

Politique d'évaluation des incidences sur la vie privée

But

La présente politique vise à assurer l'élaboration et la mise à jour des évaluations des incidences sur la vie privée de manière transparente, conformément aux ordonnances, directives, feuillets de documentation et pratiques exemplaires émis par les commissaires au respect de la vie privée. En tant qu'entité prescrite en vertu de la *Loi sur la protection des renseignements personnels sur la santé* (LPRPS) de l'Ontario, l'ICIS doit notamment procéder à l'évaluation des incidences sur la vie privée dans le cadre de son programme de respect de la vie privée.

Les évaluations des incidences sur la vie privée revêtent une importance capitale aux yeux de l'ICIS et des intervenants. L'application de la présente politique et des évaluations des incidences sur la vie privée qui en découlent démontre que les principes en matière de respect de la vie privée sont pris en compte pendant la conception, la mise en œuvre et la mise à jour des programmes, des initiatives, des processus et des systèmes de l'ICIS. L'évaluation des incidences sur la vie privée comprend l'élaboration de mesures d'atténuation et, si possible, d'élimination des risques connus, conformément au *Cadre de gestion des risques liés au respect de la vie privée et à la sécurité* de l'ICIS et à la politique connexe.

À l'ICIS, le chef de la protection des renseignements personnels est l'autorité qui gère le programme de respect de la vie privée au quotidien, alors que le chef de la sécurité de l'information est l'autorité qui gère le programme de sécurité de l'information au quotidien.

À l'ICIS, les évaluations des incidences sur la vie privée sont la responsabilité du directeur de la section, mais leur réalisation est une responsabilité partagée. Le personnel de la section (ou le gestionnaire de projets, selon le cas) ainsi que le personnel de la Direction de la vie privée et des services juridiques collaborent à l'élaboration de ces évaluations. Le rapport d'évaluation des incidences sur la vie privée peut être rédigé par le personnel de la section, aidé par le personnel de la Direction de la vie privée et des services juridiques, ou vice-versa. Le recours aux consultants externes en respect de la vie privée pour la réalisation d'une évaluation des incidences sur la vie privée doit être coordonné par la Direction de la vie privée et des services juridiques.

Portée

La présente politique porte sur les programmes, les initiatives, les processus et les systèmes de l'ICIS, lesquels comprennent des activités de collecte, de consultation, d'utilisation ou de divulgation de renseignements personnels sur la santé, sur les travailleurs de la santé et sur les employés (collectivement appelés « renseignements personnels »).

Définitions

L'évaluation des incidences sur la vie privée est un processus d'évaluation des questions de respect de la vie privée, de confidentialité et de sécurité associées à la collecte, à l'utilisation ou à la divulgation des renseignements personnels, en fonction des 10 principes énoncés dans le *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation.

Les renseignements personnels sont des renseignements factuels ou subjectifs, tous formats confondus, qui peuvent être utilisés, seuls ou avec d'autres renseignements, pour identifier une personne, photographies et vidéos comprises. Les renseignements personnels ne comprennent pas les renseignements liés à la vie professionnelle d'une personne (poste ou titre, adresse professionnelle, numéro de téléphone professionnel, adresse courriel professionnelle, etc.).

Les renseignements personnels sur la santé sont des renseignements sur la santé qui identifient une personne ou qui peuvent être utilisés ou manipulés selon une méthode raisonnablement prévisible pour identifier une personne, ou qui peuvent être associés, au moyen d'une méthode raisonnablement prévisible, à d'autres renseignements qui identifient une personne.

Les renseignements personnels sur les travailleurs de la santé sont des renseignements sur la santé qui identifient un dispensateur de services de santé ou qui peuvent être utilisés ou manipulés selon une méthode raisonnablement prévisible pour identifier un dispensateur de services de santé, ou qui peuvent être associés, au moyen d'une méthode raisonnablement prévisible, à d'autres renseignements qui identifient un dispensateur de services de santé.

Les renseignements personnels sur les employés sont des renseignements personnels sur une personne qui sont recueillis, utilisés ou communiqués aux fins d'établissement, de gestion ou de cessation d'une relation d'emploi entre l'ICIS et cette personne. Ils comprennent notamment des renseignements ayant trait au processus d'embauche, à l'administration de la rémunération et des programmes d'avantages sociaux, aux évaluations du rendement, aux mesures disciplinaires et à la planification de l'avancement.

Politique

1. Des évaluations des incidences sur la vie privée sont effectuées dans les circonstances suivantes :

- lorsque des programmes, des initiatives, des processus ou des systèmes subissent des changements importants en ce qui a trait à la collecte, à l'utilisation ou à la divulgation des renseignements personnels;
- lorsque la conception de programmes, d'initiatives, de processus ou de systèmes englobe la collecte, l'utilisation ou la divulgation de renseignements personnels, ou soulève des questions quant au respect de la vie privée — les évaluations des incidences sur la vie privée sont révisées et modifiées au besoin pendant l'étape de conception et de mise en œuvre;
- lorsque des programmes, des initiatives, des processus ou des systèmes comportent des incidences sur la vie privée, conformément aux recommandations du chef de la protection des renseignements personnels en consultation avec une section ou un bureau de gestion de projets.

Plus précisément, des évaluations des incidences sur la vie privée sont entreprises dès la conception de programmes, d'initiatives, de processus ou de systèmes, nouveaux ou mis à jour, et se poursuivent jusqu'à leur conception détaillée et leur mise en œuvre.

2. Les évaluations des incidences sur la vie privée doivent décrire au moins les éléments suivants :

- le programme, l'initiative, le processus ou le système visé;
- la nature et le type des renseignements personnels qui sont recueillis, utilisés ou divulgués ou qui pourraient l'être;
- les sources des renseignements personnels;
- les motifs pour lesquels les renseignements personnels sont recueillis, utilisés ou divulgués ou pourraient l'être;
- la raison pour laquelle les renseignements personnels sont nécessaires;
- le cheminement des renseignements personnels;
- les autorisations légales de recueillir, d'utiliser et de divulguer les renseignements personnels;
- les limites imposées aux droits de collecte, d'utilisation et de divulgation des renseignements personnels;

- les liens qui sont établis ou pourraient l'être entre les renseignements personnels et d'autres renseignements;
- les circonstances et bus précis selon lesquels les renseignements personnels sur la santé désanonymisés ou agrégés seront anonymisés, le cas échéant, ainsi que les conditions ou restrictions imposées à cet égard;
- la période de conservation des enregistrements contenant des renseignements personnels;
- la méthode sécurisée de conservation, de transfert ou de suppression des enregistrements contenant des renseignements personnels;
- le moyen utilisé pour accéder aux renseignements personnels, les utiliser, les modifier et les divulguer, et celui utilisé pour tenir des registres de contrôle de l'utilisation ou de la divulgation non autorisée;
- les risques de violation de la vie privée des personnes dont les renseignements personnels font ou feront partie de la banque de données, du système d'information, de la technologie ou du programme, et l'évaluation de ces risques;
- les recommandations visant à atténuer ou éliminer les risques de violation de la vie privée relevés;
- les dispositifs de protection administratifs, techniques et physiques qui ont été mis en œuvre ou qui pourraient l'être pour protéger les renseignements personnels.

Énoncés des objectifs des banques de données

3. À chaque banque de données de l'ICIS doivent correspondre une évaluation des incidences sur la vie privée et un énoncé des objectifs.
4. Le chef de la protection des renseignements personnels est l'autorité qui gère le programme de respect de la vie privée au quotidien en ce qui a trait aux énoncés des objectifs.
5. Les énoncés des objectifs sont inclus dans les évaluations des incidences sur la vie privée. Ces documents sont publiés sur le site Web public de l'ICIS et fournis sur demande aux dépositaires de renseignements sur la santé et aux autres personnes ou organismes qui soumettent les renseignements personnels sur la santé à la banque de données.
6. Le chef de la protection des renseignements personnels doit veiller à l'établissement d'un calendrier de réalisation des évaluations des incidences sur la vie privée.

Plan de gestion des données

7. Un plan de gestion des données peut remplacer dans certains cas une évaluation complète des incidences sur la vie privée si celle-ci n'est pas nécessaire, par exemple, dans le cas de la transmission à l'ICIS (approuvée en vertu de l'article 1 des procédures de respect de la vie privée de l'ICIS) d'un petit fichier de renseignements personnels sur la santé pour la réalisation d'une validation de principe. Il faut alors élaborer un plan de gestion des données visant le respect des processus requis de collecte, d'utilisation, de divulgation et de conservation ou de destruction des renseignements personnels sur la santé. Une évaluation complète des incidences sur la vie privée sera entreprise lorsqu'on déterminera qu'une collecte plus large aura lieu.

L'utilisation d'un plan de gestion des données sera considérée comme faisant partie du processus d'approbation pour les nouvelles collectes de renseignements personnels sur la santé en vertu de l'article 1 des procédures de respect de la vie privée de l'ICIS.

Les plans de gestion des données seront réalisés conformément à la politique d'évaluation des incidences sur la vie privée, à l'exception des points suivants :

- les plans de gestion des données seront approuvés par le directeur responsable;
- les plans de gestion des données ne seront pas publiés.

Gestion des risques pour la vie privée et la sécurité

8. Les risques pour la vie privée et la sécurité décelés dans le cadre d'une évaluation des incidences sur la vie privée doivent être vérifiés, pris en charge et surveillés, comme le prévoit la *Politique sur la gestion des risques liés au respect de la vie privée et à la sécurité* de l'ICIS.

Processus d'approbation de l'évaluation des incidences sur la vie privée

9. Avant toute publication ou diffusion externe, les évaluations des incidences sur la vie privée doivent être approuvées par le vice-président ou le directeur exécutif de la section concernée et par le chef de la protection des renseignements personnels.

Mise en œuvre des recommandations

10. La Direction de la vie privée et des services juridiques tient un registre de toutes les recommandations relatives à la protection de la vie privée, y compris celles découlant des évaluations des incidences sur la vie privée et des évaluations de la gestion des risques liés au respect de la vie privée et à la sécurité. Ce registre contient : le nom des employés responsables de superviser le processus de mise en œuvre des recommandations; la date à laquelle chaque recommandation a été ou doit être mise en œuvre; et la mesure qui a été ou doit être prise pour mettre en œuvre chaque recommandation. La Direction de la vie privée et des services juridiques entre ces renseignements dans le registre principal des plans d'action de l'ICIS, où ils feront l'objet d'une surveillance et d'un rapport à l'échelle organisationnelle. Le responsable du plan d'action (soit le vice-président ou le directeur) doit documenter les recommandations et les mesures prises (ou prévues) pour mettre en œuvre les recommandations. De plus, le responsable du plan d'action doit faire des comptes rendus et des présentations sur une base régulière auprès du Comité de la haute direction, et ce, jusqu'à la pleine mise en œuvre des recommandations.

Mise à jour ou reprise de l'évaluation des incidences sur la vie privée

11. Le directeur responsableⁱ doit veiller à ce que les évaluations des incidences sur la vie privée soient mises à jour
- lorsque des changements importants sont apportés à la fonctionnalité, aux objectifs, à la collecte de données, aux utilisations, aux divulgations, aux ententes ou aux autorités pertinentes d'un programme, d'une initiative, d'un processus ou d'un système, et que l'évaluation des incidences sur la vie privée ne fait pas état de ces changements;
 - lorsqu'une divergence est décelée entre le contenu des évaluations et les pratiques et processus en vigueur;
 - lorsque d'autres changements surviennent et risquent d'avoir des répercussions sur les aspects liés au respect de la vie privée et à la sécurité de ces programmes, initiatives, processus et systèmes.

Les évaluations des incidences sur la vie privée sont renouvelées au moins une fois tous les 5 ans, conformément au calendrier du registre des évaluations des incidences sur la vie privée.

Le chef de la protection des renseignements personnels peut juger qu'il est nécessaire de mettre à jour une évaluation des incidences sur la vie privée ou de procéder à une nouvelle évaluation.

i. Le directeur responsable est le responsable de l'évaluation des incidences sur la vie privée. Il peut s'agir du responsable de la banque de données; du directeur responsable de l'initiative, du processus ou du système; ou du responsable de projet.

Révision annuelle

12. Pour veiller à ce que les évaluations des incidences sur la vie privée restent exactes et vérifier que les renseignements personnels sur la santé recueillis pour les objectifs de la banque de données sont toujours nécessaires aux fins déterminées, les directeurs responsables révisent chaque année les énoncés des objectifs et les évaluations des incidences sur la vie privée qui sont en vigueur afin de relever toute divergence entre leur contenu et les pratiques ou processus réels, auquel cas ils avisent le chef de la protection des renseignements personnels. Ils détermineront avec ce dernier si des modifications sont nécessaires.
13. Avant toute publication ou diffusion externe, les modifications aux évaluations des incidences sur la vie privée, y compris les modifications aux énoncés des objectifs, doivent être approuvées par le vice-président ou le directeur exécutif de la section concernée et par le chef de la protection des renseignements personnels.
14. Les modifications aux évaluations des incidences sur la vie privée, y compris les modifications aux énoncés des objectifs, sont incluses dans les évaluations des incidences sur la vie privée. Ces documents sont publiés sur le site Web public de l'ICIS et fournis sur demande aux dépositaires de renseignements sur la santé et aux autres personnes ou organismes qui soumettent les renseignements personnels sur la santé à la banque de données.

Publication

15. Une fois l'évaluation des incidences sur la vie privée approuvée, conformément aux dispositions du paragraphe 4 ci-dessus, le chef de la protection des renseignements personnels rend l'évaluation ou un résumé de celle-ci accessible au grand public, notamment en l'affichant sur le site Web de l'ICIS, à l'endroit et au moment jugés opportuns.

Registre des évaluations des incidences sur la vie privée

16. La Direction de la vie privée et des services juridiques tient un registre des évaluations des incidences sur la vie privée qui sont terminées, en cours et à faire. Le registre indique
 - le nom du programme, de l'initiative, du processus ou du système visé;
 - la date à laquelle l'évaluation a été terminée ou devrait l'être;
 - le nom des employés responsables de terminer l'évaluation ou de veiller à ce qu'elle soit terminée.

Respect, vérification et application

17. 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 est encadrée par la Politique de vérification du respect de la vie privée de l'ICIS. Les contraventions au code — y compris les contraventions aux politiques, aux procédures et aux 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.

Avis de violation

Les cas de non-conformité aux politiques en matière de respect de la vie privée et de sécurité 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, en vertu duquel le personnel doit signaler tout incident ou toute violation à incident@icis.ca, ce qui comprend tout non-respect de la présente politique.

Procédures et documents connexes

Code de conduite de l'ICIS

Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité de l'information

Politique sur la gestion des risques liés au respect de la vie privée et à la sécurité

Pour de plus amples renseignements :



Comment citer ce document :

Institut canadien d'information sur la santé. *Politique d'évaluation des incidences sur la vie privée.*

Ottawa, ON : ICIS; 2023.