Politique de gouvernance en matière de protection des renseignements personnels			
Direction(s) responsable(s)	Direction de la qualité, de l'évaluation, de la performance et de l'éthique	Approuvé	2026-02-02
		Révisé	
Personne(s) concernée(s)	Membres du personnel, CMDPSF, étudiants, stagiaires, bénévoles et partenaires du CISSS de la Montérégie-Ouest.		
Document(s) associé(s)	POL-10046 Politique de déclaration et d'analyse des incidents et des accidents – Usagers PRO-10045 Procédure de déclaration et d'analyse des incidents et des accidents - Usagers et de gestion des événements sentinelles ADM-DQEPE-10003 Formulaire d'engagement à respecter la politique cadre de gouvernance des renseignements personnels et de santé et de services sociaux ADM-DSMREU-10008 Formulaire d'engagement bénévole		

1. Énoncé

Depuis le 1er décembre 2024, le Centre intégré de santé et de services sociaux de la Montérégie-Ouest (ci-après « l'Établissement ») fait partie intégrante de Santé Québec. Cette intégration implique l'harmonisation des pratiques en matière de protection des renseignements personnels (ci-après « PRP ») à l'échelle du réseau de la santé et des services sociaux (ci-après « RSSS »).

La présente politique vise à mettre en œuvre les principes et responsabilités énoncés à la Politique-cadre de Santé Québec sur l'accès à l'information et la gouvernance des renseignements personnels (ci-après « Politique-cadre »). Elle définit la structure de gouvernance, les autorités décisionnelles, les responsabilités et les mécanismes de supervision par lesquels l'Établissement assure la PRP.

La présente politique doit être interprétée de manière à favoriser la PRP des usagers et toute personne œuvrant pour l'Établissement tout en permettant à l'Établissement d'accomplir efficacement sa mission de prestation de soins et de services sociaux. En cas d'ambiguïté, l'interprétation retenue est celle qui assure le meilleur équilibre entre ces deux impératifs.

2. Champ d'application/Contexte légal

La présente politique couvre tous les renseignements personnels (ci-après « RP ») et renseignements de santé et de services sociaux (ci-après « RS ») détenus par l'Établissement, sans égard à leur support ou lieu de conservation.

Toute personne œuvrant pour l'Établissement ayant accès à des RP-RS dans le cadre de ses fonctions au sein de l'Établissement doit se conformer à cette politique. Sont notamment concernés les membres du personnel, les membres du Conseil des médecins, dentistes, pharmaciens et sages-femmes (CMDPSF), les étudiants, les stagiaires, les bénévoles ainsi que les partenaires d'affaires liés par contrat.

CONTEXTE LÉGAL

- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ c. A-2.1;
- Loi concernant le cadre juridique des technologies de l'information (RLRQ c. C-1.1);
- Loi modernisant les dispositions législatives en matière de protection des renseignements personnels, LQ 2021, c. 25;
- Loi sur les renseignements de santé et de services sociaux, RLRQ c. R-22.1;
- Loi sur les services de santé et les services sociaux, RLRQ c. S-4.1;

- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, RLRQ c. G-1.03;
- Loi sur la gouvernance du système de santé et de services sociaux, RLRQ c. G-1.021;
- Loi sur les archives, RLRQ, c. A-21.1;
- Règlement d'application de certaines dispositions de la Loi sur les renseignements de santé et de services sociaux, RLRQ à venir;
- Règlement sur l'anonymisation des renseignements personnels, RLRQ à venir;
- Règlement sur la gouvernance des renseignements de santé et de services sociaux, RLRQ à venir;
- Règlement sur les incidents de confidentialité, RLRQ c A-2.1, r 3.1;
- Règlement sur les frais exigibles pour la transcription, la reproduction et la transmission de documents et de renseignements personnels, RLRQ c A-2.1, r. 3;
- Règlement sur l'organisation et l'administration des établissements, c. S-5, r. 3.01;
- Énoncé de politique des trois conseils : Éthique de la recherche avec des êtres humains - EPTC 2;
- Charte des droits et libertés de la personne, RLRQ, c. C-12;
- Code civil du Québec, RLRQ, CCQ-191, c. 64;
- Code des professions, RLRQ, c C-26.

3. Définitions

Comité sur l'accès à l'information et la protection des renseignements personnels et des renseignements de santé et de services sociaux **(« CAIPRP »)**	Comité chargé de soutenir la personne qui exerce la fonction de responsable de la protection des renseignements personnels (ci-après « RPRP ») dans l'exercice de ses responsabilités et dans l'exécution de ses obligations et d'exercer les fonctions qui lui sont confiées par la Loi sur l'accès et la LRSSS.
Évaluation des facteurs relatifs à la vie privée (« ÉFVP ») :	Démarche préventive visant à mieux protéger les RP-RS et à respecter la vie privée des personnes physiques en considérant l'ensemble des facteurs susceptibles d'avoir un impact sur le respect de la vie privée des personnes visées par un projet ou une communication. Elle vise à identifier les risques d'atteinte à la vie privée, à évaluer les impacts de ceux-ci et à mettre en place les mesures requises afin d'atténuer ces risques.
Incident de confidentialité :	Accès, utilisation ou communication non autorisés par la loi d'un RP-RS, perte d'un tel renseignement ou toute autre atteinte à sa protection.
Préjudice sérieux :	Un préjudice sérieux correspond à un acte ou à un événement susceptible de porter atteinte à la personne concernée ou à ses biens et de nuire à ses intérêts de manière non négligeable.
Renseignement personnel (« RP »)	Tout renseignement qui porte sur une personne physique et permet, directement ou indirectement, de l'identifier. Un tel renseignement revêt les caractéristiques suivantes :

1. Il doit faire connaitre quelque chose à quelqu'un;
2. Il doit avoir un rapport avec une personne physique;
3. Il doit être susceptible de distinguer cette personne par rapport à une autre ou de reconnaître sa nature.

Cette définition inclut les renseignements:

1. Identificatoires: adresse, numéro de téléphone, sexe, âge, numéro d'assurance sociale, identifiant numérique, etc.;
2. Financiers: revenu d'une personne, renseignements relatifs à l'impôt, numéro de compte bancaire, biens possédés, numéros de cartes de crédit, etc.;
3. Relatifs au travail ou à l'affiliation: conditions de travail ou d'exercice, dossier disciplinaire, motifs d'absence, dates de vacances, salaire, évaluation du rendement, heures d'entrée et de sortie liées au lieu de travail, etc.;
4. Scolaires: résultats scolaires, diplômes, curriculum vitæ, etc.;
5. Relatifs à l'état civil: document qui atteste, par exemple, l'état civil, le fait qu'une personne ait ou non des enfants ou qu'elle reçoive des prestations d'aide sociale ou de chômage, etc.

Les renseignements visant un membre du personnel de l'Établissement ou un professionnel qui y exerce sa profession, y compris un étudiant ou un stagiaire, ou qui concerne un mandataire ou un prestataire de services, sont des RP lorsqu'ils sont recueillis à des fins de gestion des ressources humaines.

Les RP sont régis par la Loi sur l'accès.

Renseignements de santé et de services sociaux (« RS ») :

Tout renseignement qui permet, même indirectement, d'identifier une personne et qui répond à l'une des caractéristiques suivantes :

1. Il concerne l'état de santé physique ou mentale de cette personne et ses facteurs déterminants, y compris les antécédents médicaux ou familiaux de la personne;
2. 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;

3. 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;
4. Il a été obtenu dans l'exercice d'une fonction prévue par la *Loi sur la santé publique*;
5. Toute autre caractéristique déterminée par règlement du gouvernement.

Un renseignement permettant l'identification d'une personne tels son nom, sa date de naissance, ses coordonnées ou son numéro d'assurance maladie est un RS lorsqu'il est accolé à un renseignement visé ci-dessus ou qu'il est recueilli en vue de l'enregistrement, de l'inscription ou de l'admission de l'usager dans l'Établissement ou de sa prise en charge par un autre organisme du secteur de la santé et des services sociaux.

Un renseignement qui concerne un membre du personnel ou un professionnel de l'Établissement qui y exerce sa profession, y compris un étudiant ou un stagiaire, ou qui concerne un mandataire ou un prestataire de services n'est pas un RS lorsqu'il est recueilli à des fins de gestion des ressources humaines.

Par conséquent, les renseignements concernant les usagers de l'Établissement sont des RS.

Les RS sont régis par la LRSSS.

Sécurité de l'information :

Ensemble des mesures visant à assurer la confidentialité, l'intégrité et la disponibilité de l'information tout au long de son cycle de vie, afin de protéger les actifs informationnels contre les menaces et garantir la continuité des soins et des services sociaux.

4. Objectifs

- Préciser l'application des orientations établies par la Politique-cadre dans le contexte organisationnel de l'Établissement;
- Préciser les rôles et responsabilités des instances et responsables organisationnels pour assurer une gestion collaborative, supervisée et imputable des RP-RS;
- Assurer la cohérence des pratiques, en garantissant que les décisions et les actions en matière de protection des RP-RS sont prises de manière uniforme à travers l'Établissement et en alignement avec les orientations de Santé Québec;
- Établir les mécanismes de reddition de compte, en définissant comment l'Établissement rend compte de ses activités en matière de protection des RP-RS.

5. Rôles et responsabilités

Conseil d'administration

- Agit en tant qu'aviseur auprès du président-directeur général en matière de protection des RP-RS.

Président-directeur général

En tant que personne ayant la plus haute autorité au sein de l'Établissement, le président-directeur général doit :

- Adopter la présente politique;
- Veiller à assurer le respect et la mise en œuvre des lois applicables, de la présente politique et des procédures qui lui sont associées;
- Déléguer son autorité à l'un de ses cadres pour agir à titre de responsable de la protection des RP-RS;
- Arbitrer les risques résiduels ayant une criticité élevée dans le cadre des ÉFVP;
- Faciliter l'exercice des fonctions du responsable de la protection des RP-RS, en s'assurant, notamment, que l'Établissement alloue des ressources adéquates permettant l'application et la mise en œuvre de l'ensemble des exigences législatives en matière de protection des RP-RS.

Direction générale

- Favoriser la collaboration entre les directions et la sensibilisation à l'égard des obligations en matière de protection des RP-RS;
- Intégrer la protection des RP-RS dans l'ensemble des initiatives et des services.

Service des communications

- Développer, en partenariat avec le responsable de la protection des RP-RS, un plan de communication visant la compréhension et l'appropriation des obligations en matière de protection des RP-RS.

Chef des affaires juridiques – Service des affaires juridiques

- Agir à titre de responsable de l'accès aux documents administratifs;
- Recevoir, traiter et répondre aux demandes d'accès et de rectification des documents administratifs;
- Participer au CAIPRP;
- Émettre des recommandations juridiques conformément à la législation applicable.

Direction de la qualité, de l'évaluation, de la performance et de l'éthique

Directeur DQEPE

- Faciliter l'accès au RPRP aux différentes instances de l'Établissement et aux informations nécessaires à l'accomplissement de son mandat;
- Soutenir le RPRP dans la résolution des obstacles organisationnels liés à l'application des mesures de PRP;
- Participer au CAIPRP.

Responsable de la protection des renseignements personnels (conseiller cadre à la protection des renseignements personnels)

- Exercer les fonctions prévues par la loi de manière autonome et indépendante;
- Veiller au respect des obligations légales en matière de protection RP-RS;
- Tenir les registres exigés par la loi;
- Agir à titre de personne-ressource auprès du président-directeur général, du CAIPRP et des directions en matière de protection des RP-RS;
- Être consulté lors de l'élaboration de politiques, directives, projets ou initiatives impliquant des RP-RS;
- Assurer une veille sur l'évolution des obligations légales et des meilleures pratiques et conseiller l'Établissement sur les adaptations nécessaires;
- Présider le CAIPRP;

- Superviser le processus d'évaluation des facteurs relatifs à la vie privée;
- Présenter au CAIPRP les projets nécessitant son examen et aviser le président-directeur général des risques résiduels à criticité élevée;
- Soutenir l'évaluation des incidents de confidentialité pour déterminer s'ils présentent un risque de préjudice sérieux;
- Aviser son directeur et le président-directeur général, le ministre et Santé Québec de tout incident présentant un risque de préjudice sérieux;
- Déclarer à la Commission d'accès à l'information les incidents impliquant des RP-RS présentant un risque de préjudice sérieux;
- Agir comme liaison avec la Commission d'accès à l'information pour les demandes nécessitant son intervention;
- Développer des outils et ressources facilitant la compréhension et l'application des obligations en matière de protection des RP-RS.

Service de gestion de la qualité et des risques

- Recevoir les rapports de déclaration d'incidents et d'accidents liés à la protection des RP-RS, incluant les analyses sommaires et les mesures préventives et correctives identifiées par les gestionnaires, afin d'assurer la constitution et la mise à jour du registre local des incidents pour le CISSS de la Montérégie-Ouest;
- Assurer la liaison avec le RPRP lors d'incident de confidentialité avec un risque de préjudice sérieux;
- Promouvoir une culture d'amélioration continue en matière de PRP et des renseignements sur la santé (RP-RS), en facilitant l'accès aux données issues des déclarations d'incidents et d'accidents liés aux RP-RS;
- Assurer et coordonner le lien avec le programme d'assurances de la Direction des assurances du réseau de la santé et des services sociaux (DARSSS) lorsque requis.

Éthique clinique et organisationnelle

- Fournir des avis et des conseils sur les enjeux éthiques liés à la PRP;
- Collaborer avec le RPRP pour assurer une cohérence entre les approches éthiques et les exigences légales en matière de PRP;
- Intervenir à titre de membre ad hoc du CAIPRP, lorsque requis.

Pôle innovation et recherche

- Participer à la mise en œuvre, à la diffusion et à l'application de la politique ainsi que des procédures et directives qui en découlent au sein de sa direction et auprès des chercheurs et membres de leurs équipes;
- S'assurer que toute recherche fasse l'objet d'une évaluation éthique, scientifique et de convenance et, le cas échéant, d'une ÉFVP;
- Coordonner la réalisation des ÉFVP concernant la recherche;
- S'assurer que les chercheurs, les membres de leurs équipes de recherche et les étudiants complètent les formations obligatoires portant sur les modes opératoires normalisés (« MON ») de l'Établissement et sur les bonnes pratiques cliniques;
- Veiller à ce que la gestion des dossiers des chercheurs sous la responsabilité de sa direction soit conforme aux exigences de la présente politique;
- Tenir un registre des recherches qui ont nécessité une ÉFVP;
- Rendre compte annuellement au CAIPRP;
- Assurer la reddition de compte annuelle des ÉFVP concernant la recherche à la Commission d'accès à l'information (« CAI ») et au ministère de la Santé et des Services Sociaux (« MSSS »);
- Intervenir à titre de membre ad hoc du CAIPRP, lorsque requis.

Comité sur l'accès à l'information et la protection des renseignements personnels

- Conseiller le président-directeur général sur les enjeux stratégiques en matière de protection des RP-RS et d'accès à l'information;
- Formuler des recommandations sur les politiques et directives relatives à la protection des RP-RS;
- Donner son avis sur les projets à l'issue de l'ÉFVP et formuler des recommandations sur leur approbation;

- Recommander au président-directeur général l'approbation ou le refus des projets présentant un risque élevé;
- Établir les orientations relatives à la gestion des incidents de confidentialité;
- Examiner les rapports périodiques sur les incidents de confidentialité et les tendances observées;
- Recommander des mesures d'amélioration continue pour prévenir la récurrence des incidents;
- Établir annuellement le programme de sensibilisation en matière de protection des RP-RS;
- Examiner les indicateurs de participation aux activités de formation et de sensibilisation;
- Recommander des améliorations au programme selon les besoins identifiés et les risques émergents;
- Identifier et promouvoir les meilleures pratiques en matière de protection des RP-RS;
- Assurer une veille sur l'évolution des obligations légales, des normes et des pratiques exemplaires;
- Recommander des initiatives d'amélioration continue;
- Produire un rapport annuel des activités et des recommandations au président-directeur général et à Santé Québec;
- Assurer le suivi des recommandations formulées et des plans d'action convenus.

Direction régionale des ressources informationnelles (« DRIM »)

- Soutenir les détenteurs de l'information dans l'élaboration et la mise en œuvre des mesures technologiques déterminées lors des analyses de risques technologiques de sécurité ainsi que pour la gestion des risques identifiés et des mesures prises pour assurer la sécurité de leurs actifs informationnels;
- Fournir et maintenir les mesures de sécurité technologiques requises et s'assurer de leur conformité aux besoins de l'organisation en matière de sécurité de l'information;
- Soumettre au CAIPRP tout projet d'acquisition, de développement et de refonte de système d'informations ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation, la destruction ou l'anonymisation de RPRS;
- Participer aux rencontres du comité d'ÉFVP impliquant des actifs technologiques en effectuant une évaluation de la conformité et une analyse de risques technologiques de sécurité informationnelle et participer à la gestion des risques identifiés;
- Assurer une surveillance des activités des fournisseurs informatiques;
- Assurer la destruction sécuritaire des RP-RS sur support informatique sous sa responsabilité, conformément aux directives de l'Établissement;
- Assurer, en collaboration avec les directions concernées, de définir et mettre en œuvre les exigences et processus de gestion des accès et de journalisation;
- Assurer, en collaboration avec les directions concernées, la couverture des risques liés aux technologies de l'information dans le cadre des ententes avec des tiers, notamment dans le cadre de l'élaboration des contrats et des appels d'offres;
- Participer au CAIPRP.

Direction des ressources humaines et du développement organisationnel (« DRHDOA »)

- Assurer la planification et la mise en œuvre des activités de formation et de sensibilisation en lien avec la présente politique en collaboration avec le responsable de la protection des RP-RS, auprès du personnel, des étudiants, des stagiaires et des enseignants;
- Développer, en partenariat avec le responsable de la protection des RP-RS, des outils facilitant la compréhension et l'appropriation des obligations en matière de protection des RP-RS;
- Assurer les suivis requis avec les étudiants, professeurs et les stagiaires en lien avec le respect de leurs obligations en matière de protection des RP-RS;
- Tenir un registre des évaluations de la qualité de la pratique professionnelle et de pratiques réflectives autorisées dans l'Établissement menées par les étudiants;
- Accompagner les gestionnaires lors des suivis requis auprès des individus œuvrant au sein de l'Établissement, et participer aux processus d'enquêtes administratives et ou disciplinaires en cas de non respect de la présente politique;
- Veiller à ce que la gestion des dossiers des employés, professeurs, des stagiaires et des étudiants sous la responsabilité de sa direction soient conformes aux exigences de la présente politique.
- S'assurer de la complétion des formations obligatoires par les étudiants, les stagiaires et les professeurs voulant obtenir l'accès à des RP-RS pour fins de formation, d'études, ou de pratique réflexive (ex : évaluation de la qualité de l'acte médical);

- Évaluer la nécessité d'effectuer une évaluation de protection des RS pour toute demande d'accès, d'utilisation ou de communication de RS pour fins de formation, d'études, ou de pratique réflexive et coordonner la réalisation de cette évaluation si requise;
- Intervenir à titre de membre ad hoc du CAIPRP, lorsque requis.

Direction de la logistique (« DL »)

- Veiller à ce que les règles de la présente politique soient portées à l'attention de tout prestataire de services, fournisseur ou sous-traitant agissant pour le compte de l'Établissement lorsque ce dernier est susceptible d'avoir accès à des RP-RS;
- Veiller, en collaboration avec le service des affaires juridiques et la DRIM, à ce que tout appel d'offres comporte les critères appropriés en matière de protection des RP-RS et de sécurité de l'information;
- Veiller, en collaboration avec le service des affaires juridiques, à ce que tout contrat avec un prestataire de services, un fournisseur ou sous-traitant agissant pour le compte de l'Établissement comporte des clauses appropriées en matière de protection des RP-RS;
- Intervenir à titre de membre ad hoc du CAIPRP, lorsque requis.

Direction médicale et des services professionnels (« DMSP »)

- Appliquer les mesures disciplinaires ou administratives appropriées, ainsi que les mesures prévues aux codes de déontologie ou aux codes d'éthique, à l'égard des personnes régies par sa direction et reconnues responsables du non-respect de la présente politique.

Direction des programmes Soins critiques et spécialisés (« DPSCS »)

Responsable de l'accès et de la protection des renseignements personnels – Volet dossiers d'usagers

- Agir à titre de responsable de l'accès aux documents et de la protection des RS pour les dossiers usagers et pour les informations cliniques;
- S'assurer que le dossier des usagers répond aux normes des différents cadres normatifs ainsi qu'aux lois et règlements applicables;
- Collaborer, avec le responsable de la protection des RP-RS, à la révision et l'élaboration des politiques et procédures requises en matière de gestion des accès et de conservation des dossiers des usagers;
- Collaborer avec la DRHDOA dans le cadre d'enquêtes liées à des incidents de confidentialité en produisant les journaux d'accès et les visualisations nécessaire à l'analyse;
- S'assurer de la communication des dossiers usagers et des RS contenus dans ceux-ci en conformité avec les règles et lois en vigueur;
- Recevoir et répondre aux demandes de rectification aux dossiers des usagers;
- Participer à la mise à jour du calendrier de conservation et en assurer l'application pour les RS;
- Mettre en place les processus de travail nécessaires au sein de son équipe afin d'assurer la gestion, l'accès et la conservation des dossiers des usagers;
- Veiller à la protection des RS contenus au dossier de l'usager;
- Participer aux différentes ÉFVP lorsque requis;
- Participer au CAIPRP.

Archives médicales, accueil et gestion documentaire

- Élaborer et maintenir à jour les documents pour lesquels il est responsable;
- Conserver les documents selon les règles et la durée établies au calendrier de conservation;
- Procéder à la destruction des documents semi-actifs arrivés à échéance qui lui ont été transférés, conformément aux règles en vigueur;
- Assurer la confidentialité des documents comportant des RP-RS qui lui ont été transférés ou versés en vertu de la *Loi sur les archives*;
- Convertir les documents physiques en format numérique pour une conservation à long terme;
- Veiller à la sécurité des informations sensibles, en mettant en place des mesures pour empêcher l'accès non autorisé et les atteintes à la confidentialité;

- Réviser, en collaboration avec le responsable de la protection des RP-RS, les politiques et procédures en matière de gestion documentaire afin de les rendre conformes aux exigences des cadres légaux applicables.

Service du bénévolat

- Assurer la complétion du « Formulaire d'engagement bénévole » (ADM-DSMREU-10008) par tout bénévole;
- S'assurer auprès des bénévoles de leur compréhension de leurs obligations en matière de protection des RP-RS et du respect de celles-ci;
- S'assurer que les formations pertinentes en matière de protection des RP-RS leur soient rendues disponibles.

Commissaire local aux plaintes et à la qualité des services

- Traiter les plaintes concernant le respect des droits des usagers en matière de protection des RP-RS.

Ensemble des directions

- Participer à la mise en œuvre, à la diffusion et à l'application de la politique ainsi que des procédures et directives qui en découlent au sein de leur direction;
- Assurer la mise en œuvre et le suivi des activités de formation et de sensibilisation en lien avec la présente politique auprès de leur direction;
- Déclarer tout incident de confidentialité RS via le formulaire AH-223-1 selon les procédures applicables, et aviser le Service de la gestion de la qualité et des risques en cas de risque de préjudice sérieux;
- Déclarer tout incident de confidentialité RP via le formulaire de déclaration sur Intranet, et aviser le RPRP en cas de risque de préjudice sérieux.

Directeurs

- Informer et soutenir les gestionnaires de leur direction quant aux obligations liées à la protection des RP-RS.

Gestionnaires

- Informer le personnel sous son autorité du contenu du formulaire d'engagement à respecter la politique de gouvernance des RP-RS et conserver un registre de présence;
- S'assurer d'une gestion rigoureuse des accès aux RP-RS pour le personnel sous son autorité;
- Sensibiliser et communiquer les attentes à l'ensemble du personnel sous son autorité quant à l'importance de la protection des RP-RS;
- S'assurer que les membres du personnel sous son autorité connaissent et respectent l'ensemble des règles applicables en matière de protection des RP-RS ainsi que les mesures de protection recommandées par le CAIPRP;
- S'assurer de la conservation et de la destruction sécuritaire des RP-RS sous sa responsabilité conformément aux procédures en vigueur;
- Déclarer les incidents de confidentialité conformément aux procédures applicables;
- Interpeller le responsable de la protection des RP-RS pour toute question ou enjeu en lien avec les obligations liées à la protection des RP-RS;
- Interpeller le responsable de la protection des RP-RS pour tout projet ou initiative impliquant une nouvelle collecte, nouvelle communication ou nouvelle utilisation des RP-RS.

Personnes visées par la politique

- Prendre connaissance de la présente politique ainsi que des procédures et directives qui en découlent et s'y conformer;
- Accorder une grande importance à la protection des RP-RS;
- Utiliser, dans le cadre de l'exercice de ses fonctions, les droits d'accès qui lui ont été accordés strictement pour les fins pour lesquelles ils sont recueillis;
- S'assurer que tout document susceptible de contenir des RP-RS soit conservé uniquement aux emplacements expressément désignés à cette fin;

- S'adresser au responsable de la protection des RP-RS, ou à son gestionnaire s'il s'agit d'un membre du personnel, en cas de doute sur ses obligations liées à la protection des RP-RS;
- Signaler au responsable de la protection des RP-RS, ou à son gestionnaire s'il s'agit d'un membre du personnel, tout non-respect des obligations liées à la protection des RPRS;
- Déclarer tout incident de confidentialité dont il prend connaissance, conformément aux procédures applicables.

STRUCTURE DE GOUVERNANCE

Comité sur l'accès à l'information et la protection des renseignements personnels

L'Établissement institue un CAIPRP responsable de la gouvernance et de la supervision en matière de protection des RP-RS dans l'ensemble de l'Établissement. Le CAIPRP préside le cadre organisationnel en matière de PRP de l'Établissement et supervise la prise de décision stratégique en matière de conformité et de PRP.

La structure de gouvernance incarnée par le CAIPRP reflète les pratiques de gestion de l'information de l'Établissement et fournit l'assurance que les stratégies, politiques, standards, processus et ressources destinés à gérer les risques liés à la protection des RP-RS et à la sécurité de l'information sont alignés avec les objectifs de l'Établissement et conformes aux lois, standards et meilleures pratiques applicables.

Composition et représentation transversale

Le CAIPRP regroupe des représentants des secteurs organisationnels clés de l'Établissement, chacun apportant son expertise, ses perspectives et les enjeux spécifiques à son domaine. Cette composition transversale assure que les considérations relatives à la protection des RP-RS sont intégrées transversalement dans l'ensemble des processus et initiatives de l'Établissement.

Le CAIPRP est présidé par le RPRP et réunit des représentants des fonctions suivantes :

Membres permanents :

- Conseiller cadre à la protection des renseignements personnels (responsable de la protection des renseignements personnels) – DQEPE;
- Coordonnateur des services d'accueil et d'archives médicales (responsable de l'accès aux documents usagers) DPSCS;
- Chef du service des affaires juridiques (responsable de l'accès aux documents administratifs) – SAJ;
- Direction des ressources informationnelles de la Montérégie – DRIM;
- Service de la transformation numérique - DQEPE;
- Directeur de la Direction de la qualité, de l'évaluation, de la performance et de l'éthique – DQEPE.

Membres ad hoc :

- Direction de la logistique – DL;
- Direction des ressources humaines, du développement organisationnel et de l'apprentissage – DRHDOA;
- Conseiller cadre au partenariat avec les usagers et à l'éthique clinique – DQEPE;
- Direction des soins infirmiers et de l'enseignement universitaire – DSIEU;
- Pôle innovation et recherche – DQEPE.
- Direction des services multidisciplinaires, de la recherche et de l'enseignement universitaire – DSMREU
- Service des communications – DG

Mandat et rôle stratégique

Le CAIPRP constitue l'instance centrale de coordination, d'orientation et de supervision des activités liées à la protection des RP-RS de l'Établissement. Il sert de forum pour discuter des tendances émergentes en matière de risques à la PRP, pour aborder les défis de confidentialité, pour évaluer les nouvelles initiatives et pour développer des stratégies de gestion proactive des risques. Le CAIRPRP s'assure que les considérations relatives à la PRP sont intégrées dès la conception des projets et des processus organisationnels.

Le CAIPRP développe, met en œuvre et améliore la stratégie de l'Établissement en matière de protection des RP-RS. Il est consulté lors de l'élaboration de toute politique, procédure ou directive impliquant des RP-RS ou touchant à la PRP, et émet des avis sur leur conformité et leur cohérence avec la présente Politique.

Le CAIPRP approuve les évaluations des facteurs relatifs à la vie privée pour les projets technologiques et formule des recommandations au président-directeur général pour les projets à risque élevé. Il assure également une vigie sur la gestion des incidents de confidentialité, révise annuellement les activités de formation et de sensibilisation, identifie les meilleures pratiques et soutient leur diffusion au sein de l'Établissement.

Sous-comités et groupes de travail

Pour faciliter l'examen approfondi de dossiers spécifiques ou soutenir le développement de politiques et d'orientations, le CAIPRP peut constituer des sous-comités thématiques ou des groupes de travail opérationnels. Ces structures complémentaires permettent de mobiliser l'expertise des secteurs opérationnels concernés au besoin, sans alourdir le fonctionnement du CAIPRP. Les sous-comités et groupes de travail mènent leurs travaux et formulent des recommandations au CAIPRP, qui conserve l'autorité décisionnelle.

Fonctionnement et collaboration

Le CAIPRP se réunit minimalement 6 fois par année selon un calendrier établi et peut convoquer des séances extraordinaires selon les besoins.

Les membres du CAIPRP agissent à titre de relais dans leurs directions respectives, favorisant la communication bidirectionnelle entre le comité et les secteurs opérationnels. Les membres du CAIPRP détermine les canaux de diffusion appropriés pour assurer le relais des orientations et décisions stratégiques.

Reddition de compte

Le CAIPRP fait un compte rendu de ses travaux au président-directeur général et à Santé Québec annuellement. Ces rapports rendent notamment compte de l'état de la protection des RP-RS dans l'Établissement, des travaux du CAIPRP et de ses sous-comités, des incidents survenus, des projets évalués, des politiques développées et des recommandations d'amélioration.

Autorités décisionnelles

Le président-directeur général délègue au RPRP l'autorité d'exercer les fonctions prévues par la loi de manière autonome et indépendante. Le président-directeur général demeure l'autorité pour arbitrer les risques résiduels à criticité élevée identifiés dans les évaluations des facteurs relatifs à la vie privée.

ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

Principes et finalité

L'ÉFVP constitue un outil de gestion des risques permettant d'identifier et de minimiser les risques liés à la protection des RP-RS dès la conception d'un projet. L'ÉFVP s'inscrit dans une approche de protection de la vie privée dès la conception et par défaut, assurant que les considérations relatives à la PRP sont intégrées tout au long du cycle de développement des projets.

L'ÉFVP est un document évolutif qui accompagne le projet tout au long de son cycle de vie et fait l'objet de révisions lors de changements significatifs. Elle ne constitue pas un simple exercice d'approbation administrative, mais un outil de gestion intégré à la planification et au développement des projets.

Projets assujettis

L'Établissement procède à une évaluation des facteurs relatifs à la vie privée pour :

Tout projet d'acquisition, de développement ou de refonte de produits ou services technologiques ou de système de prestation électronique de services impliquant des RP-RS;

- Tout projet de recherche nécessitant l'accès à des RP-RS sans le consentement de la personne concernée;

- Toute communication de RP à des fins d'étude, de recherche ou de production de statistiques sans le consentement de la personne concernée;
- Toute communication de RP-RS à l'extérieur du Québec;
- Toute collecte de RP-RS pour le compte d'un autre organisme.

L'ÉFVP doit être réalisée avant le début du traitement des RP-RS et doit être révisée lorsque des changements importants surviennent dans le projet.

Responsabilités

Le porteur de projet initie et complète l'ÉFVP dès les premières étapes de planification d'un projet assujetti à l'obligation d'évaluation. Il documente les caractéristiques du projet, les traitements de renseignements personnels prévus et les systèmes impliqués. Il consulte les instances concernées qui apportent leur expertise pour identifier les risques relatifs à la vie privée et recommander les mesures d'atténuation appropriées. Le porteur de projet intègre ces recommandations dans l'ÉFVP et collabore à la mise en œuvre des mesures d'atténuation proposées.

Le CAIPRP accompagne le porteur de projet tout au long du processus d'élaboration de l'ÉFVP. Il examine l'ÉFVP produite par le porteur et valide sa conformité avec les exigences légales et les orientations de la présente Politique. Il identifie les risques relatifs à la vie privée et propose les mesures d'atténuation appropriées. Une fois l'ÉFVP finalisée, le CAIPRP évalue l'acceptabilité des risques résiduels qui subsistent malgré les mesures d'atténuation mises en place et émet une recommandation finale.

La Direction régionale des ressources informationnelles évalue les risques technologiques de sécurité informationnelle pour tout projet impliquant des systèmes d'information. Elle identifie les mesures de protection techniques nécessaires pour atténuer ces risques et collabore avec le porteur de projet à leur mise en œuvre.

Révision et amélioration continue

Les projets à risque élevé font l'objet d'un suivi périodique par le CAIPRP pour s'assurer que les mesures d'atténuation demeurent adéquates et que les risques identifiés sont effectivement gérés. Des audits de conformité peuvent être réalisés pour évaluer l'application des mesures de mitigation prévues.

Registre et reddition de compte

L'Établissement maintient un registre de toutes les ÉFVP réalisées, incluant le niveau de risque, l'autorité approbatrice, la date d'approbation, les mesures d'atténuation mises en place et les échéances de révision. Ce registre est tenu par le responsable de la protection des RP-RS.

Le CAIPRP produit un rapport annuel sur les ÉFVP réalisées, incluant leur nombre, les niveaux de risque, les principaux enjeux identifiés et les mesures d'amélioration recommandées, transmis au président-directeur général.

GESTION DES INCIDENTS DE CONFIDENTIALITÉ

Déclaration

Toute personne qui constate ou suspecte un incident de confidentialité le déclare sans délai à son gestionnaire et utilise les mécanismes de déclaration établis. Les incidents impliquant des RS sont déclarés via le formulaire AH-223-1, disponible dans le *Système d'information sur la sécurité des soins et des services au Québec (SISSS)* ou selon la modalité en vigueur, conformément aux procédures applicables. Les incidents impliquant les RP sont déclarés au RPRP via le formulaire disponible sur l'Intranet de la PRP.

Évaluation du risque de préjudice sérieux

Le Service de gestion de la qualité et des risques reçoit les rapports de déclaration d'incident ou d'accident, les analyses sommaires ainsi que les mesures préventives et correctives formulées par les gestionnaires, afin de constituer le registre local de l'Établissement. Il s'assure de la recevabilité et de la conformité des déclarations et analyses, et approfondit les démarches d'analyse lorsque requis.

Les directions, avec la collaboration du RPRP pour les RP, et, le cas échéant, du Service de gestion de la qualité et des risques pour les RS, sont responsables d'évaluer les incidents de confidentialité pour déterminer s'ils présentent un risque de préjudice sérieux, en fonction de l'impact pour les personnes concernées.

Notification et transparence

Lorsqu'un incident présente un risque de préjudice sérieux, le RPRP déclare l'incident à la Commission d'accès à l'information du Québec (ci-après « CAI ») et, s'il s'agit de RS, il informe également le ministre de la Santé et Santé Québec.

En collaboration avec le Service de gestion de la qualité et des risques de la DQEPE, la direction concernée procède à la notification des personnes touchées conformément aux modalités établies, en informant le Service des communications lorsqu'il y a un risque médiatique ou lorsqu'une note d'information est nécessaire.

Révision et amélioration continue

Le CAIPRP reçoit un rapport annuel sur les incidents de confidentialité et en analyse les tendances afin d'identifier les causes systémiques, les risques récurrents et les lacunes dans les mesures de protection. Il évalue l'efficacité des mesures préventives mises en place et, au besoin, formule des recommandations d'amélioration continue.

Des audits internes de conformité peuvent être réalisés pour évaluer les pratiques organisationnelles et identifier les mesures correctives nécessaires.

Registre et reddition de comptes

L'Établissement tient deux registres locaux :

1. Le registre des incidents impliquant des RP, documenté par le RPRP.
2. Le registre de tous les incidents et accidents, dans lequel les incidents de confidentialité impliquant des RS sont également inclus. Ce registre est documenté dans le *Système d'information sur la sécurité des soins et des services (SISSS*), sous la responsabilité du Comité sur la gestion des risques.

Le CAIPRP produit un rapport annuel sur les incidents de confidentialité à partir des données des systèmes sources, incluant leur nature, leur fréquence, les mesures prises et les leçons apprises, lequel est transmis au président-directeur général et aux autorités réglementaires selon les exigences applicables.

ACCÈS AUX RP-RS PAR LES PERSONNES AUTORISÉES

Principes généraux

L'accès aux RP-RS par les personnes autorisées par l'Établissement s'effectue conformément aux dispositions de la Politique cadre.

L'Établissement applique le principe du besoin de savoir, selon lequel toute personne impliquée n'accède qu'aux RP-RS strictement nécessaires à l'exercice de ses fonctions. Ce principe est mis en œuvre par des contrôles d'accès techniques dans la mesure où les locaux physiques ou les systèmes d'information le permettent.

Indépendamment des contrôles d'accès techniques, toute personne autorisée demeure tenue de ne consulter que les renseignements strictement nécessaires à l'exercice de ses fonctions, conformément à ses responsabilités professionnelles et, le cas échéant, à ses obligations déontologiques.

Lorsque les capacités techniques d'un système ne permettent pas de restreindre l'accès au strict nécessaire, l'Établissement met en place des contrôles compensatoires, comprenant notamment la journalisation et l'identification de ces systèmes comme priorités d'amélioration.

Cadre de gestion des accès

La gestion des accès aux systèmes d'information, incluant l'attribution, la révision et la révocation des droits d'accès, s'effectue conformément au cadre de gouvernance des technologies de l'information de l'Établissement.

Accès aux RP-RS conservés dans un système d'information ou banque, base ou lac de données

Extraction de données contenant des RP-RS

L'extraction de données contenant des RP-RS doit faire l'objet d'une autorisation émise par le propriétaire de la donnée, occupant une fonction décisionnelle supérieure au sein de la direction concernée, qui confirme la légitimité de l'accès au regard de la finalité du traitement et s'assure que le point de destination des données est sécuritaire.

Accès au lac de données (tables et vues)

L'accès aux données contenant des RP-RS doit faire l'objet d'une autorisation émise par le propriétaire de la donnée, occupant une fonction décisionnelle supérieure au sein de la direction concernée, qui confirme la légitimité de l'accès au regarde de la finalité du traitement. La DRIM assure ensuite la mise en œuvre technique des droits d'accès et ne peut procéder qu'à la suite de cette autorisation d'affaires dûment émise.

Accès aux entrepôts de données de la gestion et de l'évaluation de la performance

L'accès aux entrepôts de données contenant des RP-RS doit être strictement limité aux développeurs dûment autorisés par un gestionnaire occupant une fonction décisionnelle supérieure au sein de la direction concernée. Cet accès privilégié doit être accordé à un nombre minimal de personnes et être justifié par des impératifs opérationnels.

Surveillance des accès numériques

L'Établissement met en place des mécanismes de détection des accès non conformes aux RP-RS. Les modalités de surveillance, de journalisation et d'analyse sont définies dans le cadre de la gouvernance de la sécurité informationnelle.

Tout nouveau système d'information contenant des RP-RS doit posséder des capacités de journalisation permettant de détecter les accès non autorisés ou inappropriés. Les exigences relatives à la journalisation et à la surveillance sont intégrées aux processus d'acquisition et de gestion des actifs informationnels.
Lorsque les capacités techniques d'un système ne permettent pas d'ajouter ces capacités à un système existant, l'Établissement met en place des contrôles compensatoires jugées appropriées et identifie ces systèmes comme priorités d'amélioration, sous réserve que ces mesures peuvent raisonnablement être mises en œuvre.

MESURES VISANT À PROTÉGER LES RP-RS

L'Établissement met en œuvre des mesures de sécurité administratives, physiques et techniques visant à protéger les RP-RS tout au long de leur cycle de vie. Ces mesures visent à assurer la confidentialité, l'intégrité et la disponibilité des RP-RS et à les protéger contre l'accès non autorisé, l'utilisation inappropriée, la modification ou la perte. Les mesures de sécurité sont déterminées sur la base d'évaluation des risques permettant d'identifier les vulnérabilités et de définir les contrôles appropriés. Elles sont proportionnelles à la sensibilité des renseignements, aux risques identifiés et aux caractéristiques organisationnelles de l'Établissement.

En matière de sécurité technologique de l'information, des mesures de protection, incluant celles exigées par le MSSS, la DRIM et le ministre de la Cybersécurité et du Numérique, sont mises en place afin d'assurer la sécurité des infrastructures et des actifs informationnels contenant des RP-RS et de réduire le risque de menaces telles que les cyberattaques, les virus informatiques ainsi que les pannes du réseau et de ces actifs. Ces mesures incluent notamment les contrôles d'accès, les mécanismes d'authentification, les mesures de chiffrement, la journalisation et la surveillance des activités, ainsi que les plans de continuité.

La DRIM a pour mandat d'assurer la mise en œuvre et l'application des politiques et directives en matière de sécurité de l'information. Une équipe responsable de la cybersécurité veille à la mise en place des mesures selon les exigences du centre opérationnel de cyberdéfense (COCD) de Santé Québec, les normes établies et les règles internes et assure la cybersurveillance des infrastructures et des actifs informationnels contenant des RP-RS.

Le RPRP collabore avec les responsables de la sécurité de l'information pour s'assurer que les mesures de sécurité soutiennent adéquatement la PRP et la conformité avec les obligations légales applicables.

En ce qui concerne les RS contenus au dossier d'un usager, les mesures liées à leur protection sont également prévues au cadre de référence d'accès, de gestion, de conservation des dossiers des usagers.

FORMATION ET SENSIBILISATION

Formation obligatoire

Toute personne ayant accès à des RP-RS doit compléter une formation portant sur la protection des RP-RS avant l'octroi de tout accès. Cette formation est obligatoire et couvre notamment les obligations légales, les principes de confidentialité et les responsabilités individuelles.

Engagement de confidentialité

À l'embauche, toute personne concernée doit prendre connaissance de l'engagement de confidentialité de l'Établissement et confirmer sa compréhension et son adhésion aux obligations qui y sont énoncées.

Programme de sensibilisation

Le CAIPRP élabore et révise annuellement un programme de sensibilisation visant à maintenir une culture organisationnelle de PRP. Ce programme tient compte des besoins et risques identifiés, des incidents survenus, de l'évolution des pratiques et des ressources disponibles.

DEMANDES D'ACCÈS ET DE RECTIFICATION

RP-RS

Toute demande d'accès ou de rectification à un document contenant des RS détenu par l'Établissement doit être soumise au service des archives de l'installation concernée.

RP (employés, gestionnaires, médecins, étudiants, stagiaires, bénévoles)

Toute demande d'accès ou de rectification à un document contenant des RP d'un employé, gestionnaire, stagiaire détenu par l'Établissement doit être soumise à l'équipe de la rémunération et des avantages sociaux à l'adresse courriel suivante : remuneration.as.cisssmo16@ssss.gouv.qc.ca

Toute demande d'accès ou de rectification à un document contenant des RP d'un bénévole détenu par l'Établissement doit être soumise à l'adresse courriel suivante : benevolat.cisssmo16@ssss.gouv.qc.ca

Toute demande d'accès ou de rectification à un document contenant des RP d'un médecin détenu par l'Établissement doit être soumise au DMSP.

Documents administratifs

Toute demande d'accès à un document administratif détenu par l'Établissement doit être soumise à l'équipe de l'accès aux documents administratifs à l'adresse courriel suivante : acces.information.cisssmo16@ssss.gouv.qc.ca

TRAITEMENT DES PLAINTES

Les plaintes concernant les services de santé et les services sociaux sont traités par le Commissaire local aux plaintes et à la qualité des services. Un usager ou son représentant peut déposer une plainte écrite ou verbale au commissaire local aux plaintes et à la qualité des services. Le commissaire dispose de 45 jours pour examiner la plainte et transmettre ses conclusions. Si l'usager n'a pas obtenu de réponse dans les 45 jours après le dépôt de sa plainte ou s'il est insatisfait des conclusions, il peut exercer son droit de recours auprès du Protecteur du citoyen.

Les plaintes concernant les RP des employés sont traitées par l'équipe de la rémunération et des avantages sociaux à l'adresse courriel suivante : remuneration.as.cisssmo16@ssss.gouv.qc.ca

6. Références

RECUEIL DES LOIS ET DES RÈGLEMENTS DU QUÉBEC (RLRQ).

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC (GOUV.QC.CA). Modernisation des lois sur la protection des renseignements personnels au Québec

GOUVERNEMENT DU QUÉBEC (quebec.ca). Protection des renseignements personnels

7. Annexe(s)

S.O.

Processus d'élaboration		
Rédigé par	Gabriel Trépanier, responsable de la protection des renseignements personnels (conseiller-cadre à la protection des renseignements personnels).	2025-11-12
Consultation(s)	Marie-Hélène Francoeur, directrice de la qualité, de l'évaluation, de la performance et de l'éthique par intérim	2025-11-12
	Annie-Halpin Benoit, coordonnatrice gestion de la qualité et des risques par intérim, DQEPE	2025-11-12
	Hélène Jean-Baptiste, coordonnatrice des services d'accueil, d'archives médicales, de gestion documentaire et des centres de documentation, DPSCS	2025-11-24
	Sylvain Besombes, chef du service des affaires juridiques, DACJP	2025-11-24
	Samuel Lapointe, chef de service évaluation et gestion de la performance, DQEPE	2025-11-24
	Nicolas Poissant-Gilbert, chef de service, DTSN	2025-11-24
	Diane Archambault, conseillère-cadre à la sécurité des ressources informationnelles régionales, DRIM	2025-11-24
	Bruce Sexton, adjoint à la direction, DRIM	2025-11-24
	Isabelle David, commissaire adjointe aux plaintes et à la qualité des services, DACJP	2025-11-24
	Nadine Trépanier, chef de service - Développement et interopérabilité, DRIM	2025-11-27

Instance(s) de consultation		
Instance(s) consultative(s)	Services des affaires juridiques	2025-11-24

Historique du document		
Recommandé par	Comité de concertation des directeurs adjoints	2026-01-07
Recommandé par	Comité de direction	2026-01-20
Recommandé par	Comité exécutif de gouvernance	2026-01-29
Adopté par	Dominique Pilon, président-directeur général	2026-02-02
Commentaires	Numéro de l'acte d'adoption : PDG_SQ-CISSSMO_20260130-07	