Centre intégré de santé et de services sociaux des Laurentides
Québec

Politique

Titre	**Politique d'engagement en matière de confidentialité et de protection des renseignements personnels**	
N°	**POL 2026 DQEPE 036**	
En vigueur	2026-08-17	
Révision	Ne s'applique pas	
Adoption	Ne s'applique pas	
Approbation	2026-08-11	Comité de direction de Santé Québec Laurentides
Consultation	2026-05-23	Service d'éthique clinique et organisationnelle
Validation	2026-07-27 2026-07-27	Direction de la qualité, de l'évaluation, de la performance et de l'éthique (DQEPE) Comité sur l'accès et la protection des renseignements (CAIPR)
Diffusion	2026-08-17	Dépôt sur l'intranet et l'internet de Santé Québec Laurentides
Responsable de l'application	Direction de la qualité, de l'évaluation, de la performance et de l'éthique (DQEPE)	
Application et personnes concernées	Toute personne œuvrant pour Santé Québec Laurentides.	
Document(s) remplacé(s)	Ne s'applique pas	
Document(s) initiateur(s)	Politique de gouvernance sur la protection des renseignements personnels du CISSS des Laurentides – POL 2025 DQEPE 074	
Document(s) en découlant	▪ FORMULAIRE D'ENGAGEMENT au respect de la Politique en matière de confidentialité et de protection des renseignements personnels ▪ Tous les documents permettant d'encadrer et d'améliorer les pratiques de protection et de sécurité des renseignements personnels.	

Table des matières

1. Préambule 4
2. Domaine d'application 4
2.1. Intervenantes et intervenants concernés 5
2.2. Types de renseignements et personnes concernées 5
2.3. Concepts clés 5
3. Objectif général et objectifs spécifiques 6
4. Fondements 6
4.1. Responsabilité et imputabilité partagées 7
4.2. Respect des droits des personnes concernées par les renseignements 7
4.3. La confidentialité par défaut 8
4.4. Gouvernance des actifs informationnels et des renseignements 8
4.5. Droit de regard, de vérification et de surveillance 8
5. Énoncés 9
5.1. Renseignements personnels : identification directe et indirecte 9
5.2. Principe de minimisation et de nécessité 10
5.3. Consentement 10
5.4. Secret professionnel et la discrétion 11
5.5. Collecte des renseignements personnels 12
5.6. Conservation des renseignements personnels 12
5.7. Accès aux renseignements personnels 12
5.8. Utilisation des renseignements personnels 13
5.9. Communication des renseignements personnels 13
5.10. Destruction des renseignements personnels 14
5.11. Transport des renseignements personnels 14
5.12. Pratiques à risques et exigences 15
5.13. Incident de confidentialité 16
5.14. Plaintes des personnes concernées par les renseignements (publics visés) 17
5.15. Documents d'encadrement, formation et sensibilisation 18
5.16. Obligation d'information et de transparence 18
6. Rôles et responsabilités 18
6.1. Président(e)-directeur(-trice) général(e) (PDG) et Président(e)-directeur(-trice) général(e) adjoint(e) (PDGA) 19
6.2. Conseil d'administration d'établissement 19
6.3. Direction de la qualité, de l'évaluation, de la performance et de l'éthique (DQEPE) 19
6.4. Direction des ressources humaines (DRH) 20
6.5. Direction des services professionnels (DSP) 20

6.6. Directeurs(-trices) et gestionnaires 20
6.7. Intervenants 20
7. Modalités d'application de la politique 21
7.1. Processus standard de sensibilisation et d'engagement 21
7.2. Modalités adaptées à certaines catégories d'intervenants 21
7.3. Texte publié sur le site Internet 22
8. Mesures applicables en cas d'inobservation 22
9. Mécanisme de suivi et de révision 22
10. Demande de renseignements 23
Annexe 1 : Cadre légal et administratif 24
Annexe 2 : Documents de référence 25

1. Préambule

Dans le cadre de sa mission, Santé Québec Laurentides recueille et utilise des renseignements personnels essentiels à la prestation des soins et services. Les usagères et les usagers s'attendent légitimement à ce que ces renseignements soient protégés, ce qui contribue au maintien de leur confiance envers notre organisation.

Dans ce contexte, l'établissement met en œuvre la *Politique d'engagement en matière de confidentialité et de protection des renseignements personnels* (la *Politique*), laquelle s'inscrit dans la continuité de la *Politique de gouvernance sur la protection des renseignements personnels* (POL 2025 DQEPE 074), document maître en matière de protection des renseignements personnels (PRP).

La présente politique vise à rappeler les principes généraux liés à la confidentialité et à la PRP. Elle s'accompagne d'un formulaire d'engagement formel, par lequel les personnes visées confirment avoir pris connaissance de la politique, en comprennent le contenu et s'engagent à respecter les principes et les règles.

Enfin, la présente politique encadre les modalités de diffusion, sur le site Internet de l'établissement, de l'information destinée au public concernant les pratiques, les mesures de protection et les engagements de l'établissement en matière de PRP.

2. Domaine d'application

La présente politique établit les principes et les règles applicables à la protection des renseignements personnels détenus par Santé Québec Laurentides. Elle précise notamment les personnes visées, les renseignements concernés ainsi que la portée générale de son application.

La politique s'applique aux domaines de la PRP, de la confidentialité, de la sécurité de l'information et de l'accès à l'information.

Elle s'applique à l'ensemble des actifs informationnels contenant des renseignements personnels, quel qu'en soit le support ou le lieu de conservation.

Elle s'applique également à l'ensemble des activités et des secteurs de l'établissement, incluant les secteurs cliniques, administratifs, techniques et de soutien.

La présente politique **ne vise pas** à détailler l'ensemble des règles, pratiques opérationnelles ou comportements attendus. Afin de tenir compte de la diversité des contextes d'application, l'établissement met à la disposition des intervenantes et des intervenants différents documents d'encadrement complémentaires, notamment des procédures, des directives, des guides, des aide-mémoires et des formations.

La présente politique doit être appliquée en complémentarité avec ces documents, lesquels sont diffusés progressivement sur les plateformes internes et publiques de l'établissement. Cette approche favorise la cohérence de l'encadrement organisationnel, l'agilité documentaire ainsi que l'adaptation continue aux exigences légales, réglementaires et organisationnelles.

2.1. Intervenantes et intervenants concernés

La présente politique s'applique à toute personne qui, dans le cadre de ses fonctions, activités, études, recherches ou d'un mandat confié par Santé Québec Laurentides, accède à des renseignements personnels sous la responsabilité de l'établissement.

Sans s'y limiter, elle vise notamment les employées et employés, les gestionnaires, les médecins, les dentistes, les sages-femmes, les pharmaciennes et pharmaciens, les résidentes et résidents en médecine, les stagiaires, les bénévoles, les chercheuses et chercheurs, les membres du conseil d'administration d'établissement (CAÉ), les consultantes et consultants, les prestataires de services, les partenaires, les travailleuses et travailleurs autonomes ainsi que toute autre personne physique ou morale contribuant, de façon rémunérée ou non, à la mission de l'établissement.

Aux fins de la présente politique, l'ensemble de ces personnes est désigné par le terme « **intervenant** ».

2.2. Types de renseignements et personnes concernées

La politique s'applique à tous les renseignements personnels détenus par Santé Québec Laurentides, quel qu'en soit le support ou la forme (numérique, papier, verbal, audio, etc.).

La politique vise la protection de l'ensemble des renseignements personnels, qu'ils concernent des usagères ou usagers, des intervenants ou toute autre personne dont les renseignements sont recueillis, détenus, utilisés ou communiqués par l'établissement. Ces personnes sont désignées par l'expression **personnes concernées**, soit toute personne physique à laquelle se rapporte un renseignement personnel.

La présente politique encadre les pratiques liées aux renseignements personnels. **Elle ne vise pas les autres catégories de renseignements confidentiels**, notamment les informations stratégiques, financières, administratives, opérationnelles ou organisationnelles qui sont assujetties à d'autres mécanismes de gouvernance, de sécurité de l'information ou de gestion documentaire. Toutefois, plusieurs principes sous-jacents demeurent similaires, notamment ceux relatifs à la confidentialité, à la sécurité de l'information, à la limitation des usages et à la responsabilité organisationnelle.

2.3. Concepts clés

Les définitions pertinentes sont présentées et mises à jour de façon continue dans le document intitulé : Lexique des concepts clés en matière de protection des renseignements personnels.

Aux fins de la présente politique, les concepts suivants s'entendent comme suit :

Confidentialité : propriété d'un renseignement dont l'accès est limité aux seules personnes autorisées et pour lesquelles cet accès est nécessaire à l'exercice de leurs fonctions. Elle implique pour chaque intervenant une obligation de discrétion, de protection et d'utilisation appropriée des renseignements conformément aux lois, aux règlements et aux règles de l'établissement.

Protection des renseignements personnels (PRP) : ensemble des mesures organisationnelles, administratives, technologiques et physiques mises en place par l'établissement afin d'assurer la confidentialité, l'intégrité, la disponibilité et la protection des

renseignements tout au long de leur cycle de vie. Ce cadre organisationnel est mis en œuvre par l'ensemble des intervenants dans l'exercice de leurs fonctions et de leurs responsabilités.

La PRP constitue le cadre organisationnel établi par l'établissement pour assurer la conformité aux obligations légales et organisationnelles.

La confidentialité repose quant à elle sur la responsabilité individuelle des intervenants, qui doivent appliquer ce cadre dans leurs activités quotidiennes.

Incident de confidentialité : un incident de confidentialité correspond à toute collecte, accès, utilisation, communication (diffusion), destruction non autorisée ou à toute perte de renseignements personnels.

Droit au respect de la vie privée : droit fondamental de toute personne à la protection de sa vie privée et au contrôle de la collecte, de l'utilisation, de la communication, de la conservation et de la destruction des renseignements personnels la concernant, conformément aux lois applicables.

3. Objectif général et objectifs spécifiques

La présente politique vise à assurer la confidentialité et la protection des renseignements personnels détenus par Santé Québec Laurentides, conformément aux obligations légales, réglementaires et organisationnelles applicables. Plus précisément, elle a pour objectifs de :

- présenter les principes directeurs qui encadrent les pratiques de l'établissement;
- clarifier les concepts clés, les rôles, les responsabilités et les obligations des intervenants, afin de favoriser une compréhension commune et une application cohérente des exigences au sein de l'organisation;
- établir les modalités applicables lors de l'embauche, de l'entrée en fonction ou du début des activités d'une personne au sein de l'établissement;
- informer, sensibiliser et soutenir les intervenants relativement à leurs obligations et à leur imputabilité;
- promouvoir l'adoption de comportements responsables et conformes aux exigences dans l'exercice des fonctions et des activités de chacun;
- présenter les mécanismes de transparence mis en place par l'établissement afin d'informer la population sur ses pratiques, ses engagements et les droits des « personnes concernées » en matière de PRP et de respect de la vie privée.

4. Fondements

Cette politique s'inscrit dans le respect des obligations prévues par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.* ([*LADOP*] RLRQ, c. A-2.1) et la *Loi sur les renseignements de santé et de services sociaux.* ([*LRSSS*] RLRQ, c. R-22.1).

L'annexe 1 présente la liste des références juridiques, règlementaires et normatives ayant servi à son élaboration. L'annexe 2, recense les documents organisationnels complémentaires applicables à la PRP.

La présente politique ne constitue pas un avis juridique et ne doit pas être interprétée comme telle. En cas d'incompatibilité entre une disposition de la présente politique et une exigence légale ou réglementaire, cette dernière prévaut.

Les intervenants sont invités à consulter leur supérieur immédiat ou les instances compétentes de l'établissement lorsqu'une situation nécessite une interprétation ou un accompagnement particulier.

Cette politique s'inscrit dans la continuité des valeurs de Santé Québec, soit le respect, la bienveillance, l'excellence, la collaboration et l'engagement.

Les fondements présentés constituent le socle commun sur lequel reposent les pratiques, les comportements attendus et les documents d'encadrement en matière de PRP.

4.1. Responsabilité et imputabilité partagées

Santé Québec Laurentides est responsable d'assurer la protection des renseignements personnels sous sa gouverne et de mettre en place les mécanismes nécessaires afin d'assurer le respect des exigences légales, réglementaires et organisationnelles applicables.

La PRP constitue une responsabilité organisationnelle partagée. Elle repose autant sur les mécanismes mis en place par l'établissement que sur l'engagement de chaque intervenant à appliquer les règles de confidentialité dans l'exercice de ses fonctions ou de ses activités.

La présente politique constitue un cadre de référence initial, présenté dès l'embauche, l'entrée en fonction ou le début des activités au sein de l'établissement. Elle est accompagnée d'un formulaire d'engagement formel à signer, attestant que la personne a pris connaissance de la politique, en comprend la portée et s'engage à la respecter.

Chaque intervenant est personnellement responsable du respect de ses obligations en matière de PRP dans l'exercice de ses fonctions ou de ses activités. Il doit suivre les formations requises, prendre connaissance des documents d'encadrement applicables à son rôle et maintenir ses connaissances à jour. Ces obligations demeurent en vigueur au-delà de la fin du lien d'emploi, du contrat, du stage, du mandat ou de toute autre collaboration avec l'établissement.

4.2. Respect des droits des personnes concernées par les renseignements

Santé Québec Laurentides reconnaît la primauté des droits des « personnes concernées », notamment le droit au respect de la vie privée, comme prévu par le *Code civil du Québec* (RLRQ c. CCQ-1991, a. 35) et la *Charte des droits et libertés de la personne* (RLRQ c. C-12, a. 5, 9).

La présente politique repose sur les principes de transparence, d'accompagnement et de respect des droits des « personnes concernées ». Celles-ci doivent pouvoir être informées adéquatement et exercer les droits prévus par la loi, notamment le droit d'accès, de rectification, de plainte ainsi que, lorsque applicable, les droits relatifs à l'utilisation, à la communication et à la protection de leurs renseignements personnels.

L'exercice de ces droits ne doit entraîner aucune conséquence préjudiciable. Pour une usagère ou un usager, il ne doit avoir aucune incidence sur l'accès et la qualité des soins ou aux services.

Pour toute autre personne concernée, il ne doit avoir aucune incidence sur l'exercice de ses fonctions, de ses activités ou sur ses relations avec l'établissement.

4.3. La confidentialité par défaut

La confidentialité constitue une obligation légale, professionnelle et éthique. Elle doit être prise en compte de manière proactive et intégrée aux pratiques de l'établissement dès la conception des processus, des projets, des technologies et des modes de prestation de services.

Tout renseignement personnel est présumé confidentiel dès sa collecte et doit être protégé tout au long de son cycle de vie par des mesures adaptées à sa sensibilité et aux risques associés à son utilisation.

4.4. Gouvernance des actifs informationnels et des renseignements

Les renseignements personnels et les autres renseignements détenus dans les actifs informationnels de Santé Québec Laurentides demeurent sous la gouverne de l'établissement, peu importe le support ou la technologie utilisée.

Les intervenants peuvent créer, consulter, utiliser ou consigner des renseignements dans le cadre de leurs fonctions ou de leurs activités, mais n'en sont pas propriétaires à titre personnel. Ces renseignements doivent être utilisés exclusivement aux fins autorisées et protégés conformément aux lois et aux règles applicables.

4.5. Droit de regard, de vérification et de surveillance

Santé Québec Laurentides exerce un droit de regard sur l'utilisation des actifs informationnels mis à la disposition des intervenants dans le cadre de leurs fonctions ou de leurs activités. Ce droit s'exerce conformément aux lois applicables, aux règles de gouvernance et dans le respect du droit à la vie privée.

Les systèmes d'information, les équipements technologiques, les boîtes de courriel organisationnelles, les outils de collaboration (ex. : *Teams*) et tout autre actif informationnel fournis par Santé Québec Laurentides sont destinés à un usage professionnel. Les renseignements qui y sont consignés ou générés, incluant les traces d'utilisation, demeurent sous la gouverne de l'établissement.

Dans l'exercice de ses responsabilités, Santé Québec Laurentides peut, sans que le consentement préalable de l'intervenant soit requis, procéder à des activités de surveillance, d'examen ou de vérification lorsque cela est nécessaire pour répondre à une obligation légale ou réglementaire, notamment dans les situations suivantes :

- afin d'assurer la continuité des activités, notamment en cas d'absence, de départ ou d'indisponibilité d'un intervenant;
- afin de valider la qualité des interventions et des processus, notamment dans le cadre d'audits de qualité ou de performance;
- lorsqu'il existe des motifs raisonnables de croire qu'un incident de confidentialité, réel ou présumé, s'est produit;
- dans le cadre d'une enquête administrative, disciplinaire ou de conformité;
- pour assurer la sécurité des renseignements, des systèmes et des actifs informationnels.

À ces fins, Santé Québec Laurentides peut notamment :

- accéder au contenu d'une boîte de courriel organisationnelle, incluant les messages et pièces jointes, lorsque requis pour la poursuite des activités ou pour des raisons de conformité;
- analyser les journaux d'accès et d'utilisation des systèmes d'information;
- examiner l'utilisation des équipements et outils technologiques mis à disposition.

Ces interventions sont limitées à ce qui est nécessaire, réalisées de manière ciblée, justifiées et proportionnées, et effectuées uniquement par les personnes autorisées ou toute personne dûment mandatée.

En utilisant les actifs informationnels de l'établissement, les intervenants reconnaissent que certaines activités de surveillance, de vérification ou d'audit peuvent être réalisées conformément aux lois applicables et aux règles de gouvernance en vigueur. Ces activités sont exercées uniquement lorsque nécessaire et ne visent pas la surveillance généralisée des individus, mais plutôt la protection des renseignements personnels, la sécurité des systèmes et le respect des obligations légales, réglementaires et organisationnelles.

5. Énoncés

La présente section traduit les principes directeurs de la politique en attentes concrètes visant à soutenir l'adoption de comportements responsables.

Les exemples présentés ne sont pas exhaustifs. Chaque intervenant demeure responsable d'adopter, en tout temps, toute conduite conforme aux lois, aux règles organisationnelles et aux obligations applicables à ses fonctions.

La section se conclut par la présentation des mécanismes mis en place par l'établissement afin de répondre à ses obligations d'information et de transparence en matière de protection des renseignements personnels.

5.1. Renseignements personnels : identification directe et indirecte

Un renseignement personnel est toute information qui concerne une personne physique et qui permet ou pourrait permettre de l'identifier, directement ou indirectement. Un renseignement devient personnel dès qu'une personne peut raisonnablement être identifiée, même sans son nom.

Identification directe : l'identité est évidente, sans recoupement (ex. : nom, numéro d'assurance social ou de la Régie de l'assurance maladie du Québec, adresse, photo du visage).

Identification indirecte : l'identité apparaît par le croisement de plusieurs renseignements (ex. : âge + sexe + service; diagnostic rare + lieu de traitement).

Comportements attendus : considérer comme personnel tout renseignement permettant une identification directe ou indirecte.

Comportements interdits : présumer qu'un renseignement n'est pas personnel parce que le nom n'est pas mentionné.

5.2. Principe de minimisation et de nécessité

La minimisation impose de collecter, d'utiliser, de communiquer et de conserver uniquement les renseignements personnels strictement nécessaires à la finalité poursuivie.

Ce principe **ne constitue pas** une option, **mais une obligation** découlant du droit à la vie privée.

Le fait de ne pas identifier directement une personne lors d'une communication, lorsque cela est possible, permet de réduire les risques et s'inscrit dans l'application du principe de minimisation. De plus, la réduction de la quantité de renseignements personnels traités (accédés, utilisés, communiqués) contribue à limiter les risques et les préjudices en cas d'incident de confidentialité.

Ce principe constitue un fondement du respect de la vie privée et doit être appliqué à toutes les étapes du cycle de vie des renseignements personnels.

Comportements attendus : collecter, utiliser, communiquer et conserver uniquement les RP nécessaires à la finalité poursuivie. Privilégier l'utilisation de renseignements non identifiants lorsque cela est possible.

Comportements interdits : accéder à des renseignements « *au cas où* ». Consulter ou conserver des renseignements non nécessaires. Accéder à un dossier par curiosité ou facilité. Diffuser largement des données dépersonnalisées.

5.3. Consentement

Dans le cadre de la mission, plusieurs types de consentement peuvent être requis. Aux fins de la présente politique, le consentement désigne l'autorisation donnée par la personne concernée permettant **l'accès** à ses renseignements personnels, leur **utilisation ou leur communication** à des fins déterminées.

Ce type de consentement vise à obtenir de la personne concernée une autorisation explicite pour l'accès, l'utilisation, la communication ou le partage de ses renseignements personnels, que ce soit dans le cadre des soins et services ou à des fins secondaires (ex. : recherche, évaluation, enquête).

Le cadre juridique spécifique à ce type de consentement prévoit qu'il doit répondre aux critères suivants :

- De manière générale, le consentement est requis lorsqu'aucune disposition légale n'autorise l'accès, l'utilisation ou la communication des renseignements personnels.
- Les informations fournies à la personne concernée doivent notamment inclure, selon le contexte, les fins visées, les renseignements concernés, les utilisations, les communications ou accès prévus, les risques applicables ainsi que les droits dont elle dispose à l'égard de ses renseignements personnels.
- Le consentement doit être obtenu pour chaque fin distincte et ne peut être général, vague ou applicable à des utilisations multiples.
- Les informations relatives aux modalités du consentement doivent être communiquées dans un langage clair, accessible et compréhensible, tant dans les formulaires que lors des échanges avec la personne concernée.

- L'intervenant doit offrir à la personne concernée l'accompagnement nécessaire afin de favoriser sa compréhension de l'information transmise et lui permettre de prendre une décision libre et éclairée.

Comportements attendus : utiliser un langage simple et des formulaires distincts pour chaque fin spécifique; vérifier que la personne comprend la portée de son consentement; documenter le consentement conformément aux règles en vigueur (formulaire, note au dossier).

Comportements interdits : présumer qu'un consentement donné pour une fin s'applique à une autre; regrouper ou diluer les demandes de consentement dans des informations complexes ou générales; obtenir un consentement global couvrant des usages imprécis ou futurs non définis.

5.4. Secret professionnel et la discrétion

Le **secret professionnel** constitue un droit fondamental reconnu à l'article 9 de la *Charte des droits et libertés de la personne* (RLRQ, c. C-12) ainsi qu'une obligation déontologique d'ordre public. Il vise à préserver la relation de confiance entre la personne concernée et la professionnelle ou le professionnel membre d'un ordre régi par le *Code des professions* (RLRQ, c. C-26), en encadrant strictement la collecte, l'accès, l'utilisation et la communication des renseignements confiés dans le cadre de cette relation.

Un renseignement est protégé par le secret professionnel lorsque les conditions suivantes sont réunies :

- il est de nature confidentielle;
- il est porté à la connaissance d'une professionnelle ou d'un professionnel assujetti au secret;
- il est obtenu dans l'exercice de ses fonctions.

Bien que les obligations juridiques liées au secret professionnel s'appliquent spécifiquement aux membres d'un ordre professionnel, Santé Québec Laurentides attend de l'ensemble des intervenants (ex. : gestionnaires, agentes ou agents administratifs, techniciennes et techniciens, etc.) qu'ils adoptent des comportements équivalents, fondés sur les mêmes exigences de discrétion, de retenues et de respect de la vie privée

La **discrétion** constitue une obligation complémentaire au secret professionnel. Elle se traduit par un devoir de réserve, de vigilance et de retenue dans toutes les situations impliquant des renseignements personnels, notamment lors de leur accès, de leur utilisation ou de leur communication.

L'accès, l'utilisation et la communication de renseignements personnels doivent reposer sur le consentement de la personne concernée ou sur une autorisation prévue par la loi.

Toutefois, même dans ces situations, le secret professionnel n'est pas levé de manière absolue. L'obligation de discrétion demeure en tout temps et est renforcée par l'application du principe de nécessité. À titre d'exemple, même avec un consentement, une professionnelle ou un professionnel ne peut communiquer l'ensemble des renseignements dont il dispose, mais uniquement ceux qui sont strictement autorisés par sa fonction et requis aux fins poursuivies.

Comportements attendus : valider la légitimité de l'accès ou de la demande avant toute communication; limiter la communication d'un renseignement au strict nécessaire, même lorsque l'interlocuteur est autorisé.

Comportements interdits : accéder à plus d'informations que nécessaire sous prétexte qu'un consentement a été obtenu ou qu'une exception légale s'applique; communiquer des renseignements non nécessaires aux fins poursuivies.

5.5. Collecte des renseignements personnels

La collecte correspond au moment où un renseignement personnel est reçu et consigné dans un actif informationnel, qu'il soit verbal, papier ou numérique. Toute collecte doit être justifiée, légitime et limitée dès le départ (minimisation).

Comportements attendus : recueillir uniquement les renseignements nécessaires à l'exercice de ses fonctions et aux fins poursuivies.

Comportements interdits : recueillir des renseignements à des fins personnelles ou pour un proche. Prendre des photographies, enregistrements audio ou vidéo à des fins personnelles.

5.6. Conservation des renseignements personnels

La conservation désigne le fait de détenir un renseignement personnel dans un actif informationnel de l'établissement, qu'il soit sur un support papier ou numérique. Elle débute dès la collecte et se poursuit tant que le renseignement n'est pas détruit conformément aux règles applicables dont le calendrier de conservation, lequel détermine la durée pendant laquelle un renseignement doit être conservé.

Comportements attendus : conserver les renseignements uniquement dans les lieux et systèmes autorisés par l'établissement.

Comportements interdits : utiliser des comptes de messagerie personnelle ou des espaces de stockage externes non autorisés pour conserver des renseignements personnels[1].

5.7. Accès aux renseignements personnels

L'accès aux renseignements personnels s'entend à deux niveaux complémentaires :

L'accès comme action : il s'agit du fait de voir ou consulter un RP.

La gestion des accès : il s'agit de mécanismes de contrôle des droits accordés (ex. : profils d'accès, rôles, permissions), elle détermine les renseignements, systèmes et fonctionnalités auxquels une personne peut accéder.

[1] À titre d'exemples (liste non exhaustive) : comptes de courriel personnels (*Gmail, Hotmail, Yahoo*, etc.), services infonuagiques personnels (*Dropbox, Google Drive, iCloud, OneDrive personnel*, etc.), médias sociaux et applications de messagerie (*Facebook, Messenger, Instagram, TikTok, WhatsApp, Telegram,* etc.), ainsi que les outils d'intelligence artificielle générative non autorisés (*ChatGPT et autres outils similaires*).

Ces deux dimensions sont indissociables, mais distinctes : le fait de disposer d'un accès (*gestion des accès*) ne signifie pas que l'on est autorisé à consulter ou à utiliser l'information (*l'accès comme action*).

Comportements attendus : accéder uniquement aux renseignements nécessaires à l'exercice de ses fonctions ou à la réalisation de ses activités. Orienter toute personne (proche, collègue, connaissance ou son propre dossier) souhaitant obtenir de l'information ou accéder à son dossier vers les services responsables (ex. : archives médicales, guichet d'accès, service concerné).

Comportements interdits : consulter le dossier d'un proche, d'un collègue, d'une connaissance ou son propre dossier. Accéder à des renseignements en utilisant les accès ou les identifiants d'un autre intervenant. Accéder par curiosité ou intérêt personnel.

5.8. Utilisation des renseignements personnels

L'utilisation correspond à toute action par laquelle un renseignement personnel est consulté, analysé, traité, exploité ou utilisé dans le cadre des fonctions ou des activités autorisées d'un intervenant.

Dans le réseau de la santé et des services sociaux, l'utilisation comprend notamment les **échanges de renseignements personnels entre les intervenants autorisés** lorsqu'ils sont nécessaires à l'exercice de leurs fonctions, à la prestation de soins et de services ou à toute autre fin prévue par la loi.

L'utilisation doit en tout temps respecter les principes de nécessité, de proportionnalité et de confidentialité.

Comportements attendus : utiliser les RP uniquement à des fins autorisées; documenter l'utilisation lorsque requis (notes au dossier, registre, etc.).

Comportements interdits : utiliser des RP à des fins personnelles, par curiosité, pour obtenir un avantage personnel ou causer un préjudice à une personne.

5.9. Communication des renseignements personnels

La communication d'un renseignement personnel consiste à transmettre ce renseignement à une personne ou à un organisme **à l'extérieur de Santé Québec** ou du réseau de la santé et des services sociaux.

Il est important de distinguer la communication de l'accès et de l'utilisation. Lorsque des intervenants autorisés consultent, utilisent ou échangent des renseignements personnels dans le cadre de leurs fonctions et pour une fin prévue par la loi, **il ne s'agit pas d'une communication**, mais plutôt d'un accès ou d'une utilisation autorisée.

La communication vise plutôt la **transmission de renseignements personnels à un tiers**, c'est-à-dire à une personne ou à un organisme externe. Selon le contexte, il peut notamment s'agir d'un syndicat, d'un corps policier, d'un établissement d'enseignement, d'un service de garde éducatif à l'enfance, d'un assureur, d'un employeur, d'un organisme communautaire ou d'un autre organisme public ou privé.

La communication d'un renseignement personnel est permise uniquement lorsque la personne concernée y a consenti ou lorsqu'une disposition légale l'autorise expressément. Dans tous les cas, seuls les renseignements nécessaires à la finalité poursuivie peuvent être communiqués.

Comportements attendus : vérifier, avant toute communication, si vous êtes légitimé. S'assurer que le destinataire est autorisé à recevoir l'information. Documenter la communication conformément aux règles en vigueur (ex. : note au dossier, registre applicable).

Comportements interdits : transmettre des renseignements personnels dans un contexte non sécurisé (ex. : utilisation d'un courriel personnel tel que *Gmail*, échanges dans un lieu public). Communiquer plus de renseignements que nécessaire pour atteindre la finalité visée. Supposer qu'une bonne intention justifie la communication.

5.10. Destruction des renseignements personnels

La destruction consiste à éliminer de façon définitive et sécuritaire un renseignement personnel afin qu'il ne soit plus possible d'y accéder ni de le reconstituer. Elle marque la fin du cycle de vie de l'information.

La destruction des renseignements personnels doit respecter les délais prévus au calendrier de conservation. Chaque intervenant doit s'assurer qu'il est autorisé avant d'y procéder et, en cas de doute, consulter la direction propriétaire des renseignements concernés.

Comportements attendus : respecter en tout temps les règles du calendrier de conservation. Utiliser des moyens de destruction sécuritaires et autorisés : papier (bacs verrouillés ou déchiquetage certifié) et numérique (suppression définitive y compris corbeilles, sauvegardes locales).

Comportements interdits : détruire un renseignement ou un document unique avant la fin de sa durée de conservation légale. Conserver inutilement des copies ou des brouillons.

5.11. Transport des renseignements personnels

Le transport désigne le fait de déplacer des renseignements personnels à l'extérieur des installations de l'établissement, que ce soit sur un support papier ou numérique. Ces situations comportent des risques accrus de perte, de vol, d'accès non autorisé ou de bris de confidentialité.

Conformément à l'article 61 du *Règlement sur l'organisation et l'administration des établissements* (RLRQ, c. S-5, r. 5), nul ne peut sortir de l'établissement un original d'une partie ou de l'ensemble d'un dossier d'usagère ou d'usager, **sauf dans les cas expressément prévus**.

Santé Québec Laurentides autorise, sans demande explicite, la sortie de dossier dans les situations suivantes :

- Lorsque le tribunal l'exige ou dans les cas expressément prévus par la loi.
- Pour les renseignements de santé et services sociaux (RSSS), dans le cadre de la prestation de services, soit au domicile de l'usagère ou de l'usager ou dans toute ressource externe desservie par les intervenants de l'établissement (ex. : écoles).

Dans toute autre situation, l'intervenant doit formuler une demande. Avant la sortie du dossier, selon le contexte, une autorisation doit être obtenue :

- Service des archives médicales, pour les renseignements de santé et de services sociaux (RSSS);
- Direction des ressources humaines (DRH), pour les dossiers RH;
- Service de la gestion stratégique de l'information (GSI), pour les autres types de dossiers.

Comportements attendus : une surveillance directe et constante doit être exercée en tout temps à l'égard des renseignements transportés. Privilégier les copies plutôt que les originaux. Retourner dans les plus brefs délais dans le lieu d'archives.

Comportements interdits : sortir de l'établissement un dossier original ou un exemplaire unique sans en avoir obtenu au préalable l'autorisation, sauf dans les situations mentionnées plus haut. Laisser un dossier dans sa voiture.

5.12. Pratiques à risques et exigences

5.12.1. Le télétravail et le travail à domicile

Le télétravail, le travail à distance et le travail à domicile permettent d'exercer ses fonctions à partir de divers environnements (domicile, lieux publics, véhicule, etc.) situés à l'extérieur des installations et du réseau informatique de l'établissement. Cette modalité accroît les risques, notamment en raison de l'utilisation de réseaux moins sécurisés et de la présence de personnes non autorisées à proximité.

Comportements attendus : les conversations téléphoniques ou *Teams* doivent se faire dans un lieu sécuritaire. Ranger les documents papier dans un endroit sécurisé et appliquer la mise en veille sur votre écran d'ordinateur.

Comportements interdits : donner accès aux RP à des personnes non autorisées (amies ou amis, conjointe ou conjoint, enfants, visiteuses ou visiteurs).

5.12.2. Bonne hygiène informatique

La bonne hygiène informatique repose sur l'adoption de pratiques sécuritaires visant à protéger les renseignements personnels et les actifs informationnels contre les accès non autorisés, les erreurs humaines, les menaces technologiques et les incidents de sécurité.

5.12.2.1. Protection des identifiants de connexion

Les identifiants de connexion (*identifiant unique, nom d'utilisateur, mot de passe, jeton téléaccès, authentification multifacteur (MFA)*) constituent la clé d'accès aux systèmes contenant des renseignements. Leur protection est essentielle. Toute personne doit :

- protéger ses identifiants contre toute utilisation par une autre personne;
- jamais partager ses identifiants, mots de passe ou facteurs d'authentification avec une autre personne;
- utiliser des mots de passe robustes, idéalement sous forme de phrases, avec des symboles, des lettres et des chiffres;
- faire preuve de vigilance face aux demandes d'authentification inhabituelles ou suspectes;

- utiliser des gestionnaires de mots de passe sécuritaires.

5.12.2.2. Mesures de sécurité pour les appareils informatiques et mobiles

Dans l'exercice de ses fonctions, toute personne doit maintenir les mises à jour de sécurité des appareils et des applications. Il est demandé de respecter le verrouillage automatique et l'écran de veille lorsque l'appareil est non utilisé. Les réseaux sécurisés et de confiance doivent être utilisés et il faut éviter les réseaux Wi-Fi publics.

5.12.2.3. Utilisation exceptionnelle de supports amovibles (clé USB)

L'utilisation de supports amovibles doit être évitée autant que possible, compte tenu des outils sécurisés déjà mis à disposition. Lorsqu'aucune alternative n'est possible, seule, une clé USB chiffrée et fournie par l'établissement peut être utilisée.

5.12.2.4. Messagerie électronique et vigilance numérique

Toute communication électronique doit respecter les règles suivantes :

- Utiliser exclusivement les moyens de communication sécuritaires et autorisés par l'établissement[2].
- Vérifier attentivement les destinataires et les pièces jointes avant l'envoi d'un courriel.
- Reconnaître et signaler les tentatives d'hameçonnage (ex. : *courriels, messages textes, liens suspects*) à l'aide des outils prévus (ex. : fonction « *Signaler le message* » dans *Outlook*).

5.13. Incident de confidentialité

La gestion des incidents de confidentialité est encadrée par les lois, lesquelles obligent l'établissement à mettre en place des mécanismes de déclaration, d'interventions, des mesures préventives et correctives, afin de protéger les renseignements personnels et les droits des « personnes concernées ».

Un incident de confidentialité correspond à l'accès, l'utilisation, la communication ou la destruction non autorisés d'un renseignement personnel, de la perte d'un renseignement personnel ou tout autre atteinte à sa protection. On distingue deux types de situations :

- **Situation à risque :** une situation qui pourrait entraîner une atteinte (ex. : *mot de passe partagé, courriel adressé à la mauvaise personne*).
- **Incident avéré :** une atteinte confirmée (ex. : *dossier consulté sans autorisation, perte définitive d'un document ou d'une partie de dossier*).

Un incident de confidentialité peut entraîner des préjudices importants pour les « personnes concernées », notamment une atteinte à la dignité et à la réputation, une atteinte à l'intégrité ou à la sécurité physique d'une personne, une atteinte à la réputation professionnelle, une fraude ou un vol d'identité, une perte financière. Un **préjudice sérieux** est un dommage important, durable ou difficilement réversible. Lorsqu'un tel préjudice est identifié ou est à risque de se produire, une

[2] Adresse de courrier électronique (xxxx@ssss.gouv.qc.ca). Outils de la suite M365 du MSSS dont *Teams*, *Copilot* messagerie instantanée et l'appareil photo.

déclaration obligatoire doit être effectuée auprès des autorités compétentes (Commission d'accès à l'information, ministère de la Santé et des Services sociaux (MSSS), Santé Québec).

Tous les intervenants ayant connaissance d'une situation à risque ou d'un incident doivent :

- agir sans délai et informer sa supérieure ou son supérieur immédiat;
- appliquer immédiatement des mesures de protection pour limiter les impacts;
- contribuer à l'analyse des causes et à la mise en place de mesures correctives;
- collaborer avec les services concernés (DRILLL, gestion des risques, ressources humaines, relations de travail, responsable de la protection des renseignements personnels);
- compléter un formulaire de déclaration d'incident ou d'accident (AH-223) pour les renseignements personnels d'usagères ou d'usagers;
- documenter les circonstances et les actions prises.

Les rôles et responsabilités des gestionnaires en matière d'intervention et les critères encadrant l'implication de la Direction des ressources humaines sont précisés à la section 6.8.

5.14. Plaintes des personnes concernées par les renseignements (publics visés)

La personne concernée par un renseignement personnel peut déposer une plainte lorsqu'elle estime que ses droits n'ont pas été respectés, que les pratiques sont inadéquates ou qu'il existe un risque à l'égard de la protection des renseignements personnels. Un tel recours doit être accessible, sans représailles et traité de façon confidentielle, diligente et impartiale.

Selon la nature des renseignements visés, les plaintes sont acheminées vers les responsables désignés par l'établissement :

- Renseignements de santé et de services sociaux : Commissaire aux plaintes et à la qualité des services (CPQS).
- Renseignements liés aux employées et employés : Direction des ressources humaines.
- Autres types de renseignements : Responsable de la protection des renseignements personnels – Direction de la qualité, de l'évaluation, de la performance et de l'éthique (DQEPE).
- En complément, toute personne conserve le droit d'exercer un recours externe auprès de la Commission d'accès à l'information du Québec (CAI).

Des encadrements spécifiques viennent préciser les pratiques applicables. En cas de doute, les intervenants doivent se référer à leur gestionnaire ou à une ressource désignée.

Les personnes concernées doivent également être informées des mécanismes d'accompagnement mis à leur disposition pour exercer leurs droits.

Comportements attendus : accueillir toute plainte ou préoccupation avec respect, ouverture et professionnalisme. Informer la personne responsable immédiatement. Collaborer au traitement de la plainte lorsque requis.

Comportements interdits : Ignorer, minimiser ou retarder la transmission d'une plainte vers les responsables identifiés. Exercer des représailles, de l'intimidation ou toute pression envers une

personne ayant porté plainte. Divulguer de l'information liée à une plainte à des personnes non autorisées.

5.15. Documents d'encadrement, formation et sensibilisation

La protection efficace des renseignements personnels repose sur l'engagement, les connaissances et les compétences des intervenants.

Santé Québec Laurentides met à la disposition des intervenants des documents d'encadrement, de la formation et de la sensibilisation continue. Ces outils constituent des leviers essentiels pour le développement et le maintien des compétences et permettent d'assurer une protection efficace des renseignements personnels.

Les intervenants sont tenus de comprendre, appliquer et respecter les règles.

Comportements attendus : lire et signer le formulaire de la présente politique. Participer à la formation initiale lors de son entrée en fonction. Prendre connaissance des documents d'encadrement applicables à ses fonctions. Prendre connaissance des activités de sensibilisation. Actualiser ses connaissances. Poser des questions ou solliciter un avis en cas de doute, notamment auprès de son gestionnaire.

Comportements interdits : appliquer des pratiques non conformes par méconnaissance ou absence de formation. Ignorer les documents d'encadrement applicables à ses fonctions.

5.16. Obligation d'information et de transparence

Santé Québec Laurentides a l'obligation légale d'informer le public de ses pratiques organisationnelles en matière de protection des renseignements personnels. Pour ce faire, l'établissement diffuse sur son site Internet une information adaptée et facile à comprendre pour la population qui comprend notamment :

- Les mesures mises en place pour la collecte, l'utilisation, la communication, la conservation et la protection des renseignements personnels;
- Les modalités applicables à la collecte de renseignements par des moyens technologiques, notamment lors de l'utilisation du site Internet de l'établissement;
- Les droits des « personnes concernées » à l'égard de leurs renseignements et des modalités pour les exercer, des mécanismes de plainte et des processus en cas d'incident de confidentialité.

Le contenu diffusé sur le site Internet est révisé périodiquement afin de demeurer à jour, refléter les pratiques réelles de l'établissement et respecter les exigences légales en vigueur.

6. Rôles et responsabilités

La protection des renseignements personnels et le respect de la confidentialité relèvent d'une responsabilité organisationnelle partagée, exercée à tous les niveaux de l'établissement, selon les rôles et responsabilités propres à chacun.

6.1. Président(e)-directeur(-trice) général(e) (PDG) et Président(e)-directeur(-trice) général(e) adjoint(e) (PDGA)

Le PDG et le PDGA exercent un rôle de leadership et de promotion organisationnelle en matière de protection des renseignements personnels et de confidentialité. À ce titre, ils :

- démontrent un engagement exemplaire à l'égard du respect de la confidentialité et de la protection des renseignements personnels.
- soutiennent la mise en œuvre de la présente politique et favorisent son intégration dans les pratiques organisationnelles.
- appuient les initiatives de sensibilisation, de formation et d'amélioration continue menées par la DQEPE.

6.2. Conseil d'administration d'établissement

Pour les membres du conseil d'administration d'établissement (CAÉ), la ou le PDG est responsable de remettre la présente politique, de s'assurer qu'elle est lue et comprise, d'obtenir la signature du *formulaire d'engagement à la confidentialité*, d'en assurer la conservation au dossier du membre concerné et de veiller au respect de la présente politique.

6.3. Direction de la qualité, de l'évaluation, de la performance et de l'éthique (DQEPE)

La DQEPE agit à titre de responsable de la présente politique et assure le leadership organisationnel de sa mise en œuvre. À ce titre, elle :

- assure l'élaboration, la mise en œuvre, le suivi et la révision de la présente politique.
- exerce un rôle de conseil, de vigie, de promotion et de sensibilisation en matière de confidentialité et de protection des renseignements personnels.
- soutient les directions, les gestionnaires et les intervenants dans l'interprétation et l'application de la politique ainsi que des documents d'encadrement qui en découlent.
- développe, diffuse et maintient les outils, guides, formulaires, activités de sensibilisation et documents d'encadrement nécessaires à l'application de la présente politique.
- évalue et approuve les modalités particulières de sensibilisation, de formation, d'engagement ou d'encadrement proposées en remplacement des mécanismes prévus à la présente politique.
- s'assure que les modalités particulières approuvées offrent des garanties équivalentes et qu'elles respectent les exigences légales et organisationnelles applicables.
- maintient et diffuse le registre ou la fiche des modalités particulières approuvées.
- coordonne ou réalise les activités de surveillance, d'audit, d'évaluation et d'amélioration continue liées à l'application de la présente politique.
- formule, lorsque requis, des recommandations visant à renforcer les pratiques organisationnelles en matière de PRP et de confidentialité.
- assure la cohérence de la présente politique avec les obligations légales, les orientations de Santé Québec et les autres documents d'encadrement organisationnels.

6.4. Direction des ressources humaines (DRH)

La DRH joue un rôle central dans l'intégration de la politique aux processus d'embauche et de gestion des ressources humaines. Elle :

- collabore à l'intégration des exigences de confidentialité et de PRP dans les processus d'embauche, d'accueil et d'intégration.
- s'assure que les engagements requis sont obtenus et conservés au dossier de l'employée et de l'employé ou du gestionnaire.
- collabore, lorsque requis, à l'application des mesures administratives ou disciplinaires découlant du non-respect de la présente politique.

6.5. Direction des services professionnels (DSP)

La DSP est responsable de la mise en œuvre de la présente politique auprès des médecins, dentistes, sages-femmes ainsi que des pharmaciennes et pharmaciens exerçant leurs activités au sein de l'établissement.

À ce titre, elle veille à ce que les mécanismes d'information, d'engagement et de respect de la présente politique soient appliqués auprès des membres du conseil des médecins, dentistes, pharmaciens et sages-femmes (CMDPSF).

6.6. Directeurs(-trices) et gestionnaires

Les directrices, directeurs et gestionnaires jouent un rôle clé dans l'application de la présente politique et dans le maintien d'une culture de protection des renseignements personnels au sein de leurs équipes. À ce titre, ils :

- s'assurent que les personnes sous leur responsabilité connaissent et respectent les exigences applicables.
- favorisent la sensibilisation, la formation et l'adoption de pratiques conformes.
- interviennent rapidement lors de situations à risque ou d'incidents de confidentialité.
- mettent en œuvre les mesures correctives requises.
- soumettent à la DQEPE toute demande de dérogation concernant les mécanismes d'engagement prévus à la présente politique, notamment la lecture de la politique et la signature du formulaire d'engagement.

6.7. Intervenants

Tous les intervenants doivent respecter la politique et les règles de confidentialité, mais les modalités retenues pour démontrer leur engagement, leur sensibilisation ou leur formation peuvent varier selon leur statut ou leur contexte d'exercice.

L'intervenant » assume les responsabilités suivantes :

- prend connaissance et respecte les exigences de la présente politique ainsi que les documents d'encadrement applicables à ses fonctions ou à ses activités.
- adhère aux modalités de sensibilisation, de formation, d'engagement ou d'encadrement établies par l'établissement ou approuvées par la DQEPE pour sa catégorie d'intervenants.

- maintient à jour ses connaissances en matière de confidentialité et de protection des renseignements personnels.
- adopte des comportements responsables, éthiques et respectueux de la confidentialité.
- accède, utilise, communique, conserve et détruit les renseignements personnels conformément aux lois applicables ainsi qu'aux règles de l'établissement.
- signale sans délai à son gestionnaire toute situation à risque, anomalie ou incident de confidentialité dont il a connaissance.
- collabore à toute intervention visant à prévenir, analyser, corriger ou mettre en place des mesures d'atténuation à l'égard d'une situation à risque ou d'un incident de confidentialité.

7. Modalités d'application de la politique

Santé Québec Laurentides met en place les mécanismes nécessaires afin de s'assurer que les intervenants connaissent et comprennent leurs obligations en matière de confidentialité et de PRP dès leur arrivée au sein de l'organisation.

La présente politique est portée à la connaissance des intervenants lors de leur embauche, de leur entrée en fonction ou avant le début de leurs activités au sein de l'établissement.

7.1. Processus standard de sensibilisation et d'engagement

La diffusion de la politique, la sensibilisation aux obligations qui en découlent et la gestion des engagements relèvent des directions responsables de l'accueil, de l'intégration ou de l'encadrement des différentes catégories d'intervenants. À ce titre :

- la Direction des ressources humaines veille à l'application de ces exigences pour les employées ou les employés et les gestionnaires.
- la Direction des services professionnels veille à leur application pour les médecins, dentistes, sages-femmes, pharmaciennes et pharmaciens.
- les autres directions concernées veillent à l'application des modalités prévues pour les intervenants sous leur responsabilité, conformément aux mécanismes établis ou approuvés par l'établissement.

7.2. Modalités adaptées à certaines catégories d'intervenants

Toutefois, pour certaines catégories d'intervenants, des modalités particulières peuvent être mises en œuvre relativement à la sensibilisation initiale, à la présentation de la présente politique ou à l'engagement de confidentialité requis lors de l'arrivée au sein de l'établissement.

Ces modalités particulières ne dispensent pas les intervenants du respect des obligations prévues à la présente politique. Elles visent uniquement à adapter les mécanismes utilisés pour informer les intervenants de leurs obligations et obtenir leur engagement à les respecter.

Toute modalité particulière doit offrir des garanties équivalentes aux mécanismes prévus au processus standard et être approuvée par la Direction de la qualité, de l'évaluation, de la performance et de l'éthique (DQEPE).

Les modalités particulières applicables sont consignées dans le registre ou la fiche maintenue par la DQEPE. Elles peuvent notamment concerner les résidentes et résidents en médecine, les stagiaires, les bénévoles ou toute autre catégorie d'intervenants pour laquelle un mécanisme adapté a été approuvé.

7.3. Texte publié sur le site Internet

Le texte publié sur le site Internet de l'établissement répond aux obligations de transparence prévues par les lois applicables. Il est mis à jour de façon continue afin de refléter l'évolution des pratiques, des documents d'encadrement et des exigences légales.

Des mécanismes de communication adaptés sont également mis en place afin d'informer le public des pratiques, des engagements et des mesures mises en œuvre par l'établissement en matière de protection des renseignements personnels.

8. Mesures applicables en cas d'inobservation

Tout manquement à la confidentialité, au secret professionnel ou à la protection des renseignements personnels peut entraîner des conséquences importantes pour les personnes concernées, les intervenants impliqués ainsi que pour l'établissement.

Le respect de la présente politique et des documents d'encadrement qui en découlent est obligatoire.

Toute personne qui contrevient aux exigences applicables s'expose à des mesures proportionnelles à la nature, à la gravité, à la fréquence et aux conséquences du manquement constaté.

Selon le contexte, ces mesures peuvent notamment comprendre :

- des mesures d'accompagnement, de sensibilisation ou de formation;
- des mesures administratives;
- des mesures disciplinaires pouvant aller jusqu'au congédiement;
- des mesures académiques ou pédagogiques, pouvant notamment mener à la suspension ou à la fin d'un stage;
- des mesures contractuelles, incluant la résiliation d'un contrat ou l'exclusion d'un fournisseur;
- des mesures professionnelles, incluant un signalement à un ordre professionnel lorsque requis;
- des recours civils, administratifs, pénaux ou criminels prévus par les lois applicables.

La Commission d'accès à l'information du Québec (CAI), dans l'exercice de ses pouvoirs de surveillance et de contrôle, peut également imposer des sanctions administratives ou pénales, incluant, le cas échéant, l'octroi de dommages punitifs lorsqu'une atteinte illicite est constatée.

9. Mécanisme de suivi et de révision

La DQEPE assure le suivi de l'application de la présente politique. Une première évaluation de sa mise en œuvre est réalisée dans les vingt-quatre (24) mois suivant son adoption. Par la suite, la politique peut être révisée en tout temps afin de tenir compte de l'évolution des exigences légales,

réglementaires, organisationnelles ou opérationnelles. Elle doit faire l'objet d'une révision complète au plus tard cinq (5) ans après son entrée en vigueur.

10. Demande de renseignements

Pour une interprétation du texte ou pour une demande de renseignements concernant la présente politique, veuillez communiquer avec :

Service de la protection des renseignements personnels (PRP)
Direction de la qualité, de l'évaluation, de la performance et de l'éthique (DQEPE)
Santé Québec Laurentides
Courriel : prp.cissslau@ssss.gouv.qc.ca

Annexe 1 : Cadre légal et administratif

Cette liste ne présente pas un recensement exhaustif des lois, règlements et normes auxquels le Santé Québec Laurentides est assujetti.

Charte des droits et libertés de la personne. (RLRQ, chapitre C-12).
https://www.legisquebec.gouv.qc.ca/fr/document/lc/c-12

Code civil du Québec. (RLRQ, c. CCQ-1991) et ses règlements.
https://www.legisquebec.gouv.qc.ca/fr/document/lc/ccq-1991

Code des professions. (RLRQ, chapitre C-26)
https://www.legisquebec.gouv.qc.ca/fr/document/lc/c-26

Codes de déontologie des professionnels du domaine de la santé et des services sociaux.

Loi canadienne sur les droits de la personne. (L.R.C. (1985), ch. H-6.)
https://laws-lois.justice.gc.ca/fra/lois/h-6/

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. ([*LADOP*] RLRQ, c. A-2.1).
https://www.legisquebec.gouv.qc.ca/fr/document/lc/A-2.1

Loi sur les renseignements de santé et de services sociaux. ([*LRSSS*] RLRQ, c. R-22.1).
https://www.legisquebec.gouv.qc.ca/fr/document/lc/R-22.1

Loi sur la gouvernance et la gestion des services de santé et des services sociaux. ([*LGSSSS*] RLRQ, c. G-1.021). https://www.legisquebec.gouv.qc.ca/fr/document/lc/G-1.021

Loi sur les services de santé et les services sociaux. (RLRQ, c. S-4.2).
https://www.legisquebec.gouv.qc.ca/fr/document/lc/s-4.2

Loi sur la santé publique. (RLRQ, c. S-2.2)
https://www.legisquebec.gouv.qc.ca/fr/document/lc/s-2.2

Loi sur la protection des renseignements personnels et les documents électroniques. (L.C. (2000), ch. 5). https://laws-lois.justice.gc.ca/fra/lois/p-8.6/

Loi sur les archives. (RLRQ, chapitre A-21.1) et ses règlements.
https://www.legisquebec.gouv.qc.ca/fr/document/lc/a-21.1

Loi sur la Bibliothèque et les Archives Canada. (L.C. (2004), ch.11). https://laws-lois.justice.gc.ca/fra/lois/l-7.7/

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement. (RLRQ, c. G-1.03).
https://www.legisquebec.gouv.qc.ca/fr/document/lc/G-1.03

Loi concernant le cadre juridique des technologies de l'information. (RLRQ, chapitre C-1.1).
https://www.legisquebec.gouv.qc.ca/fr/document/lc/C-1.1

Loi facilitant la divulgation d'actes répréhensibles à l'égard des organismes publics. (RLRQ, c. D-11.1.) https://www.legisquebec.gouv.qc.ca/fr/document/lc/d-11.1

Règlement sur la diffusion de l'information et sur la protection des renseignements personnels. (RLRQ, c. A-2.1, r. 2). https://www.legisquebec.gouv.qc.ca/fr/document/rc/a-2.1,%20r.%202

Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques. (RLRQ, c. A-21.1, r.2). https://www.legisquebec.gouv.qc.ca/fr/document/rc/A-21.1,%20r.%202

Règlement sur les incidents de confidentialité. (RLRQ, c. A-2.1, r. 3.1).
https://www.legisquebec.gouv.qc.ca/fr/document/rc/A-2.1,%20r.%203.1%20/

Règlement sur la gouvernance des renseignements de santé et de services sociaux. ([RLRQ, c. R-22.1, r.2) https://www.legisquebec.gouv.qc.ca/fr/document/rc/R-22.1,%20r.%202%20/

Règlement d'application de certaines dispositions de la Loi sur les renseignements de santé et de services sociaux. (RLRQ, c. R-22.1, r. 1)
https://www.legisquebec.gouv.qc.ca/fr/document/rc/R-22.1%2C%20r.%201%20/

Annexe 2 : Documents de référence

Code d'éthique de Santé Québec https://sante.quebec/inc/documents/sante_quebec-code_ethique_deontologie_synthese.pdf

Santé Québec Laurentides. *Lexique des concepts clés en matière de protection des renseignements personnels*. http://cissslaurentides.intranet.reg15.rtss.qc.ca/fileadmin/intranet/cisss_laurentides/A_Propos/Directions/DPACQ/PRP/LI_Lexique_PRP.pdf

Santé Québec – Bureau de la PCD, des affaires juridiques et de la gouvernance (2025, juin). *Politique-cadre sur l'accès à l'information et la gouvernance des renseignements personnels*. https://msss365.sharepoint.com/sites/SanteQc-SanteQuebecInfo/Documents%20partages/Forms/AllItems.aspx?id=%2Fsites%2FSanteQc%2DSanteQuebecInfo%2FDocuments%20partages%2FPolitique%2Dcadre%5FAIPRP%2Epdf&parent=%2Fsites%2FSanteQc%2DSanteQuebecInfo%2FDocuments%20partages