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 (EIVP) 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, il incombe notamment à l’ICIS de réaliser des EIVP dans le cadre de son programme de respect de la vie privée.

Les EIVP revêtent une importance capitale aux yeux de l’ICIS et des intervenants. L’application de la présente politique et des EIVP 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 et des initiatives de l’ICIS. L’EIVP implique 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 EIVP sont la responsabilité du directeur de la section concernée, mais leur réalisation est une responsabilité conjointe du personnel de la section (ou du gestionnaire de projets, selon le cas) et du Secrétariat à la vie privée et aux services juridiques. Le rapport d’évaluation des incidences sur la vie privée peut être rédigé par le personnel de la section, avec l’aide du personnel de la Secrétariat à la vie privée et aux services juridiques, ou vice-versa. Le recours aux consultants externes en respect de la vie privée pour la réalisation d’une EIVP doit être coordonné par le Secrétariat à la vie privée et aux services juridiques.

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

Application

La présente politique s’applique aux programmes et aux initiatives de l’ICIS, qui font appel à des activités de collecte, d’utilisation ou de divulgation de renseignements personnels sur la santé, sur les travailleurs de la santé et sur les employés.

Définitions

« Évaluation des incidences sur la vie privée (EIVP) » désigne 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 de renseignements personnels, en fonction des 10 principes énoncés dans le Code type sur la protection des renseignements personnels de l’Association canadienne de normalisation.

« Renseignements personnels » désigne les renseignements personnels sur la santé, sur les travailleurs de la santé et sur les employés.

« Renseignements personnels sur la santé » désigne des renseignements sur la santé d’une personne qui identifient cette personne ou qui peuvent être utilisés ou manipulés selon une méthode raisonnablement prévisible pour identifier cette personne, ou qui peuvent être associés, au moyen d’une méthode raisonnablement prévisible, à d’autres renseignements qui identifient cette personne.

« Renseignements personnels sur les travailleurs de la santé » désigne des renseignements sur un dispensateur de services de santé qui identifient cette personne ou qui peuvent être utilisés ou manipulés selon une méthode raisonnablement prévisible pour identifier cette personne, ou qui peuvent être associés, au moyen d’une méthode raisonnablement prévisible, à d’autres renseignements qui identifient cette personne.

« Renseignements personnels sur les employés » désigne 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. Circonstances exigeant la réalisation d’une évaluation des incidences sur la vie privée

Il convient d’effectuer une EIVP lorsque

- des banques de données existantes ou proposées impliquent la collecte, l’utilisation ou la divulgation de renseignements personnels;
- un changement important est envisagé à l’égard d’une banque de données existante contenant des renseignements personnels;
- des programmes ou des initiatives comportent des incidences sur la vie privée, conformément aux recommandations du chef de la protection des renseignements personnels en consultation avec la section.

1.1 Processus visant à déterminer la nécessité de réaliser une EIVP

- En ce qui concerne les collectes de données proposées, le Comité exécutif détermine s’il faut réaliser une EIVP ou un plan de gestion des données conformément à l’article 1.4 des procédures de respect de la vie privée.
- En ce qui concerne les bases de données existantes, le processus indiqué au paragraphe 3 ci-dessous doit être suivi.

2. Circonstances n’exigeant pas la réalisation d’une EIVP

Le cas échéant, les motifs qui justifient le recours à un plan de gestion des données plutôt qu’à une EIVP, compte tenu du faible risque couru, doivent être consignés.

Un plan de gestion des données peut remplacer dans certains cas précis une EIVP complète si celle-ci n’est pas nécessaire compte tenu du faible risque couru, par exemple dans le cas de la transmission à l’ICIS d’un petit fichier de renseignements personnels pour la réalisation d’une validation de principe. Il faut alors élaborer un plan initial 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. Une EIVP complète sera entreprise lorsqu’il sera déterminé qu’une collecte plus large aura lieu.

L’utilisation d’un plan de gestion des données doit faire partie du processus d’approbation pour les nouvelles collectes de renseignements personnels conformément au paragraphe 1 des procédures de respect de la vie privée de l’ICIS.

Le plan de gestion des données est la responsabilité du directeur de la section concernée, mais son élaboration est une responsabilité conjointe du personnel de la section et du Secrétariat à la vie privée et aux services juridiques.

Les plans de gestion des données seront réalisés conformément à la présente politique, 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.

3. Calendrier de réalisation et de révision des EIVP

Des EIVP seront entreprises dès la conception de programmes ou d’initiatives, nouveaux ou mis à jour, et seront révisées et modifiées, au besoin, pendant l’étape de conception détaillée et de mise en œuvre.

Le chef de la protection des renseignements personnels doit veiller à l’établissement d’un calendrier de réalisation et de révision des EIVP. Le directeur responsable[i] doit réviser les EIVP au moins une fois l’an pour assurer leur exactitude et leur conformité aux pratiques de gestion de l’information de l’ICIS. De telles révisions garantiront la mise à jour des EIVP 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 ou d’une initiative sans que l’EIVP en fasse état;
- des divergences sont décelées entre le contenu des EIVP et les pratiques et processus en vigueur;
- d’autres changements surviennent et risquent de compromettre le respect de la vie privée et la sécurité de ces programmes et initiatives.

En outre, le chef de la protection des renseignements personnels peut à tout moment juger qu’il est nécessaire de mettre à jour une EIVP ou de procéder à une nouvelle EIVP.

4. Éléments de contenu obligatoires dans une EIVP

Une EIVP doit indiquer au moins les éléments suivants :

- la banque de données, l’initiative ou le programme 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;

i. Le directeur responsable est le responsable de l’EIVP. Il peut s’agir du responsable de la banque de données, du directeur responsable de l’initiative ou du processus, ou du responsable de projet.

- la raison pour laquelle les renseignements personnels sont nécessaires;
- le cheminement des renseignements personnels;
- les limites imposées à la collecte, à l’utilisation et à la divulgation des renseignements personnels;
- les liens existants ou éventuels entre les renseignements personnels et d’autres renseignements;
- l’éventuelle dépersonnalisation et/ou agrégation des renseignements personnels, les fins auxquelles et les circonstances dans lesquelles les renseignements dépersonnalisés et/ou agrégés seront repersonnalisés, le cas échéant, ainsi que les conditions ou restrictions imposées;
- les autorisations légales de recueillir, d’utiliser et de divulguer les renseignements personnels;
- 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 autorisées;
- les risques de violation de la vie privée des personnes dont les renseignements personnels font ou feront partie de la banque de données, du programme ou de l’initiative, 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 mis en œuvre ou proposés pour protéger les renseignements personnels.

5. Énoncés des objectifs

Les énoncés des objectifs sont inclus dans les EIVP, au point 3.4, Deuxième principe : établissement des objectifs de la collecte de renseignements personnels sur la santé. Les EIVP sont publiées sur le site Web public de l’ICIS et fournies sur demande aux dépositaires de renseignements sur la santé et aux autres personnes ou organismes qui soumettent les renseignements personnels à la banque de données.

Les énoncés des objectifs doivent

- établir les motifs pour lesquels les renseignements personnels sont recueillis, utilisés ou divulgués ou pourraient l’être;
- décrire la nature et le type des renseignements personnels qui sont recueillis, utilisés ou divulgués ou qui pourraient l’être;
- identifier les sources des renseignements personnels;
- expliquer les raisons pour lesquelles les renseignements personnels sont nécessaires à la réalisation des objectifs définis;
- expliquer pourquoi des renseignements dépersonnalisés ou agrégés ne permettent pas d’atteindre les objectifs définis.

6. Évaluations de la gestion des risques liés au respect de la vie privée et à la sécurité

Les risques en matière de respect de la vie privée, de confidentialité et de sécurité associés à la banque de données, à l’initiative ou au programme visé par l’EIVP doivent être définis et évalués à l’aide du *Cadre de gestion des risques liés au respect de la vie privée et à la sécurité* de l’ICIS.

Une évaluation de la gestion des risques liés au respect de la vie privée et à la sécurité doit être réalisée pour chaque nouvelle banque de données ou initiative et chaque nouveau programme.

En ce qui concerne les banques de données, initiatives ou programmes existants, un changement important apporté à la fonctionnalité, aux objectifs, à la collecte de données, aux utilisations, aux divulgations, aux ententes ou aux autorités pertinentes d’une banque de données, d’une initiative ou d’un programme peut nécessiter la réalisation d’une évaluation de la gestion des risques liés au respect de la vie privée et à la sécurité si telle est la recommandation du chef de la protection des renseignements personnels, en consultation avec la section.

Les risques en matière de respect de la vie privée et de sécurité associés au processus d’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 et sa méthodologie de gestion des risques liés au respect de la vie privée et à la sécurité.

7. Constatations et recommandations découlant d’une EIVP

Le Secrétariat à la vie privée et aux services juridiques tient un registre de toutes les recommandations relatives à la protection de la vie privée, y compris celles découlant des EIVP et de l’évaluation de la gestion des risques liés au respect de la vie privée et à la sécurité connexe. Le registre indique

- le nom des employés responsables du processus de mise en œuvre des recommandations;
- la date à laquelle chaque recommandation a été ou doit être mise en œuvre;
- la mesure qui a été ou doit être prise pour la mise en œuvre de chaque recommandation;
- l’évaluation du risque résiduel une fois les mesures d’atténuation et les recommandations mises en œuvre.

Le Secrétariat à la vie privée et aux services juridiques consigne ces informations 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 consigner les recommandations et les mesures prises (ou prévues) pour la mise en œuvre des recommandations. De plus, chaque 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.

8. Registre des évaluations des incidences sur la vie privée

Le Secrétariat à la vie privée et aux services juridiques tient un registre des EIVP qui sont terminées, en cours ou prévues. Le registre indique

- le nom de la banque de données, de l’initiative ou du programme visé;
- la date à laquelle l’EIVP a été terminée ou devrait l’être;
- le nom des employés responsables de réaliser l’EIVP ou de veiller à sa réalisation;
- le cas échéant, la raison pour laquelle l’EIVP n’a pas été réalisée, le nom de la ou des personnes qui ont pris cette décision et la date à laquelle la décision a été prise.

9. Processus d’approbation de l’EIVP

Avant toute publication ou diffusion externe, l’EIVP doit être approuvée par le vice-président ou le directeur exécutif de la section concernée et par le chef de la protection des renseignements personnels.

La documentation relative au processus d’approbation doit comprendre la version finale de l’EIVP et l’évaluation de la gestion des risques liés au respect de la vie privée et à la sécurité connexe (s’il y a lieu). Si la documentation relative au processus d’approbation comprend des formulaires d’évaluation de la gestion des risques liés au respect de la vie privée et à la sécurité, ces derniers ne seront pas inclus dans la version publiée de l’EIVP.

10. Publication

Une fois l’EIVP approuvée, conformément aux dispositions du paragraphe 9 ci-dessus, le chef de la protection des renseignements personnels rend l’évaluation ou un résumé de celle-ci publiquement accessible, notamment en l’affichant sur le site Web de l’ICIS, à l’endroit et au moment jugés appropriés.

11. Conformité, vérification et application

- Le *Code de conduite de l’ICIS* définit le comportement éthique et professionnel attendu des employés 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, procédures et pratiques de l’ICIS.
- 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.
- Le chef de la protection des renseignements personnels veille à garantir la conformité aux politiques, procédures et pratiques en matière de respect de la vie privée. Le chef de la sécurité de l’information veille quant à lui à garantir la conformité aux politiques, procédures et pratiques en matière de sécurité de l’information.
- Tout manquement au code — y compris aux politiques, procédures et pratiques de respect de la vie privée et de sécurité — est signalé à la direction Personnel, Culture et Apprentissage, s’il y a lieu, et peut entraîner des mesures disciplinaires pouvant aller jusqu’au congédiement, conformément aux lignes directrices sur les mesures disciplinaires pour les employés de l’ICIS.
- La conformité est encadrée par la *Politique de vérification du respect de la vie privée* ou le Programme de vérification de la sécurité de l’information de l’ICIS, selon le cas.

Rôles et responsabilités

Le chef de la protection des renseignements personnels est responsable de l’élaboration, de la mise en œuvre et de la supervision de la présente politique.

Politiques, procédures et documents connexes

Code de conduite de l’ICIS

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

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

Pour de plus amples renseignements, écrivez-nous à

vieprivee@icis.ca.

Comment citer ce document :
Institut canadien d’information sur la santé. *Politique d’évaluation des incidences sur la vie privée.* Ottawa, ON : ICIS; 2025.