Institut canadien d'information sur la santé

Politique de vérification du respect de la vie privée

Politique : Politique de vérification du respect de la vie privée

Numéro de version : 1.1

Responsable de la politique : Chef de la protection des renseignements personnels

Division/direction/secteur : Vie privée et Services juridiques

Date d'entrée en vigueur : Septembre 2021

Responsable de l'approbation : Comité exécutif

Date de la prochaine révision : Mars 2025

Objectif

La présente politique a pour objectif d'énoncer les exigences relatives aux vérifications du respect de la vie privée réalisées par l'Institut canadien d'information sur la santé (ICIS).

Portée

La présente politique porte sur les programmes, les initiatives, les processus et les systèmes de l'ICIS, lesquels comprennent des activités de collecte, d'utilisation ou de divulgation de renseignements personnels sur la santé, de renseignements personnels sur les travailleurs de la santé ainsi que de données dépersonnalisées dérivées de renseignements personnels sur la santé ou de renseignements personnels sur les travailleurs de la santé.

Définitions

Le terme « données dépersonnalisées » désigne les renseignements personnels sur la santé ou les renseignements personnels sur les travailleurs de la santé qui ont été modifiés au moyen de processus de dépersonnalisation appropriés de sorte que l'identité de la personne ne peut être déterminée selon une méthode raisonnablement prévisible.

Le terme « renseignements personnels sur les travailleurs de la santé » désigne les renseignements au sujet d'un dispensateur de services de santé qui permettent d'identifier cette personne, 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 la personne.

Pour les besoins de la présente politique, le terme « organisme de services informatiques » désigne le tiers tel que défini dans l'entente applicable avec l'ICIS, qui a accès aux renseignements confidentiels de l'ICIS à des fins de stockage et de gestion des renseignements confidentiels de l'ICIS pour le compte de l'organisme principal.

Le terme « renseignements personnels sur la santé » désigne les renseignements sur la santé qui identifient une personne, 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.

Pour les besoins de la présente politique, le terme « organisme principal » désigne le tiers responsable de la protection et de la sécurité des renseignements confidentiels de l'ICIS et des actes des personnes autorisées, conformément aux obligations énoncées dans l'entente applicable avec l'ICIS.

Le terme « membre du personnel » désigne toute personne qui travaille à l'ICIS, y compris les employés à temps plein ou à temps partiel, les personnes qui travaillent à l'ICIS en détachement, les travailleurs temporaires, les étudiants et les employés contractuels, ainsi que les experts-conseils externes ou tout autre tiers fournisseur de services ayant besoin d'accéder aux données ou aux systèmes d'information de l'ICIS, conformément à la *politique d'utilisation acceptable des systèmes d'information* de l'ICIS.

Politique

1.0 Vérifications du respect de la vie privée

1.1 Le chef de la protection des renseignements personnels est l'autorité qui gère le programme de respect de la vie privée de l'ICIS au quotidien. Les vérifications du respect de la vie privée seront réalisées dans le cadre de ce programme, conformément au calendrier des vérifications établi dans le *plan pluriannuel de vérification du respect de la vie privée* de l'ICIS.

1.2 Le chef de la protection des renseignements personnels a la responsabilité d'élaborer et de tenir à jour le *plan pluriannuel de vérification du respect de la vie privée* de l'ICIS, et de s'assurer que le plan est approuvé annuellement par le Comité de gouvernance et de respect de la vie privée du Conseil d'administration de l'ICIS.

1.3 L'ICIS réalisera des vérifications internes du respect de la vie privée pour évaluer la conformité à ses propres politiques et procédures en matière de respect de la vie privée et de sécurité. Les vérifications faites pour s'assurer que les membres du personnel de l'ICIS sont autorisés à accéder aux renseignements personnels sur la santé au titre des politiques et procédures en matière de respect de la vie privée et de sécurité de l'ICIS sont effectuées dans le cadre du programme de vérification du système de gestion de la sécurité de l'information (SGSI) de l'ICIS. Au minimum, une vérification des agents autorisés à accéder à des renseignements personnels sur la santé et à les utiliser, en vertu de la politique et des procédures limitant l'accès des agents aux renseignements personnels sur la santé et leur utilisation de ces renseignements, doit être effectuée une fois par année.

1.4 L'ICIS procédera à des vérifications de tiers ciblant les destinataires externes de renseignements personnels sur la santé, de renseignements personnels sur les travailleurs de la santé ainsi que de données dépersonnalisées dérivées de renseignements personnels sur la santé et de renseignements personnels sur les travailleurs de la santé pour évaluer le respect des modalités de l'entente de divulgation qui régissent l'utilisation des données de l'ICIS, puis formulera des recommandations visant à résoudre les éventuels problèmes relevés.

2.0 Exigences relatives aux vérifications du respect de la vie privée

2.1 La nature et la portée des vérifications du respect de la vie privée seront déterminées en fonction du *plan pluriannuel de vérification du respect de la vie privée* de l'ICIS et peuvent comprendre des visites en personne (ou à distance), des inspections, l'examen de documents et des entrevues, si l'ICIS l'estime nécessaire.

2.2 La portée des vérifications du respect de la vie privée auprès de tiers inclura l'organisme principal et le ou les organismes de services informatiques, selon le cas.

2.3 Les vérifications du respect de la vie privée seront réalisées par le personnel du Secrétariat à la vie privée et aux services juridiques de l'ICIS ou par du personnel chargé de procéder aux vérifications du respect de la vie privée, en collaboration avec la Division de la sécurité de l'information, au besoin.

2.4 Les vérifications du respect de la vie privée seront réalisées conformément au calendrier des vérifications établi dans le *plan pluriannuel de vérification du respect de la vie privée* de l'ICIS ou sur demande pour répondre à des risques émergents liés à la vie privée et à la sécurité (p. ex. en cas d'incident et de violation du respect de la vie privée) ou pour répondre à des demandes externes comme une enquête, une recommandation ou l'ordonnance d'un commissaire à la protection de la vie privée ou d'un ombudsman.

3.0 Processus de vérification du respect de la vie privée

3.1 Les critères pris en compte dans la sélection du sujet des vérifications internes du respect de la vie privée comprennent les renseignements d'évaluation découlant du respect de la *Politique d'évaluation des incidences sur la vie privée*, de la *Politique sur la gestion des risques liés au respect de la vie privée et à la sécurité* et du *Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité de l'information* de l'ICIS, ou encore les facteurs externes comme une enquête, une recommandation ou une ordonnance d'un commissaire à la protection de la vie privée ou d'un ombudsman. Les critères de sélection du sujet des vérifications du respect de la vie privée auprès de tiers seront décrits dans le *plan pluriannuel de vérification du respect de la vie privée* de l'ICIS et comprennent, par exemple, les changements proposés à l'utilisation des données divulguées à un tiers, la complexité de la gestion des données d'un projet, la divulgation de renseignements personnels sur la santé et l'évaluation, par l'ICIS, de sources de risques émergents et actuels liés à la vie privée et à la sécurité résultant de la divulgation de données de l'ICIS à des organismes tiers.

3.2 Un avis sera envoyé dans le format exigé par le chef de la protection des renseignements personnels pour les vérifications internes et les vérifications auprès de tiers du respect de la vie privée. Le chef de la protection des renseignements personnels (ou son remplaçant) émettra un avis pour les vérifications internes et les vérifications auprès de tiers du respect de la vie privée.

3.3 Les avis de vérification du respect de la vie privée seront envoyés par écrit, conformément à l'entente connexe s'il y a lieu, et comprendront ce qui suit : la politique ou le cadre contractuel à la base de la vérification; les coordonnées des membres du personnel de l'ICIS qui effectueront la vérification; la nature et la portée de la vérification; les participants potentiellement visés par les entrevues et les inspections liées à la vérification; le moment proposé pour la vérification.

3.4 Les documents seront créés, reçus et tenus à jour dans le format exigé par le chef de la protection des renseignements personnels afin de constituer la preuve de l'administration et des activités liées aux vérifications du respect de la vie privée de l'ICIS ou de répondre aux obligations légales. Ces documents comprendront la liste des participants présents aux réunions, le registre des visites des lieux et des inspections liées à la vérification, les questionnaires d'évaluation créés et utilisés pour procéder à la vérification, les documents soumis ou recueillis aux fins de la vérification, les confirmations écrites d'acceptation et d'approbation interne, le rapport final de vérification et les recommandations découlant de la vérification.

3.5 Il incombe aux membres du personnel de l'ICIS qui réalisent une vérification du respect de la vie privée de remplir les documents sur la vérification du respect de la vie privée comme demandé. Ces documents seront tenus à jour par le Secrétariat à la vie privée et aux services juridiques de l'ICIS.

3.6 À l'issue de la vérification du respect de la vie privée, un rapport de vérification sera remis à l'entité vérifiée dans le format exigé par le chef de la protection des renseignements personnels. Dans le cas d'une vérification interne, un rapport sera remis au membre du personnel de l'ICIS du service responsable occupant un poste de directeur ou à un échelon supérieur. Dans le cas d'une vérification du respect de la vie privée auprès de tiers, le rapport sera remis à une personne en mesure de lier l'organisme principal ou les organismes de services informatiques.

4.0 Réponse aux recommandations découlant des vérifications du respect de la vie privée

4.1 Les membres du personnel qui réalisent une vérification du respect de la vie privée désigneront la personne de l'entité vérifiée responsable de répondre aux recommandations découlant de la vérification du respect de la vie privée et indiqueront les délais accordés pour y répondre. Ils devront aussi obtenir une confirmation écrite attestant que l'entité vérifiée accepte le rapport de vérification et les recommandations.

4.2 Les membres du personnel qui effectuent une vérification interne du respect de la vie privée devront obtenir, auprès d'un directeur ou d'une personne d'un échelon supérieur, une confirmation écrite attestant l'acceptation du rapport de vérification et des recommandations connexes. Une fois que les recommandations sont acceptées, le Secrétariat à la vie privée et aux services juridiques doit voir à ce que toutes les recommandations soient consignées dans le registre des recommandations relatives au respect de la vie privée, puis dans le registre principal des plans d'action de l'ICIS. Les responsables internes de la mise en œuvre d'une recommandation sont tenus de faire des comptes rendus et des présentations sur une base régulière au Comité de la haute direction de l'ICIS, et ce, jusqu'à la pleine mise en œuvre de la recommandation.

4.3 Les membres du personnel qui effectuent une vérification du respect de la vie privée auprès de tiers devront obtenir, auprès d'une personne capable de lier l'organisme principal ou les organismes de services informatiques, une confirmation écrite attestant l'acceptation du rapport de vérification et des recommandations connexes.

4.4 Dans le cas des vérifications du respect de la vie privée auprès de tiers, le Secrétariat à la vie privée et aux services juridiques effectue un suivi à l'égard de chaque recommandation, jusqu'à ce que l'organisme confirme que la recommandation a fait l'objet d'une mesure corrective adéquate.

5.0 Rapport sur la vérification du respect de la vie privée

5.1 Les membres du personnel qui effectuent une vérification du respect de la vie privée prépareront un rapport de vérification dans le format exigé par le chef de la protection des renseignements personnels et devront lui remettre le rapport au terme de la vérification.

5.2 Dans son format habituel, le rapport de vérification du respect de la vie privée comprend des renseignements contextuels, une description de la portée de la vérification et de la méthode utilisée, les résultats de la vérification et les observations, ainsi que les recommandations et les possibilités d'amélioration.

6.0 Communication des résultats et des recommandations découlant de la vérification du respect de la vie privée

6.1 Le chef de la protection des renseignements personnels (ou son remplaçant) doit déterminer comment, dans quel format et dans quelles circonstances communiquer les résultats de la vérification — y compris les recommandations qui en découlent et l'état d'avancement de leur mise en œuvre — aux intervenants internes et externes. Cela comprend le mécanisme et le format de communication des résultats, notamment le degré de précision des résultats communiqués. À la fin d'une vérification du respect de la vie privée, les résultats seront communiqués dès que possible, au moment approprié.

6.2 Les recommandations résultant des vérifications internes du respect de la vie privée seront transmises à la division visée par la vérification, aux autres divisions de l'ICIS directement touchées par les résultats de la vérification et de façon plus générale à l'ICIS dans le cadre d'activités de sensibilisation au respect de la vie privée et à la sécurité. Elles peuvent être communiquées par courriel ou publiées sur le site intranet de l'ICIS.

6.3 Les recommandations découlant des vérifications du respect de la vie privée auprès de tiers seront communiquées à l'entité vérifiée. Dans les cas où les résultats pourraient entraîner des améliorations dans les activités internes de l'ICIS, des communications pourraient aussi être envoyées aux divisions visées de l'ICIS. Les renseignements sommaires dérivés des recommandations découlant des vérifications du respect de la vie privée auprès de tiers seront transmis aux tiers destinataires de données de l'ICIS et aux organismes qui envisagent de demander des données à l'ICIS.

6.4 Le chef de la protection des renseignements personnels rendra compte régulièrement de toutes les activités de vérification, y compris les résultats et les recommandations, au Comité de la haute direction de l'ICIS et au Comité de gouvernance et de respect de la vie privée du Conseil d'administration de l'ICIS, dont fait partie le président-directeur général de l'ICIS.

7.0 Registre des vérifications du respect de la vie privée

7.1 Le chef de la protection des renseignements personnels (ou son remplaçant) établira et tiendra à jour un registre des vérifications du respect de la vie privée qui contiendra au moins les recommandations découlant des vérifications internes du respect de la vie privée; le nom de la ou des personnes chargées de mettre en œuvre chaque recommandation; la date à laquelle chaque recommandation a été ou doit être mise en œuvre; la mesure qui a été ou doit être prise pour mettre en œuvre chaque recommandation.

7.2 Le chef de la protection des renseignements personnels (ou son remplaçant) doit s'assurer que la documentation relative à une vérification du respect de la vie privée est conservée dans les dossiers du Secrétariat à la vie privée et aux services juridiques.

8.0 Intervention en cas d'incident et de violation du respect de la vie privée

8.1 Les membres du personnel qui effectuent une vérification du respect de la vie privée traiteront les incidents liés au respect de la vie privée ou à la sécurité et les violations de la vie privée ou de la sécurité de l'information présumés ou avérés, conformément au *Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité de l'information* de l'ICIS.

Procédures et documents connexes

Politique d'utilisation acceptable des systèmes d'information

Manuel de vérification du système de gestion de la sécurité de l'information

Plan pluriannuel de vérification du respect de la vie privée

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

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

Politique d'évaluation des incidences sur la vie privée

Vous demandez des données à l'ICIS? Voici ce que vous devez savoir sur le programme de vérification du respect de la vie privée de l'ICIS

Pour en savoir plus, écrivez à vieprivee@icis.ca.

Historique des révisions

Date	Version	Description des révisions	Responsable de l'approbation
Septembre 2021	1.0	Nouvelle politique	Comité de la haute direction
Mars 2022	1.1	Légères modifications apportées afin de satisfaire aux exigences du manuel révisé du CIPVP de l'Ontario	Comité exécutif