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 provinces 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 à la population canadienne 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.

Objet

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

- orienter et appuyer la direction et 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 de la direction et des membres du personnel 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 employés, 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;
- le Cadre de 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);
- 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;
- 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.

Les obligations et les responsabilités qui incombent à la direction et au personnel à l’égard du programme de sécurité de l’information sont décrites ci-dessous.

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 :

- l’ensemble du personnel
- la haute direction
- le dirigeant principal de l’information
- le chef de la sécurité de l’information
- le conseiller principal, Sécurité de l’information
- le directeur, Ressources humaines et Administration

Ensemble du personnel

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 l’ensemble du personnel; ce dernier doit comprendre et accepter son obligation de protéger ces actifs tout au long de leur cycle de vie (création, acquisition, conservation et stockage, utilisation, divulgation et élimination). Le personnel de l’ICIS peut 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.

Le personnel doit 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. Il est par ailleurs tenu de signaler tout incident lié à la sécurité de l’information et tout incident présumé lié à la sécurité de l’information dès qu’il en a 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.

Dirigeant principal de l’information

Le 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 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.

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.

Conseiller principal, Sécurité de l’information

Le conseiller principal, Sécurité de l’information, est responsable de la supervision quotidienne du SGSI de l’ICIS ainsi que de la création et de la gestion des principales initiatives de sécurité en matière de technologie de l’information. Il est responsable du développement et du respect des pratiques nécessaires afin que la sécurité et l’intégrité des banques de données de l’ICIS soient toujours assurées conformément au cadre de respect de la vie privée et de sécurité de l’ICIS et à l’ensemble de ses politiques, procédures, normes et lignes directrices visant le respect de la vie privée et la sécurité. Il lui incombe également de s’assurer que l’ICIS recourt aux pratiques exemplaires de l’industrie au chapitre de la sécurité de l’information et respecte les attentes et exigences des principaux intervenants externes (p. ex. le Commissaire à l’information et à la protection de la vie privée de l’Ontario).

Conformité

Le Code de conduite de l’ICIS définit les comportements éthiques et professionnels au chapitre des relations, des renseignements, y compris des renseignements personnels sur la santé, et du milieu de travail. Les employés sont tenus de se conformer au code ainsi qu’aux politiques, procédures et protocoles de l’ICIS. La conformité aux programmes de respect de la vie privée et de sécurité de l’ICIS fait l’objet d’un contrôle 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. Toutes contraventions au code, y compris toutes violations des politiques, procédures et protocoles de respect de la vie privée et de sécurité, sont référées aux Ressources humaines, au besoin, et peuvent entraîner des mesures disciplinaires allant 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

Le personnel comprend tous les employés à temps plein, à temps partiel et occasionnels de l’ICIS, y compris les personnes qui travaillent à l’ICIS en détachement, les étudiants, les bénévoles, les entrepreneurs et les experts-conseils.

Autres renseignements

securite@icis.ca