Institut canadien d'information sur la santé

Politique en matière de formation sur le respect de la vie privée et la sécurité

But

La présente politique a pour objectif d'énoncer les exigences relatives à une formation traçable et obligatoire sur le respect de la vie privée et la sécurité à l'intention de l'ensemble du personnel de l'ICIS.

Il est essentiel d'offrir un programme de formation solide pour assurer la mise en place et le maintien d'une culture qui favorise le respect de la vie privée et la sécurité. Un tel programme représente aussi une mesure préventive essentielle contre la collecte, l'utilisation et la divulgation non autorisées de renseignements personnels sur la santé et contre l'accès non autorisé à ceux-ci. La formation visera principalement à réduire les risques pour l'organisme et aidera le personnel à réaliser le mandat de l'ICIS, conformément à ses politiques et aux lois applicables.

Portée

La présente politique vise l'ensemble du personnel de l'ICIS, y compris les employés à temps plein et à temps partiel de l'ICIS, les employés contractuels, les personnes qui travaillent à l'ICIS en détachement, les étudiants et certains consultants de services professionnels externes qui ont besoin d'accéder aux données de l'ICIS ou aux systèmes d'information, conformément à la Politique d'utilisation acceptable des systèmes d'information de l'ICIS. Toute exception aux exigences en matière de formation obligatoire sur le respect de la vie privée et la sécurité doit être approuvée par le chef de la protection des renseignements personnels, le chef de la sécurité de l'information ou les deux.

Politique

Interprétation

1. La présente politique sera interprétée d'après 2 principes directeurs :
    a. la formation sur le respect de la vie privée et la sécurité est obligatoire;
    b. la formation sur le respect de la vie privée et la sécurité est traçable aux fins de conformité.

Formation obligatoire sur le respect de la vie privée et la sécurité

2. Tout nouveau membre du personnel de l'ICIS doit réussir la formation de base obligatoire de l'ICIS sur le respect de la vie privée et la sécurité dans les 15 jours suivant son entrée en fonction et avant d'obtenir l'accès à tout renseignement personnel sur la santé. La formation comprend les rudiments du respect de la vie privée et de la sécurité, l'utilisation acceptable des systèmes d'information de l'ICIS, les risques liés à l'ingénierie sociale (hameçonnage) et la gestion des incidents.
3. La date d'entrée en fonction correspond à la dated'embauche inscrite dans la lettre d'offre d'emploi ou dans le contrat de l'ICIS.

Formation de mise à jour annuelle

4. L'ensemble du personnel de l'ICIS doit réussir la formation de mise à jour annuelle obligatoire sur le respect de la vie privée et la sécurité, avant le 31 janvier, à compter de l'année suivant l'année d'entrée en fonction. Le personnel doit en outre remplir le formulaire intitulé *Renouvellement annuel de l'entente entre l'ICIS et ses employés concernant le respect de l'information confidentielle et de la vie privée*.

Formation supplémentaire

5. En plus de satisfaire aux exigences mentionnées ci-dessus, le personnel de l'ICIS doit réussir les séances de formation supplémentaires obligatoires sur le respect de la vie privée et la sécurité exigées par le chef de la protection des renseignements personnels et le chef de la sécurité de l'information. Par exemple, une formation supplémentaire peut être exigée à la suite d'un cas de violation du respect de la vie privée ou d'un incident lié à la sécurité, de la publication des résultats d'une vérification du respect de la vie privée ou de la sécurité, ou de l'adoption ou la mise en œuvre de nouvelles politiques et procédures.

Contenu du programme de formation sur le respect de la vie privée et la sécurité

6. Le chef de la protection des renseignements personnels est chargé de déterminer le contenu de la formation sur le respect de la vie privée, et le chef de la sécurité de l'information est chargé de déterminer le contenu de la formation sur la sécurité.
7. Les éléments suivants doivent faire partie du programme de formation de l'ICIS sur le respect de la vie privée et la sécurité aux fins d'exactitude et de pertinence :
    - la désignation de l'ICIS en vertu de la *Loi sur la protection des renseignements personnels sur la santé* (LPRPS) de l'Ontario et les obligations et responsabilités qui découlent de cette désignation;
    - la nature des renseignements personnels sur la santé qui sont recueillis et les personnes ou entités auprès desquelles ces renseignements sont habituellement recueillis;

- les buts pour lesquels des renseignements personnels sur la santé sont recueillis et utilisés et la façon dont cette collecte et cette utilisation sont autorisées en vertu de la LPRPS;
- les restrictions imposées à l'égard de l'accès aux renseignements personnels sur la santé et de leur utilisation par les employés;
- la procédure qui doit être respectée lorsqu'un employé est appelé à divulguer des renseignements personnels sur la santé;
- une vue d'ensemble des politiques, procédures et pratiques de l'ICIS visant le respect de la vie privée et la sécurité, et les obligations qui en découlent;
- les conséquences de la violation des politiques, procédures et pratiques prévues en matière de respect de la vie privée et de sécurité;
- une explication du programme sur le respect de la vie privée, y compris les activités principales du programme ainsi que celles du chef de la protection des renseignements personnels;
- une explication du programme sur la sécurité, y compris les activités principales du programme ainsi que celles du chef de la sécurité de l'information et du conseiller principal, Sécurité de l'information;
- les mesures de sécurité administratives, techniques et physiques mises en place par l'ICIS pour protéger les renseignements personnels sur la santé contre le vol, la perte et l'utilisation ou la divulgation non autorisée, et pour protéger les dossiers contenant des renseignements personnels sur la santé contre la reproduction, la modification ou la destruction non autorisée;
- les obligations et responsabilités des employés dans la mise en œuvre des mesures de sécurité administratives, techniques et physiques mises en place par l'ICIS;
- une discussion de la nature et du but de l'entente de confidentialité que les employés doivent signer et les dispositions principales de cette entente de confidentialité;
- une explication du *Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité de l'information* et des obligations et responsabilités qui incombent aux employés afin que les incidents liés à la vie privée et à la sécurité de l'information soient repérés, signalés, confinés, fassent l'objet d'une enquête et soient corrigés.

Responsabilité du suivi de l'achèvement de la formation de mise à jour annuelle

8. Le Secrétariat à la vie privée et aux services juridiques est chargé d'assurer le suivi de l'achèvement de la formation de mise à jour annuelle sur le respect de la vie privée et la sécurité; il doit faire part du taux d'achèvement au Comité de la haute direction.

Conséquences du non-respect

9. Les membres du personnel doivent satisfaire aux exigences en matière de formation mentionnées ci-dessus avant que soit accordé le premier accès aux données, puis chaque année par la suite, pour conserver leurs privilèges d'accès.
10. Si la formation obligatoire sur le respect de la vie privée et la sécurité n'est pas complétée avec succès, l'accès aux données ou aux autres composantes de l'infrastructure de l'ICIS (p. ex. le réseau de l'ICIS) pourrait être refusé ou révoqué.
11. La décision de refuser ou révoquer l'accès aux données sera prise par le chef de la sécurité de l'information et le chef de la protection des renseignements personnels, en consultation avec le directeur, Ressources humaines, dans le cas des employés de l'ICIS, ou avec le directeur ou le gestionnaire de la section contractante dans le cas des consultants de services professionnels externes.
12. Outre le refus ou la révocation de l'accès aux données, le fait de ne pas réussir la formation obligatoire peut entraîner des sanctions disciplinaires, y compris le congédiement ou la cessation des relations de travail avec l'ICIS.

Conformité

13. Le *Code de conduite* de l'ICIS définit les comportements éthiques et professionnels au chapitre des relations de travail, 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 au Programme 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. Les cas de violation du code, y compris les cas de violation des politiques, procédures et protocoles de respect de la vie privée et de sécurité, sont soumis aux Ressources humaines, au besoin, et peuvent entraîner des mesures disciplinaires allant jusqu'au congédiement.

Procédures et documents connexes

- *Procédure : Politique en matière de formation sur le respect de la vie privée et la sécurité*
- *Code de conduite*
- *Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité de l'information*

Pour de plus amples renseignements :

vieprivee@icis.ca