Institut canadien d'information sur la santé

Politique sur la sécurité de l'information

Introduction

L'Institut canadien d'information sur la santé (ICIS) s'engage à protéger la vie privée des personnes et à assurer la sécurité de leurs renseignements personnels sur la santé.

L'ICIS est un collecteur secondaire de renseignements personnels sur la santé. Pour être en mesure de recueillir ces renseignements, l'ICIS a conclu des ententes bilatérales et de partage de données avec la plupart des autorités compétentes et d'autres intervenants du système de santé de partout au Canada. En vertu de ces ententes, l'ICIS est tenu par des obligations contractuelles d'assurer la sécurité et la confidentialité des renseignements qu'il reçoit de ses fournisseurs de données. De plus, 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 assujetti à la surveillance indépendante du Bureau du commissaire à l'information et à la protection de la vie privée (CIPVP) de l'Ontario et doit faire approuver tous les 3 ans ses pratiques et procédures de gestion de l'information par le CIPVP. Ce processus de surveillance garantit aux intervenants que les pratiques de gestion de l'information de l'ICIS sont conformes à la LPRPS de l'Ontario ainsi qu'aux normes de respect de la vie privée et de sécurité du CIPVP. Par conséquent, l'ICIS se conforme à la LPRPS et à toutes les autres lois applicables en matière de respect de la vie privée.

L'ICIS s'emploie à protéger son système de technologie de l'information, à sécuriser ses banques de données ainsi qu'à protéger les renseignements sur la santé qu'il détient au moyen de mesures de sécurité administratives, physiques et techniques appropriées, selon la sensibilité de l'information. Ces mesures protègent les banques de données de l'ICIS contre le vol, la perte, l'utilisation ou la divulgation non autorisée ainsi que la reproduction, la modification ou l'élimination non autorisée.

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

Objectifs

La *Politique sur la sécurité de l’information* vise à

- orienter et appuyer le personnel de l’ICIS au chapitre de la sécurité de l’information à des fins de conformité aux exigences opérationnelles et aux lois et règlements en vigueur;
- préciser les responsabilités du personnel de l’ICIS en matière de sécurité de l’information.

Portée

La présente politique et l’ensemble des normes, lignes directrices et procédures connexes s’appliquent à tous les membres du personnel, entrepreneurs, experts-conseils, employés temporaires et autres employés de l’ICIS.

Politique

La direction de l’ICIS appuie l’élaboration et la tenue à jour du programme de sécurité de l’information conformément aux exigences opérationnelles et législatives ainsi qu’aux exigences en matière de respect de la vie privée. Ce programme doit comprendre, au minimum, les objectifs et pratiques de contrôle suivants :

- un cadre de gouvernance sur la sécurité;
- la gestion des risques liés au respect de la vie privée et à la sécurité;
- l’évaluation continue des politiques, procédures et pratiques de sécurité mises en œuvre;
- un programme de sensibilisation et de formation à la sécurité de l’information à l’intention de tous les employés;
- des politiques, normes, pratiques et procédures portant sur la sécurité physique des lieux, la sécurité des installations de traitement de l’information et la protection de l’information pendant tout son cycle de vie (création, acquisition, conservation et stockage, utilisation, divulgation et élimination), y compris des politiques et procédures liées aux appareils mobiles, à l’accès à distance et à la sécurité des données au repos;
- un processus de gestion de l’accès à l’information et aux installations de traitement de l’information;
- l’acquisition, le développement et la maintenance de systèmes sécuritaires;
- une gestion des vulnérabilités techniques;
- un programme de cybersécurité;
- des audits de sécurité;
- l’usage acceptable de la technologie de l’information;
- la sécurité de la sauvegarde et de la récupération;
- la continuité des opérations et la reprise après sinistre;

- la gestion des incidents liés à la sécurité de l’information;
- la protection contre les programmes malveillants et les codes mobiles;
- l’amélioration continue du programme de sécurité de l’information.

L’ICIS veille à ce que des mesures raisonnables soient prises pour garantir que les renseignements personnels sur la santé sont protégés contre le vol ou la perte, ainsi que contre l’accès, la divulgation, la copie, l’usage, la modification et la destruction non autorisés.

Responsabilités

Les personnes et les groupes de l’ICIS qui suivent doivent assumer des responsabilités précises à l’égard du programme de sécurité de l’information :

- tout le personnel de l’ICIS
- la haute direction
- le vice-président et dirigeant principal de l’information
- le chef de la sécurité de l’information
- le chef de la protection des renseignements personnels et avocat général
- le directeur, Ressources humaines et Administration
- le gestionnaire, Sécurité de l’information

Personnel de l’ICIS

Tous les renseignements dont l’ICIS a la garde et le contrôle constituent des actifs de l’organisme et doivent faire l’objet d’une gestion sécuritaire tout au long de leur cycle de vie. La responsabilité fondamentale de protéger les actifs informationnels de l’ICIS incombe à tous les membres du personnel, qui doivent comprendre et accepter leur obligation de protéger ces actifs tout au long de leur cycle de vie (création, acquisition, conservation et stockage, utilisation, divulgation et élimination). Les membres du personnel de l’ICIS peuvent créer, acquérir, conserver, stocker, utiliser, divulguer, transférer ou éliminer les renseignements uniquement en respectant les politiques, normes et lignes directrices de l’ICIS et les lois et règlements en vigueur.

Les membres du personnel de l’ICIS doivent en tout temps recourir à des pratiques conformes aux politiques, procédures, normes et lignes directrices en matière de sécurité de l’information qui ont été publiées. Ils sont par ailleurs tenus de signaler tout incident lié à la sécurité de l’information et tout incident présumé lié à la sécurité de l’information dès qu’ils en ont connaissance. (Pour obtenir des précisions, consulter le *Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité de l’information* de l’ICIS.)

Haute direction

La haute direction fournit les conseils et le soutien nécessaires à l’élaboration et à la tenue à jour du programme de sécurité de l’information, conformément aux exigences en matière de respect de la vie privée, aux exigences légales et aux objectifs des stratégies commerciales.

Ce soutien consiste notamment à

- intégrer les objectifs de sécurité de l’information aux processus pertinents;
- fournir des directives claires et un soutien administratif manifeste à l’égard des initiatives touchant la sécurité de l’information;
- fournir les ressources nécessaires au maintien de la sécurité de l’information;
- approuver l’attribution de rôles et responsabilités précis en ce qui concerne la sécurité de l’information dans l’ensemble de l’organisme.

Vice-président et dirigeant principal de l’information

Le vice-président et dirigeant principal de l’information, qui représente le Comité exécutif de l’ICIS, assume la pleine responsabilité de la sécurité de l’information. Il doit veiller à ce que les objectifs en matière de sécurité de l’information soient définis, respectent les exigences de l’organisme et soient pris en compte dans le cadre du programme de sécurité de l’information.

Chef de la sécurité de l’information

Relevant du vice-président et dirigeant principal de l’information, le chef de la sécurité de l’information est responsable de diriger le programme de sécurité de l’information de l’ICIS, notamment de définir les buts, objectifs et paramètres du programme conformément au plan stratégique de l’ICIS et à son programme de respect de la vie privée, de manière à ce que les principes, politiques, procédures et pratiques en matière de sécurité de l’organisme favorisent la protection de ses données. Le chef de la sécurité de l’information gère et coordonne la conception, la mise en œuvre, l’exploitation et la maintenance du Système de gestion de la sécurité de l’information (SGSI) de l’ICIS, selon son mandat.

Il incombe par ailleurs au chef de la sécurité de l’information de favoriser activement un environnement propice à la sécurité de l’information en dirigeant et en appuyant, à l’interne et à l’externe, des activités visant à mieux faire connaître les principes, politiques et procédures de sécurité de l’information de l’ICIS.

Chef de la protection des renseignements personnels et avocat général

Le chef de la protection des renseignements personnels et avocat général est responsable d’informer le chef de la sécurité de l’information de ses obligations législatives, réglementaires et contractuelles. Il doit en outre collaborer avec le chef de la sécurité de l’information aux aspects clés des programmes de respect de la vie privée et de sécurité de l’information, qui comprennent notamment

- la gestion des risques liés au respect de la vie privée et à la sécurité;
- la gestion des incidents liés au respect de la vie privée et à la sécurité;
- la formation et la sensibilisation.

Directeur, Ressources humaines et Administration

Le directeur, Ressources humaines et Administration, conformément aux objectifs de l’ICIS en matière de sécurité de l’information, est responsable

- de la sécurité physique des lieux;
- des politiques, procédures et pratiques en matière de gestion des documents et de l’information;
- de la sécurité des processus liés aux ressources humaines.

Gestionnaire, Sécurité de l’information

Le gestionnaire, Sécurité de l’information, est responsable de la supervision du programme de sécurité de l’information de l’ICIS. Plus particulièrement, le gestionnaire s’engage à créer et à maintenir

- un programme de cybersécurité conforme aux objectifs de l’ICIS en matière de sécurité de l’information;
- un ensemble de politiques, de procédures, de normes et de lignes directrices sur la sécurité de l’information, afin d’assurer la confidentialité, l’intégrité et l’accessibilité des actifs informationnels de l’ICIS.

Le gestionnaire, Sécurité de l’information est également responsable de la conformité et de la certification continues ayant trait aux pratiques de l’ICIS en matière de sécurité de l’information, y compris des exigences au titre de la LPRPS.

Conformité, vérification et application

Le *Code de conduite de l’ICIS* (en anglais seulement) définit le comportement éthique et professionnel attendu en ce qui concerne les relations professionnelles, les renseignements (y compris les renseignements personnels sur la santé) et le milieu de travail. Tous les employés sont tenus de se conformer au code et à l’ensemble des politiques, protocoles et procédures de l’ICIS. La conformité est surveillée dans le cadre des programmes de vérification du respect de la vie privée et de la sécurité de l’information, et 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. Tout manquement au code — y compris aux politiques, procédures et protocoles de respect de la vie privée et de sécurité — est signalé aux Ressources humaines, s’il y a lieu, et peut entraîner des mesures disciplinaires pouvant aller jusqu’au congédiement.

Glossaire

Documents commerciaux

Les documents commerciaux comprennent toute information créée, reçue ou tenue à jour par l’ICIS sous forme de données probantes et d’information dans le cadre de ses activités ou conformément à ses obligations légales.

Les documents commerciaux peuvent être constitués d’éléments physiques ou électroniques et comprennent notamment

- les renseignements recueillis auprès des fournisseurs de données, des clients et des intervenants;
- les documents officiels de l’organisme;
- les documents temporaires;
- les documents relevant du domaine public qui appartiennent à l’ICIS.

Actif informationnel

Pour les besoins de la présente politique, l’information et l’actif informationnel englobent

- tous les renseignements sur la santé que l’ICIS tient à jour en vue de réaliser son mandat;
- tous les documents commerciaux de l’organisme, sans égard à leur classification de sécurité.

L’information peut être constituée d’éléments physiques ou électroniques.

Sécurité de l’information

La sécurité de l’information fait référence aux concepts, techniques, mesures techniques et mesures administratives servant à empêcher l’acquisition, l’altération, la divulgation, la manipulation, la modification ou la perte, délibérée ou accidentelle et non autorisée, des actifs informationnels.

Personnel de l’ICIS

Toute personne qui travaille à l’ICIS, y compris les employés à temps plein ou à temps partiel, les personnes en détachement, les travailleurs temporaires, les étudiants et les employés contractuels, ainsi que les experts-conseils externes ou tout autre tiers fournisseur de services dont le rôle comporte la responsabilité du stockage sécuritaire des renseignements personnels sur la santé.

Autres renseignements :

securite@icis.ca

Comment citer ce document :
Institut canadien d’information sur la santé. *Politique sur la sécurité de l’information*. Ottawa, ON : ICIS; 2021.