Institut national de santé publique Québec	**POLITIQUE SUR LA GOUVERNANCE DES RENSEIGNEMENTS DE SANTÉ ET DE SERVICES SOCIAUX ET DES RENSEIGNEMENTS PERSONNELS**	
	Direction :	Bureau d'information et d'études en santé des populations / Secrétariat général
	Autorisée par :	Conseil d'administration
PO-26-2025	Date d'entrée en vigueur :	12 février 2025
	Révisée le :	

OBJET DE LA POLITIQUE

1. Pour remplir sa mission, l'Institut national de santé publique du Québec (ci-après « l'Institut ») recueille, produit, gère et utilise des renseignements de santé et de services sociaux et des renseignements personnels (ci-après conjointement désignés les « renseignements »). Ces renseignements ont une importance stratégique dans la réalisation des mandats de l'Institut.
2. Conscient de la valeur des renseignements qu'il détient, l'Institut a la responsabilité d'en assurer la protection en mettant en place des mesures soutenues par la présente politique. D'autres politiques, directives et procédures complètent le cadre de gouvernance qu'adopte l'Institut en matière de protection des renseignements.
3. En conformité avec les lois, les règlements et les directives gouvernementales en vigueur, dont la Loi sur les renseignements de santé et de services sociaux (LRSSS) et la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LADPRP), la présente politique définit les objectifs, les principes directeurs, les exigences institutionnelles en matière de sécurité ainsi que les rôles et responsabilités des membres de l'Institut concernant la gouvernance des renseignements.

OBJECTIFS DE LA POLITIQUE

4. Cette politique consacre l'engagement de l'Institut à l'égard de la protection et de la sécurité des renseignements qu'il détient, tout en instaurant une gouvernance adéquate, efficace et transparente. Plus particulièrement, elle vise les objectifs suivants :

    - Désigner un responsable de la gouvernance et de la protection des renseignements de santé et de services sociaux (RGPRSSS) et un responsable de la protection des renseignements personnels (RPRP);
    - Protéger et sécuriser les renseignements en mettant en place des mesures appropriées pour prévenir l'accès non autorisé ou la divulgation de ces renseignements;
    - Restreindre l'accès aux renseignements, avec ou sans le consentement de la personne concernée, aux seuls membres de son personnel qualifiés pour les recevoir, lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions;

- Définir les exigences de journalisation et les mesures de sécurité propres à assurer la protection des renseignements qu'il détient;
- Faire connaitre les conditions et les modalités suivant lesquelles des renseignements peuvent être communiqués;
- Décrire les attentes en lien avec la conservation et la destruction des renseignements qu'il détient d'une manière à assurer en tout temps leur protection;
- Identifier les processus en place pour gérer les incidents de confidentialité et les plaintes relatives à la protection des renseignements;
- Assurer la formation et la sensibilisation en matière de protection des renseignements auprès des membres du personnel, y compris les étudiants et les stagiaires.

CHAMP D'APPLICATION

5. Cette politique porte sur les renseignements détenus ou utilisés par l'Institut, peu importe leur localisation et le support sur lequel ils se trouvent, et ce, durant tout leur cycle de vie, c'est-à-dire de leur collecte, leur création ou leur communication jusqu'à leur destruction. Elle concerne également les renseignements confiés à des tiers et ceux confiés à l'Institut dans le cadre d'un mandat.
6. La présente politique s'applique à tous les membres du personnel.

DÉFINITIONS

7. **Incident de confidentialité :** accès non autorisé par la loi à un renseignement, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection.
8. **Incident de sécurité :** un ou plusieurs évènements liés à la sécurité de l'information, indésirable(s) ou inattendu(s), présentant une probabilité forte de compromettre les opérations liées à la continuité des activités de l'organisation et de menacer la sécurité de l'information (disponibilité, intégrité ou confidentialité). Un incident de sécurité de l'information peut être lié ou non à l'utilisation des technologies de l'information et des communications.
9. **Jeu de données :** groupe de données cohérent et structuré, portant sur un sujet déterminé, accessible pour la consultation ou le téléchargement en un ou plusieurs fichiers.
10. **Membres du personnel :** tout employé de l'Institut, tout médecin ayant un mandat de l'Institut, toute personne non rémunérée ou rémunérée dans le cadre d'un contrat avec l'Institut, quelle que soit la source de financement utilisée pour assurer cette rémunération, tout étudiant et stagiaire ainsi que toute personne externe travaillant sur des mandats ou des projets de recherche de l'Institut dans l'accomplissement de leurs fonctions à l'Institut.
11. **Renseignement anonymisé :** tout renseignement dont il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier, même indirectement, la personne qu'il concerne.

12. **Renseignement dépersonnalisé :** renseignement personnel qui ne permet plus d'identifier directement la personne concernée. La dépersonnalisation d'un renseignement personnel est réversible, contrairement à l'anonymisation qui est irréversible.

13. **Renseignement de santé et de services sociaux** : tout renseignement qui permet, même indirectement, d'identifier une personne et qui répond à l'une des caractéristiques suivantes :

    - il concerne l'état de santé physique ou mental de cette personne et ses facteurs déterminants, y compris les antécédents médicaux ou familiaux de la personne;
    - il concerne tout matériel prélevé sur cette personne dans le cadre d'une évaluation ou d'un traitement, incluant le matériel biologique, ainsi que tout implant ou toute orthèse, prothèse ou autre aide suppléant à une incapacité de cette personne;
    - il concerne les services de santé ou les services sociaux offerts à cette personne, notamment la nature de ces services, leurs résultats, les lieux où ils ont été offerts et l'identité des personnes ou des groupements qui les ont offerts;
    - il a été obtenu dans l'exercice d'une fonction prévue par la Loi sur la santé publique (chapitre S-2.2);
    - toute autre caractéristique déterminée par règlement du gouvernement.

    De plus, un renseignement permettant l'identification d'une personne telle que son nom, sa date de naissance, ses coordonnées ou son numéro d'assurance maladie est un renseignement de santé et de services sociaux lorsqu'il est accolé à un renseignement visé au premier alinéa ou qu'il est recueilli en vue de l'enregistrement, de l'inscription ou de l'admission de la personne concernée dans un établissement ou de sa prise en charge par un autre organisme du secteur de la santé et de services sociaux.

    Un renseignement qui concerne un membre du personnel n'est pas un renseignement de santé et de services sociaux lorsqu'il est recueilli à des fins de gestion des ressources humaines.

14. **Renseignement personnel :** tout renseignement qui concerne une personne physique et qui permet de l'identifier directement (numéro d'assurance sociale, nom, prénom, adresse, numéro de dossier) ou indirectement (âge, sexe, région, etc.).

CADRE JURIDIQUE

15. Charte des droits et libertés de la personne (RLRQ, c. C-12).
16. Code civil du Québec (RLRQ, c. CCQ-1991).
17. Loi sur les renseignements de santé et de services sociaux (LRSSS, c. R-22.1)
18. Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1).
19. Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ c G-1.03).
20. Loi sur l'Institut national de santé publique du Québec (RLRQ, c. I-13.1.1).

21. Loi sur les laboratoires médicaux, la conservation des organes, des tissus, des gamètes et des embryons et la disposition des cadavres (RLRQ c. L-0.2).
22. Loi sur la santé publique (RLRQ c. S-2.2).
23. Loi concernant le cadre juridique des technologies de l'information (RLRQ, c. C-1.1)
24. Loi sur les archives (RLRQ c. A-21.1).

PRINCIPES DIRECTEURS

25. L'Institut s'engage à prendre toutes les mesures requises en matière de sécurité pour assurer la confidentialité des renseignements.
26. Tout renseignement détenu par l'Institut est confidentiel et, sous réserve du consentement exprès de la personne qu'il concerne, il ne peut être utilisé ou communiqué que conformément à la LRSSS ou à la LADPRP.
27. Sauf exception prévue à la LRSSS ou à la LADPRP, le consentement est demandé pour chacune des fins visées, en termes simples et clairs. Il ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.
28. La protection des renseignements détenus par l'Institut contribue au développement d'une relation de confiance avec les citoyens, les membres du personnel, les partenaires et les clients. Les mesures de protection doivent donc contribuer à renforcer cette confiance tout en permettant aux membres du personnel d'avoir accès aux renseignements nécessaires et justifiés pour la réalisation des mandats de l'Institut.
29. L'efficacité et l'efficience de la protection et de la sécurité des renseignements requièrent la collaboration et la concertation à tous les niveaux de l'organisation. À cet effet, l'Institut a créé un comité sur l'accès à l'information et la protection des renseignements. Ce comité a pour fonction de soutenir les responsables désignés au sein de l'Institut.

RÈGLES GÉNÉRALES

30. Tout membre du personnel de l'Institut peut utiliser les renseignements détenus par celui-ci, s'ils sont nécessaires à la réalisation de ses fonctions. Cependant, toute utilisation des renseignements devra préalablement avoir été autorisée par le RGPRSSS ou le RPRP, selon le cas. La demande d'accès doit inclure la liste des renseignements demandés, la liste des personnes qui y accéderont ainsi que les finalités pour lesquelles l'accès aux renseignements est requis.

Mécanismes de journalisation et mesures de sécurité

31. Seules les personnes ayant la fonction de récolter ou saisir les renseignements ou de procéder au nettoyage et au jumelage des jeux de données ont accès aux données nominatives. Ces personnes ont la responsabilité de dépersonnaliser les jeux de données qui servent à réaliser les analyses.
32. L'engagement de confidentialité de toutes les personnes ayant accès à des renseignements doit être renouvelé annuellement.
33. Les droits d'accès aux renseignements sont consignés dans un registre d'accès. La conformité des droits accordés doit faire l'objet d'une vérification annuelle.

34. Les accès aux renseignements détenus par l'Institut sont journalisés.

35. Un rapport concernant les accès et autres utilisations ou communications des renseignements de santé et de services sociaux doit être transmis annuellement au ministre.

36. Sauf exception autorisée, conformément à la Directive sur les meilleures pratiques de travail en matière de sécurité de l'information (DI-31-2021), aucun renseignement détenu ne doit être copié localement sur un poste de travail ou un support de stockage externe.

37. L'Institut doit veiller à ce que les renseignements qu'il recueille soient saisis et enregistrés de façon uniforme afin d'en assurer la qualité, l'intégrité et la fiabilité, en fonction du support, pour faciliter leur utilisation et leur communication.

Modalités de conservation et de destruction des renseignements

38. Des mesures de sécurité raisonnables relatives à l'intégrité physique des lieux où sont conservés les renseignements, et ce, peu importe le support, afin de garantir la confidentialité des renseignements sont mises en place.

39. L'Institut conserve les renseignements qu'il détient d'une manière à assurer en tout temps leur protection, notamment en prenant les moyens nécessaires afin que soit contrôlé l'accès aux lieux où sont conservés ces renseignements.

40. Tous les renseignements détenus par l'Institut sur un support technologique sont déposés sur un espace sécurisé, accessible par un identifiant personnel associé à un mot de passe et dont les accès sont restreints.

41. Au terme de la durée de conservation applicable, l'Institut s'engage à détruire ou anonymiser les renseignements qu'il détient.

42. Un renseignement anonymisé doit l'être selon les meilleures pratiques généralement reconnues et selon les critères et modalités déterminés par un règlement pris en vertu de l'article 73 de la LADPRP, avec les adaptations nécessaires.

43. La destruction de tout renseignement détenu par l'Institut se fait d'une manière sécuritaire et adaptée à la sensibilité et au support du renseignement, dans le respect des meilleures pratiques généralement reconnues. Elle doit également être irréversible afin d'empêcher la reconstitution du renseignement et en conserver une preuve de destruction.

Modalités de communication des renseignements

44. L'Institut doit s'assurer que les moyens pour communiquer les renseignements soient sécuritaires, et ce autant lors de l'envoi que de la réception de renseignements.

45. Conformément à la LRSSS (art. 74 à 76 de la R22.1), une autorisation de communication des renseignements de santé et de services sociaux dans des cas de sécurité publique ou de poursuites pour une infraction à une loi applicable au Québec pourrait être accordée.

Maintien et évaluation des produits ou services technologiques

46. L'Institut doit tenir un registre des produits et services technologiques qu'il utilise en lien avec les renseignements de santé et de services sociaux.

47. L'Institut prendra les mesures nécessaires afin d'éviter ou de mitiger les impacts possibles sur l'exercice de ses fonctions ou de ses activités dû au fait qu'un produit technologique qu'il utilise cesse d'être conforme à l'usage auquel il est destiné ou que cesse la prestation d'un service technologique qu'il utilise. À cette fin, il tiendra un calendrier des dates connues ou appréhendées de telles cessations afin d'analyser au moins tous les deux ans, la pertinence de maintenir ou de remplacer ou non un tel produit ou un tel service.

Gestion des incidents de confidentialité

48. Tout incident de confidentialité ou de sécurité doit être déclaré, documenté et faire l'objet d'un suivi. Si nécessaire, des mesures raisonnables pour diminuer les risques qu'il ne se reproduise doivent être mises en place, conformément à la Procédure de gestion des incidents de confidentialité ou de sécurité de l'information (PR-12-2014).

49. Si l'incident présente le risque qu'un préjudice sérieux soit causé, l'Institut doit, avec diligence, aviser la Commission d'accès à l'information et s'il s'agit de renseignements de santé et de services sociaux, le ministre de la Santé. Il doit également aviser toute personne dont les renseignements sont visés par l'incident. Il peut également aviser toute personne ou tout groupement en mesure de diminuer le risque de préjudice et lui transmettre, sans le consentement de la personne concernée, tout renseignement nécessaire à cette fin.

Gestion des plaintes et droits des personnes relatifs à leurs renseignements

50. Toute plainte relative à la protection des renseignements doit être acheminée à l'adresse suivante : responsable.acces@inspq.qc.ca

51. Toute personne qui souhaite restreindre l'accès aux renseignements de santé et de services sociaux la concernant en application de l'article 7 de la LRSSS doit en aviser par écrit le RGPRSSS à l'adresse suivante : responsable.acces@inspq.qc.ca

52. Toute personne qui souhaite accéder aux renseignements à son sujet ou les faire rectifier ou mettre à jour doit communiquer à l'adresse suivante : responsable.acces@inspq.qc.ca

Formation et sensibilisation

53. L'Institut offre une formation en matière de protection des renseignements aux membres du personnel dès leur entrée en fonction.

54. Les connaissances des membres du personnel en matière de protection des renseignements devront être mises à jour annuellement. Ces connaissances devront porter sur :

    - les rôles et les responsabilités des membres du personnel à l'égard des renseignements qu'il détient;
    - les règles et les modalités de conservation, de destruction et d'anonymisation des renseignements;

- les mesures de sécurité propres à assurer la protection des renseignements, notamment celles visant à minimiser les risques d'incident de confidentialité;
- le processus de traitement des incidents de confidentialité;
- l'utilisation sécuritaire des produits ou services technologiques de l'organisme.

RESPONSABILITÉS

Conseil d'administration

55. Approuve la présente politique.

Président-directeur général (PDG)

56. À titre de premier responsable de la protection et de la sécurité des renseignements ainsi que de sa gouvernance, il est imputable du respect du cadre réglementaire applicable.
57. Désigne un responsable de la gouvernance et de la protection des renseignements de santé et de services sociaux (RGPRSSS) et un responsable de la protection des renseignements personnels (RPRP) qui s'assurent de la mise en œuvre de cette politique. Ces fonctions peuvent être cumulées.
58. Constitue le Comité sur l'accès à l'information et la protection des renseignements (CAIPR) et en nomme les membres.

Responsable de la gouvernance et de la protection des renseignements de santé et de services sociaux (RGPRSSS)

59. Veille au respect et à la mise en œuvre des présentes règles et des obligations de l'Institut en matière de protection des renseignements de santé et des services sociaux prévues à la LRSSS.
60. Assure la prévention et la gestion des incidents de confidentialité, le traitement des demandes d'accès et de rectification de renseignements de santé et de services sociaux et la gestion des plaintes concernant la protection de ces renseignements.
61. Est responsable de communiquer avec la personne qui formule un avis de restriction à ses renseignements de santé, en application de l'article 3 du Règlement d'application de certaines dispositions de la LRSSS (#83485), afin de l'informer adéquatement, en termes simples et clairs, des conséquences potentielles et des risques associés à l'exercice du droit de restriction.
62. Tient les registres relatifs à la protection des renseignements de santé et de services sociaux prévus par la LRSSS.
63. Conseille et soutient les directions de l'Institut dans l'application de la Politique.

Responsable de la protection des renseignements personnels (RPRP)

64. Veille au respect et à la mise en œuvre des présentes règles et des obligations de l'Institut en matière de protection des renseignements personnels prévues à la LADPRP.

65. Assure la prévention et la gestion des incidents de confidentialité, le traitement des demandes d'accès et de rectification de renseignements personnels et la gestion des plaintes concernant la protection des renseignements personnels.

66. Tient les registres relatifs à la protection des renseignements personnels prévus par la LADPRP.

67. Conseille et soutient les directions de l'Institut dans l'application de la Politique.

Comité sur l'accès à l'information et sur la protection des renseignements (CAIPR)

68. Définit et recommande les orientations en matière de protection des renseignements;

69. Recommande les règles encadrant la gouvernance des renseignements concernant notamment :

- les rôles et responsabilités des membres du personnel tout au long du cycle de vie de ces renseignements;
- le processus de traitement des plaintes relatives à la protection des renseignements;
- les activités de formation et de sensibilisation offertes au personnel de l'Institut en matière de protection des renseignements et de divulgation des incidents de confidentialité;
- les mesures de protection à prendre à l'égard des renseignements recueillis ou utilisés dans le cadre d'un sondage;

70. Rend un avis à l'égard du contenu d'une politique de confidentialité des renseignements personnels, notamment ceux recueillis par un moyen technologique;

71. Est consulté, dès le début de tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements, aux fins de l'évaluation des facteurs relatifs à la vie privée et recommande des mesures de protection de ces renseignements à toute étape d'un tel projet;

72. Évalue annuellement le niveau de protection des renseignements à l'Institut.

Chef de la sécurité de l'information organisationnelle (CSIO)

73. Veille à l'application des normes applicables aux produits ou services technologiques utilisés par l'Institut, notamment les règles particulières définies par le dirigeant réseau de l'information en vertu de l'article 97 de la LRSSS.

74. Est responsable de superviser la mise en place et le maintien des mesures de sécurité propres à assurer la protection des renseignements contenus dans ces produits ou services.

75. Au moins une fois tous les deux ans, il doit évaluer les produits ou services technologiques qu'il utilise (en application de l'article 17 du règlement d'application #83481).

Gestionnaire

76. Est responsable de l'application et du respect de cette politique au sein de son unité administrative.
77. Sensibilise les membres de son équipe à la protection des renseignements, aux conséquences d'une atteinte à la sécurité de ces renseignements ainsi qu'à leurs responsabilités en la matière.

Membre du personnel

78. Doit prendre connaissance de la présente politique, en respecter les modalités prévues et se conformer aux lois, règlements et politiques internes concernant la gouvernance des renseignements.
79. Utilise les renseignements disponibles aux seules fins auxquelles elles sont destinées et selon les droits qui lui sont accordés. Cela inclut la non-divulgation de renseignements à des tiers sans le consentement approprié.
80. Signale sans tarder à son supérieur immédiat toute situation pouvant compromettre la protection et la sécurité des renseignements.

APPROBATION

La présente politique entre en vigueur à la date de sa signature par le président-directeur général de l'Institut national de santé publique du Québec

Originale signée	12 février 2025
Pierre-Gerlier Forest	Date

Versions antérieures de la présente politique :
NA