des rapports sur toutes les vérifications effectuées à l'intention du Comité de gouvernance et de respect de la vie privée du Conseil d'administration de l'ICIS. Dans le cadre du programme de vérification de la sécurité, le chef de la sécurité de l'information fait état des résultats de toutes les vérifications externes au Comité des finances et de la vérification du Conseil d'administration.

Le chef de la protection des renseignements personnels et avocat général ou le chef de la sécurité de l'information doit également soumettre au Conseil d'administration, le cas échéant, des présentations sur des questions sensibles concernant le respect de la vie privée ou la sécurité.

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

Le présent cadre sera actualisé en fonction de l'évolution des pratiques en matière de respect de la vie privée et de sécurité de l'information.

Renseignements supplémentaires

L'ICIS fournit dans son site Web des renseignements sur ses programmes de respect de la vie privée et de sécurité de l'information.

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

23135-1020