

TITRE : Politique de gouvernance des renseignements de santé et de services sociaux et des renseignements personnels	
RESPONSABLE : Direction des affaires corporatives et partenariats	ÉMISE LE : 2024-11-19
ADOPTÉE PAR : Conseil d'administration	DERNIÈRE RÉVISION : -
POLITIQUE <input checked="" type="checkbox"/>	PROCÉDURE <input type="checkbox"/>

1 PRÉAMBULE

Chaque organisme public a le devoir de protéger les renseignements de santé et de services sociaux et les renseignements personnels qu'il détient, que leur conservation soit assurée par ce dernier ou par un tiers. À cette fin, le Centre intégré de santé et de services sociaux (CISSS) de la Montérégie-Centre (ci-après l'« **Établissement** ») doit appliquer le principe de responsabilité lui imposant notamment le devoir de protéger les renseignements personnels et les renseignements de santé et de services sociaux qu'il détient. Il doit également être en mesure de prouver en tout temps qu'il respecte toutes les obligations en matière de protection des renseignements personnels et des renseignements de santé et de services sociaux, et qu'il prend les mesures nécessaires afin de protéger efficacement ces renseignements.

Pour ce faire, l'Établissement doit notamment adopter une politique de gouvernance à l'égard des renseignements de santé et de services sociaux et des renseignements personnels, et rendre compte de sa conformité à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après « **Loi sur l'accès** ») et à la *Loi sur les renseignements de santé et de services sociaux* (ci-après « **LRSSS** »).

La présente politique énonce les principes fondamentaux applicables au maintien de la sécurité et de la confidentialité des renseignements personnels et des renseignements de santé et de services sociaux détenus par l'Établissement. Elle prévoit également les rôles et responsabilités des personnes visées par la présente politique et des instances appelées à assurer le respect des cadres légaux applicables. Elle établit les normes assurant la protection des renseignements de santé et de services sociaux et des renseignements personnels, tout en permettant l'optimisation de l'utilisation qui en est faite et leur communication en temps opportun. Elle vise ainsi à améliorer la qualité des services offerts en simplifiant la circulation des renseignements de santé et de services sociaux de façon à ce qu'ils suivent les usagers qu'ils concernent dans leur parcours de soins et de services. Plus précisément, elle établit différentes possibilités d'accès à ces renseignements et prévoit les cas et les conditions dans lesquels ils peuvent être utilisés ou communiqués.

Finalement, elle institue un modèle de gouvernance fondé sur la transparence ainsi que sur la responsabilité et l'imputabilité de l'Établissement et des personnes visées.

Cette politique est complémentaire aux politiques, procédures et documents de l'Établissement en vigueur et applicables en matière de protection et de gestion des renseignements personnels et des renseignements de santé et de services sociaux, à savoir notamment :

- CISSSMC, Politique d'accès, de gestion, de conservation des dossiers des usagers, DSM-702;
- CISSSMC, Politique de sécurité des ressources informationnelles, DRIM-101;
- CISSSMC, Politique sur l'attribution et l'utilisation d'équipements et d'appareils de télécommunication mobile, DRIM-201;
- CISSSMC, Procédure relative à l'encadrement de la présence des représentants de fournisseurs dans les installations du CISSSMC, DL-101;
- CISSSMC, Politique de déclaration des incidents et des accidents liés à une prestation de soins et de services aux usagers, DQEPEL-206;
- CISSSMC, Procédure de déclaration des incidents et des accidents liés à une prestation de soins et de services aux usagers, DQEPEL-206a (AH223);
- CISSSMC, Politique de gestion intégrée des documents administratifs, DG-301;
- CISSSMC, Procédure de gestion des documents semi-actifs sous format papier, DG-301a;
- CISSSMC, Procédure de gestion des formulaires cliniques intégrés au dossier de l'utilisateur, DSM-701a;
- CISSSMC, Calendrier de conservation des documents;
- Cadre réglementaire sur l'organisation et les bonnes pratiques de la recherche au CISSS de la Montérégie-Centre;
- CISSSMC, Politique sur la conduite responsable et l'intégrité scientifique en recherche, DR-001;
- CISSSMC, Modes opératoires normalisés (MON) des essais cliniques au CISSS de la Montérégie-Centre, R-2023-33;
- CISSSMC, Politique d'utilisation des médias sociaux, DCAP-001;
- CISSSMC, Politique sur le dossier du cadre, DRHDO-AJ-012;
- CISSSMC, Politique sur le télétravail, DRHDO-AJ-501;
- CISSSMC, Procédure sur la gestion du télétravail, DRHDO-AJ-501a;
- CISSSMC, Procédure sur l'appartenance au système professionnel, DSM-001;
- CISSSMC, Politique sur le consentement aux soins, DSP-002;
- CISSSMC, Politique sur la prise, l'utilisation et la diffusion et/ou partage d'enregistrements audio, photo et vidéo par les usagers et les visiteurs, DSP-005;
- CISSSMC, Politique sur le transfert de l'information aux points de transition des soins et services pour l'utilisateur inscrit ou admis, DSI-101;
- CISSSMC, Code d'éthique organisationnel, R-2017-15;
- Tout autre procédure et document découlant de la présente politique.

La présente politique remplace les documents suivants :

- CSSS Champlain-Charles-Le Moyne, Politique sur l'accès aux documents administratifs et la protection des renseignements personnels, 1-570-01;
- Régie régionale de la santé et des services sociaux, Procédure de gestion des renseignements personnels, 2000-03;
- CSSS Haut-Richelieu-Rouville, Procédure en matière de sécurité des actifs informationnels, de télécommunications et à la protection des données et des renseignements confidentiels, 25 octobre 2005 (révisée en mars 2010).

2 CHAMPS D'APPLICATION

La présente politique s'applique aux personnes visées, aux lieux, aux ressources et aux renseignements suivants :

- **Personnes visées** : Tous les membres du personnel de l'Établissement, les membres du Conseil des médecins, dentistes et pharmaciens (« **CMDP** ») et les sages-femmes, les étudiants, les stagiaires et les bénévoles, ainsi que toute personne physique ou morale liée à l'Établissement par un contrat de services ou d'approvisionnement.
- **Lieux** : Ensemble des installations de l'Établissement de même que tous les lieux où les personnes à qui cette politique est destinée offrent des soins ou des services sociaux, ou des services administratifs.
- **Ressources** : Tous les actifs informationnels sans égard à leur support ou à leur format, qu'ils soient conservés à l'interne ou à l'externe de l'Établissement.
- **Renseignements** : Les renseignements de santé et de services sociaux (« **RS** ») et les renseignements personnels (« **RP** ») que détient l'Établissement, peu importe leur format et leur endroit de conservation.

La présente politique traite de deux types de renseignements, chacun soumis à des régimes juridiques distincts : **(1)** les RP régis par la Loi sur l'accès, et **(2)** les RS encadrés par la LRSSS. L'acronyme « RP », lorsqu'utilisé seul, fait uniquement référence aux renseignements personnels, de sorte que le texte n'est applicable qu'à ce type de renseignements. De même, l'utilisation seule de l'acronyme « RS » indique que le texte s'applique uniquement aux renseignements de santé et de services sociaux. À moins que le contexte ne précise le contraire, l'utilisation des acronymes « RP-RS » englobe à la fois les renseignements personnels et les renseignements de santé et de services sociaux.

3 CADRE JURIDIQUE ET ADMINISTRATIF

Cette politique s'applique conformément aux lois et aux règlements en vigueur, soit :

- *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 des 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.

4 DÉFINITIONS

Dans cette politique, les termes suivants ont le sens qui leur est donné ci-après. À moins que le contexte ne le requière autrement, les variations grammaticales de tout terme défini ont une signification similaire, le singulier inclut le pluriel, et le masculin inclut le féminin, et vice versa.

Actif informationnel :	Actif composé ou supportant de l'information ou des RP-RS, notamment, une banque d'informations, un système d'informations, un réseau de télécommunication, une infrastructure technologique ou un ensemble de ces éléments.
Anonymisation :	Processus de traitement d'un RP ou d'un RS selon les meilleures pratiques généralement reconnues et selon les critères et modalités déterminés par règlement. Un renseignement anonymisé est un renseignement dont tous les identificateurs directs sont irrévocablement retirés et pour lesquels aucun code permettant une réidentification ultérieure n'est conservé. Le risque de réidentification de la personne à partir des identificateurs indirects est faible ou très faible.
Blessures graves :	Toute blessure physique ou psychologique qui nuit d'une manière importante à l'intégrité physique, à la santé ou au bien-être d'une personne ou d'un groupe de personnes identifiable.
Calendrier de conservation :	Calendrier de conservation au sens de la <i>Loi sur les archives</i> et approuvé par la Bibliothèque et Archives nationales du Québec.
Catégorisation :	Processus permettant à l'Établissement d'évaluer les catégories de personnes exerçant leur profession à l'Établissement et du degré de sensibilité des RP-RS auxquels elles auront accès, dans le but d'en déterminer le niveau de protection eu égard aux risques encourus en matière de disponibilité, d'intégrité et de confidentialité.
Comité sur l'accès à l'information et la protection des renseignements	Comité constitué par l'Établissement en vertu de la Loi sur l'accès et chargé de soutenir la personne qui

personnels et des renseignements de santé et de services sociaux (« CAI-PRPRS ») :

exerce la fonction de Responsable de l'accès aux documents et de la protection des renseignements personnels et des renseignements de santé et de services sociaux 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.

Cycle de vie d'un renseignement :

Ensemble des étapes visant le traitement d'un RP-RS, soit la collecte, l'utilisation, la communication, la conservation, la destruction et l'anonymisation, le cas échéant.

Communication :

Toute action visant à transmettre à un tiers des RP-RS ou à y donner accès.

Document administratif :

Tout document qui se rapporte aux activités de l'administration de l'Établissement dans ses divers aspects, peu importe le support (incluant les correspondances par courriel). Inclut notamment le dossier administratif des employés, le dossier de santé des employés, les dossiers de paie et le dossier médical des travailleurs (santé au travail).

Pour les fins de la présente politique, cette définition exclut le dossier des usagers et tout autre document contenant des RS.

Dans la présente politique, l'utilisation du mot « document » réfère à un document administratif.

Dossier d'emploi ou d'affiliation :

Dossier administratif ou de santé des membres du personnel ou des personnes affiliées à l'Établissement qui comprend tout RP relatif à l'emploi ou à l'affiliation qu'il reçoit, quel qu'en soit le support.

Dossier de l'usager :

Dossier médical d'un usager qui comprend tout RS relatif aux soins et services qu'il reçoit quel qu'en soit le support.

Évaluation des facteurs relatifs à la vie privée (« ÉFVP ») :

Démarche préventive visant à prendre en considération l'ensemble des facteurs susceptibles d'avoir un impact sur le respect de la vie privée des personnes visées par un projet. 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.

Format structuré et couramment utilisé :

Format que des applications logicielles d'usage courant peuvent facilement reconnaître et dont elles peuvent extraire les informations qui y sont contenues. Un format difficile à traiter et dont l'utilisation implique l'acquisition d'un logiciel ou d'une licence payante n'est pas considéré comme étant un

	format technologique structuré et couramment utilisé.
Incident de confidentialité :	Accès à un RP-RS, ou toute autre utilisation ou communication d'un tel renseignement non autorisée par la loi, la perte d'un tel renseignement ou toute autre atteinte à sa protection.
Intervenant :	Personne physique qui offre des services de santé ou des services sociaux au sein de l'Établissement ou d'un autre organisme du secteur de la santé et des services sociaux, ou qui fournit à une telle personne des services de soutien technique ou administratif. L'intervenant peut être professionnel (par exemple, un médecin, une infirmière, une inhalothérapeute, etc.), ou non-professionnel (par exemple, un ambulancier, un préposé au bénéficiaire, une adjointe, etc.).
Membre du personnel :	L'ensemble du personnel de l'Établissement, que leur fonction soit en lien ou non avec l'utilisateur.
Participant :	Toute personne dont les RP-RS, le matériel biologique, les réactions ou les réponses à des interventions, des stimuli ou des questions de la part de chercheurs sont utilisés pour répondre aux questions d'une recherche.
Personnes affiliées à l'Établissement :	Les membres du CMDP, les chercheurs, les sages-femmes, les étudiants, les stagiaires et les bénévoles.
Personne concernée :	Personne concernée par le RP.
Préjudice sérieux :	Acte ou événement susceptible de porter atteinte à la personne concernée ou à l'utilisateur, ou à ses biens, et de nuire à ses intérêts de manière non négligeable.
Produit ou service technologique :	Équipement, application ou service requis afin de recueillir, de conserver, d'utiliser ou de communiquer un RP-RS, tels qu'une banque, un système d'informations, un réseau de télécommunication, une infrastructure technologique, un logiciel ou une composante informatique d'un équipement médical.
Professionnel :	Toute personne qui est titulaire d'un permis délivré par un ordre professionnel et qui est inscrite au tableau de ce dernier, au sens du <i>Code des professions</i> .
Recherche :	Démarche visant le développement des connaissances, notamment à des fins d'innovation, au moyen d'un projet structuré ou d'une investigation systématique.
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 connaître 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.

Renseignement personnel à caractère public :

Un RP revêt un caractère public lorsque la loi ou un règlement l'indique expressément. Par exemple, celui concernant l'exercice par la personne concernée d'une fonction au sein d'une entreprise ou organisme, tels que son nom, son titre et sa fonction, de même que l'adresse, l'adresse de courrier électronique et le numéro de téléphone de son lieu de travail.

Un RP qui a un caractère public n'est pas soumis aux règles de protection des RP prévues par la présente politique.

Renseignement personnel sensible : Tout RP qui, par sa nature ou en raison du contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de respect de la vie privée. Certains RP sont sensibles par leur nature ou en raison du contexte de leur utilisation ou de leur communication. Leur référence se révèle assez large et englobante et tient compte des circonstances particulières dans lesquelles s'inscrivent l'utilisation ou la communication eu égard à l'expectative élevée, mais raisonnable, de protection de la vie privée qui en découle. Pour déterminer la sensibilité d'un tel RP, il faut évaluer l'attente en matière de respect de la vie privée de la personne concernée et se demander si une personne raisonnable et bien informée, placée dans la même situation que la personne concernée, aurait un haut degré d'attente en matière de respect de sa vie privée. Par exemple, le numéro d'assurance sociale est considéré comme un RP sensible.

Les RP sensibles 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.

Responsable de l'accès aux documents administratifs :

Personne exerçant la fonction de Responsable de l'accès aux documents administratifs en vertu des cadres légaux applicables.

Pour l'Établissement, cette fonction a été déléguée par la présidente-directrice générale aux personnes suivantes:

Responsable de l'accès aux documents administratifs

Directrice des affaires corporatives et des partenariats

Direction des affaires corporatives et des partenariats

CISSS de la Montérégie-Centre

3141, boulevard Taschereau, bureau 220

Greenfield Park (Québec) J4V 2H2

Courriel: prp.cisssmc16@ssss.gouv.qc.ca

Responsable de l'accès aux documents et de la protection des RS pour les dossiers usagers et pour les informations cliniques:

Cheffe de service des archives

Direction des services multidisciplinaires

3120, boulevard Taschereau

Greenfield Park (Québec) J4V 2H1

HCLM:

archivesmedicales.hclm.cisssmc16@ssss.gouv.qc.ca

HHR: corr.hrr.cisssmc16@ssss.gouv.qc.ca

Autres sites :

<https://www.santemonteregie.qc.ca/services/archives#installation-33>

Afin de l'appuyer dans ses fonctions, la Responsable de l'accès aux documents administratifs peut s'adjoindre de substituts, dont la suivante :

Cheffe des affaires juridiques, substitut à la Responsable de l'accès aux documents administratifs

Direction des affaires corporatives et des partenariats
2727 boulevard Taschereau
Longueuil (Québec) J4T 2E6
acces.information.cisssmc16@ssss.gouv.qc.ca

Responsable de la protection des renseignements personnels et des renseignements de santé et de services sociaux (« Responsable de la protection des RP-RS ») ou ses substituts :

Personne exerçant la fonction de la protection des RP-RS en vertu des cadres légaux applicables.

Pour l'Établissement, cette fonction a été déléguée par la présidente-directrice générale aux personnes suivantes:

Responsable de la protection des RP-RS:

Directrice des affaires corporatives et des partenariats
Direction des affaires corporatives et des partenariats
CISSS de la Montérégie-Centre
3141, boulevard Taschereau, bureau 220
Greenfield Park (Québec) J4V 2H2
Courriel: prp.cisssmc16@ssss.gouv.qc.ca

Responsable de l'accès aux documents et de la protection des RS pour les dossiers usagers et pour les informations cliniques:

Cheffe de service des archives
Direction des services multidisciplinaires
3120, boulevard Taschereau
Greenfield Park (Québec) J4V 2H1
HCLM:
archivesmedicales.hclm.cisssmc16@ssss.gouv.qc.ca

HHR: corr.hrr.cisssmc16@ssss.gouv.qc.ca

Autres sites :

<https://www.santemonteregie.qc.ca/services/archives#installation-33>

Responsable de la protection des RP des dossiers des employés :

Coordonnatrice des ressources humaines – volet relations de travail et relations avec les employés
Direction des ressources humaines et du développement organisationnel

CISSS de la Montérégie-Centre
365 rue Normand
Saint-Jean-sur-Richelieu (Québec) J3A 1T6
Courriel: prp.cisssmc16@ssss.gouv.qc.ca

Afin de l'appuyer dans ses fonctions, la Responsable de la protection des RP-RS peut s'adjoindre de substituts, dont les suivantes :

Conseillères-cadres à la protection des RP-RS, substituts à la Responsable de la protection des RP-RS

Direction des affaires corporatives et des partenariats
CISSS de la Montérégie-Centre
3141, boulevard Taschereau,
Greenfield Park (Québec) J4V 2H2
Courriel: prp.cisssmc16@ssss.gouv.qc.ca

Usager :

Toute personne recevant ou ayant reçu des services de santé ou des services sociaux dispensés par l'Établissement ou par un prestataire de services pour le compte de l'Établissement.

5 OBJECTIFS

- Instituer un modèle de gouvernance fondé sur la transparence, la responsabilité et l'imputabilité;
- Promouvoir et supporter une approche d'amélioration continue;
- Établir les principes directeurs devant soutenir les décisions relatives au maintien de la sécurité et de la confidentialité des RP-RS détenus par l'Établissement;
- Établir les mécanismes de journalisation et les normes assurant la protection des RP-RS tout en permettant l'optimisation de l'utilisation qui en est faite et leur communication en temps opportun;
- Améliorer la qualité des services offerts en simplifiant la circulation des RS;
- Établir les différentes possibilités d'accès aux RP-RS;
- Prévoir les cas et les conditions dans lesquels peuvent être utilisés ou communiqués les RP-RS;
- Définir les rôles et les responsabilités des différents acteurs et instances concernés;
- Définir la composition et le mandat du CAI-PRPRS;
- Prévoir une procédure de gestion des incidents de confidentialité;
- Définir une procédure portant sur l'utilisation ou la communication de RP-RS à des fins de recherche.

6 RÔLES ET RESPONSABILITÉS

Les rôles, responsabilités et obligations en matière de protection des RP-RS sont les suivants :

6.1 CONSEIL D'ADMINISTRATION

- Adopter la présente politique.

6.2 PRÉSIDENTE-DIRECTRICE GÉNÉRALE

En tant que personne ayant la plus haute autorité au sein de l'Établissement, la présidente-directrice générale doit :

- 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 de la Responsable de la protection des RP-RS, en s'assurant 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.

6.3 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.

6.3.1 Bureaux des projets organisationnels et de la transformation numérique

- Participer aux ÉFVP pour les projets dont ils sont porteurs;
- Intégrer la protection des RP-RS dans l'ensemble des projets et des initiatives;
- Solliciter la Responsable de la protection des RP-RS ou ses substituts lors d'enjeux impliquant la protection des RP-RS.

6.4 DIRECTION DES AFFAIRES CORPORATIVES ET DES PARTENARIATS (« DACP »)

6.4.1 Responsable de la protection des RP-RS ou ses substituts

- Exercer les fonctions qui lui sont déléguées par la présidente-directrice générale de manière autonome et indépendante;
- Veiller au respect et la mise en œuvre des cadres légaux applicables à la protection des RP-RS détenus par l'Établissement;
- Présider et coordonner les travaux du CAI-PRPRS de l'Établissement;
- Agir à titre de personne-ressource en matière de protection des RP-RS;
- Contribuer, en partenariat avec les différents partenaires, au développement des outils facilitant la compréhension et l'appropriation des obligations en matière de protection des RP-RS;
- Assurer une vigie concernant les processus de traitement des demandes d'accès, de communication ou de rectification des RP-RS;
- Tenir les registres exigés par la Loi sur l'accès et la LRSSS;
- Prendre part à l'évaluation des risques organisationnels liés à la protection des RP-RS et à l'identification des mesures d'atténuation;
- Aviser la présidente-directrice générale de tout incident de confidentialité présentant un risque de préjudice sérieux;

- Aviser la Commission d'accès à l'information (« **CAI** ») et la personne concernée/l'utilisateur de tout incident de confidentialité impliquant un RP-RS présentant un risque de préjudice sérieux. Si l'incident de confidentialité présentant un risque de préjudice sérieux implique plutôt un RS, le ministre doit également en être avisé;
- Collaborer à l'élaboration des ÉFVP lorsque requis et assurer le suivi avec la présidente-directrice générale pour les risques résiduels à criticité élevée;
- Assurer la mise en œuvre des activités de formation et de sensibilisation;
- Assurer l'application de la politique dans l'Établissement et soutenir les secteurs dans sa mise en œuvre;
- Assurer les suivis avec la CAI lorsque requis;
- Voir à la reddition de comptes.

6.4.2 Cheffe des affaires juridiques – Service des affaires juridiques

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

6.4.3 Service de la 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 numériques et papier comportant des RP-RS qui sont transférés ou versés en vertu de la *Loi sur les archives*;
- Convertir les documents physiques en formats numériques 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 la Responsable de la protection des RP-RS ou ses substituts, les politiques et procédures en matière de gestion documentaire afin de les rendre conformes aux exigences des cadres légaux applicables;
- Participer au CAI-PRPRS.

6.5 CAI-PRPRS

- Soutenir l'Établissement dans l'exercice de ses responsabilités et dans l'exécution de ses obligations découlant de la Loi sur l'accès et de la LRSSS;
- Approuver une politique unifiée encadrant la gouvernance de l'Établissement à l'égard des RP-RS ainsi que toute autre politique ou procédure régissant la gouvernance des RP-RS;
- Assurer la mise en place d'un plan de diffusion entourant la protection des RP-RS en partenariat avec la Direction des communications et des affaires publiques;
- Identifier les bonnes pratiques en matière de protection des RP-RS et soutenir leur diffusion au sein de l'Établissement;

- Assurer la mise en place d'un plan de formation entourant la protection des RP-RS en partenariat avec la Direction des ressources humaines et du développement organisationnel;
- Donner son avis sur l'ÉFVP de tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation, la destruction ou l'anonymisation de RP-RS;
- Émettre les orientations, assurer une vigie et élaborer un plan d'amélioration continue quant à la gestion des incidents de confidentialité;
- Réviser annuellement l'offre d'activités de formation et de sensibilisation en matière de protection des RP-RS et évaluer le taux de participation à ces activités;
- Faire un compte rendu annuel des travaux à la présidente-directrice générale.

6.6 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 CAI-PRPRS 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 RP-RS;
- Participer aux Comités 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;
- Participer, lorsque la nature de l'incident le requiert, au Comité de gestion des incidents de confidentialité concernant les RP-RS;
- Assurer une surveillance des activités des fournisseurs informatiques;
- Assurer la destruction sécuritaire des RP-RS sur support informatique sous sa responsabilité;
- 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 de sécurité informationnelle dans le cadre des ententes avec des tiers, notamment dans le cadre de l'élaboration des contrats et des appels d'offres;
- Participer au CAI-PRPRS.

6.7 DIRECTION DES RESSOURCES HUMAINES ET DU DÉVELOPPEMENT ORGANISATIONNEL (« DRHDO »)

- Assurer la planification et la mise en œuvre des activités de formation et de sensibilisation en lien avec la présente politique en collaboration avec la Responsable de la protection des RP-RS ou ses substituts;
- Développer, en partenariat avec la Responsable de la protection des RP-RS ou ses substituts, des outils facilitant la compréhension et l'appropriation des obligations en matière de protection des RP-RS;
- Assurer la complétion du formulaire d'engagement à respecter la politique de gouvernance des RP-RS de l'Établissement par les membres du personnel;
- Verser au dossier des membres du personnels le formulaire d'engagement à respecter la politique de gouvernance des RP-RS de l'Établissement;

- Accompagner les gestionnaires lors des suivis requis auprès des membres du personnel en lien avec le respect de leurs obligations en matière de protection des RP-RS;
- Assurer une gestion des dossiers des employés de l'Établissement conforme aux exigences prévues à la présente politique;
- Agir à titre de Responsable de la protection des RP pour les dossiers des employés;
- Participer aux processus d'enquête administratives et/ou disciplinaires dans le cadre de non-respect de la présente politique;
- Participer au CAI-PRPRS.

6.8 DIRECTION DE LA RECHERCHE (« DR »)

- 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, chercheuses, membres de leurs équipes, ainsi que de la communauté étudiante;
- Assurer la complétion du formulaire d'engagement à respecter la politique de gouvernance des RP-RS de l'Établissement par les chercheurs, les chercheuses, les membres de leurs équipes et les étudiants;
- 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 chercheuses, 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 CAI-PRPRS;
- Assurer la reddition de compte annuelle des ÉFVP concernant la recherche à la CAI et au ministère de la Santé et des Services Sociaux (« MSSS »).

6.9 DIRECTION DE L'ENSEIGNEMENT ET DES AFFAIRES UNIVERSITAIRES (« DEAU »)

- 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 étudiants, stagiaires et professeurs;
- Assurer la complétion du formulaire d'engagement à respecter la politique de gouvernance des RP-RS de l'Établissement par les étudiants, professeurs et stagiaires;
- 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);
- 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;
- 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;
- Tenir un registre des évaluations de la qualité de l'acte médical et de pratiques réflexives autorisées dans l'Établissement menées par les étudiants;
- Veiller à ce que la gestion des dossiers des professeurs, des stagiaires et des étudiants sous la responsabilité de sa direction soient conformes aux exigences de la présente politique.

6.10 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, la Responsable de la protection RP-RS ou ses substituts 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;
- Assurer la complétion du formulaire d'engagement à respecter la politique de gouvernance des RP-RS de l'Établissement par les prestataires de services, les fournisseurs et les sous-traitants agissant pour le compte de l'Établissement.

6.11 DIRECTION DES SERVICES PROFESSIONNELS ET DE LA FLUIDITÉ HOSPITALIÈRE (« DSP-FH »)

- Assurer la complétion du formulaire d'engagement à respecter la politique de gouvernance des RP-RS de l'Établissement par tout membre du CMDP exerçant leur profession à l'Établissement;
- 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.

6.12 DIRECTION DES COMMUNICATIONS ET DES AFFAIRES PUBLIQUES (« DCAP »)

- Développer, en partenariat avec la Responsable de la protection des RP-RS ou ses substituts, un plan de communication visant la compréhension et l'appropriation des obligations en matière de protection des RP-RS;
- Participer, lorsque la nature de l'incident le requiert, au Comité de gestion des incidents de confidentialité concernant les RP-RS.

6.13 DIRECTION DES SERVICES MULTIDISCIPLINAIRES (« DSM »)

6.13.1 Cheffe des archives – Service des archives

- 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 la Responsable de la protection des RP-RS ou ses substituts, à la révision et l'élaboration des politiques et procédures requises en matière de gestion des accès et de conservation des dossiers des usagers;
- S'assurer de la communication des dossiers usagers et des RS contenues 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 dossiers des usagers;
- 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'utilisateur;

- Participer aux différentes ÉFVP lorsque requis;
- Participer, lorsque la nature de l'incident le requiert, au Comité de gestion des incidents de confidentialité concernant les RP-RS;
- Participer au CAI-PRPRS.

6.13.2 Service des bénévoles

- Assurer la complétion du formulaire d'engagement à respecter la politique de gouvernance des RP-RS de l'Établissement par tout bénévole;
- Assurer les suivis requis avec les membres bénévoles en lien avec le respect de leurs obligations en matière de protection des RP-RS;
- S'assurer que les formations pertinentes en matière de protection des RP-RS soient disponibles, suffisantes et qu'elles soient suivies par les bénévoles.

6.14 DIRECTION DE LA QUALITÉ ÉVALUATION PERFORMANCE ÉTHIQUE ET «LEAN» (« DQÉPÉL »)

- Participer au CAI-PRPRS;
- Intégrer la protection des RP-RS aux points statutaires du Comité de gestion des risques organisationnel;
- Participer, lorsque la nature de l'incident le requiert, au Comité de gestion des incidents de confidentialité concernant les RP-RS.

6.15 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 RS.

6.16 ENSEMBLE DES DIRECTIONS CLINIQUES ET ADMINISTRATIVES, INCLUANT LES DIRECTIONS MENTIONNÉES DANS LES RUBRIQUES CI-DESSUS

- 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;
- Aviser le CAI-PRPRS de tout incident de confidentialité dont leur direction prend connaissance en effectuant une déclaration d'incident de confidentialité conformément aux procédures applicables.

6.16.1 Directeurs

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

6.16.2 Gestionnaires

- 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 CAI-PRPRS;
- 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 la Responsable de la protection des RP-RS ou ses substituts pour toute question ou enjeu en lien avec les obligations liées à la protection des RP-RS;
- Interpeller la Responsable de la protection des RP-RS ou ses substituts pour tout projet ou initiative impliquant une nouvelle collecte, nouvelle communication ou nouvelle utilisation des RP-RS.

6.17 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 sensibilité à la protection des RP-RS;
- Respecter l'ensemble des règles applicables en matière de protection des RP-RS ainsi que des mesures de protection recommandées par le CAI-PRPRS;
- Appliquer les pratiques ainsi que les orientations prônées dans la présente politique, notamment en prenant les mesures nécessaires pour que les conversations comportant des RP-RS demeurent confidentielles;
- Utiliser, dans le cadre de l'exercice de ses fonctions, les droits d'accès qui lui sont confiés strictement pour les fins pour lesquelles ils sont recueillis;
- S'adresser à la 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 à la 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 RP-RS;
- Déclarer tout incident de confidentialité dont il prend connaissance, conformément aux procédures applicables.

7 PRINCIPES DIRECTEURS

- L'Établissement peut recueillir des RP-RS lorsque ces renseignements sont nécessaires à l'accomplissement des différentes missions qui lui sont confiées;
- Sous réserve des exceptions prévues aux lois et encadrées par la présente politique, l'Établissement doit, avant de recueillir des RP-RS, obtenir le consentement libre et éclairé de la personne concernée par ceux-ci ou de son représentant;
- Le droit d'un usager de recevoir des services de santé et des services sociaux ne peut être compromis par sa décision de ne pas consentir à l'utilisation ou à la communication d'un RS le concernant ou par sa volonté d'en restreindre ou d'en refuser l'accès;
- Toute personne a droit au respect de sa vie privée, de même qu'au respect du secret professionnel;
- L'Établissement doit faire preuve de transparence envers les personnes concernées et les usagers auprès de qui sont recueillis des RP-RS. La transparence est essentielle à la protection de la vie privée de la personne concernée ou de l'utilisateur qui doit recevoir une information claire

et simple lui permettant de savoir de quelle façon et à quelles fins ses RP-RS seront utilisés et circuleront afin qu'il puisse exercer un contrôle et faire valoir ses droits en toute connaissance de cause;

- Les RP-RS détenus par l'Établissement sont confidentiels;
- L'Établissement est responsable d'assurer la protection des RP-RS afin de garantir leur confidentialité et cette responsabilité est partagée par l'ensemble des personnes visées par la présente politique;
- Les personnes visées par la politique doivent respecter les restrictions quant à l'accès aux RP-RS, prendre les mesures de sécurité propres à assurer la protection de ces renseignements et s'assurer d'appliquer l'ensemble des procédures, des directives et des consignes applicables à l'accès, à l'utilisation, à la communication, à la destruction et à l'anonymisation des RP-RS, le cas échéant;
- L'Établissement doit veiller à ce que les RP-RS qu'il détient soient à jour, exacts et complets pour servir aux fins pour lesquelles ils ont été recueillis. L'Établissement doit également veiller à ce que ces RP-RS soient détruits au terme de la durée de conservation applicable;
- L'Établissement doit s'assurer que la communication des RP-RS qu'il recueille s'effectue de manière structurée et conforme aux dispositions des différentes lois applicables.

8 CAI-PRPRS

8.1 GOUVERNANCE DU COMITÉ

Le comité relève de la présidente-directrice générale.

8.2 COMPOSITION

Le comité se compose de la Responsable de la protection des RP-RS et de toute autre personne dont l'expertise est requise, incluant, notamment :

- Conseillère(s)-cadre(s) à la protection des RP-RS;
- Responsable substitut de l'accès aux documents administratifs;
- Conseillère-cadre à la sécurité des ressources informationnelles régionales;
- Responsable de l'accès aux documents et de la protection des RS pour les dossiers usagers et pour les informations cliniques (DSM);
- Responsable de la gestion documentaire;
- Directrice de la qualité, évaluation, performance, éthique et Lean;
- Coordinatrice des ressources humaines, volet relations de travail et relations avec les employés et responsable de la protection des RP pour les dossiers des employés.

Le comité peut inviter des représentants de toutes autres directions de l'Établissement ou du CMDP, lorsque jugé requis.

8.3 SÉANCES

Le comité se réunit un minimum de 10 séances par an.

8.4 RAPPORT

Le comité soumet un rapport à la présidente-directrice générale le 31 mars de chaque année.

8.5 SOUS-COMITÉS

Afin d'assurer une gouvernance rigoureuse, le CAI-PRPRS a procédé à la création de plusieurs sous-comités notamment :

- Comité d'ÉFVP – Volet technologiques, ententes, communications et sondages;
- Comité d'ÉFVP – Volet recherche;
- Comité des incidents de confidentialité;
- Comité d'arrimage Affaires juridiques – Protection des RP-RS.

Pour plus d'informations, veuillez consulter la *Structure des comités organisationnels – Protection des RP-RS* ([Annexe 1](#)).

9 CONSENTEMENT

Sous réserve des exceptions prévues à la présente politique et aux lois applicables, l'Établissement obtient le consentement des personnes concernées et des usagers avant de procéder à la collecte, l'utilisation ou la communication d'un RP-RS. Un consentement peut être donné de façon écrite ou verbale, et doit, pour être valide, répondre aux critères suivants :

1. Être manifeste : le consentement doit être évident, certain et indiscutable et il ne doit laisser aucun doute quant à la volonté qui y est exprimée. Afin de s'assurer d'obtenir un consentement manifeste, toute demande de consentement faite par écrit est présentée distinctement de toute autre information présentée à la personne concernée ou à l'utilisateur.
2. Être libre : le consentement doit être donné sans contrainte. Ce critère ne serait pas satisfait si, par exemple, le consentement résultait d'une pression exercée sur la personne concernée ou l'utilisateur.
3. Être éclairé : le libellé de l'action requérant le consentement doit être précis et rigoureux et permettre à la personne concernée ou à l'utilisateur de donner son consentement en toute connaissance de cause.
4. Être donné à des fins spécifiques : le consentement doit être demandé pour chacune de ces fins. Il ne peut donc pas être général ni englober d'autres fins. Cependant, en matière de recherche, le consentement peut viser des thématiques de recherche, des catégories d'activités de recherche ou des catégories de chercheurs. La personne concernée ou l'utilisateur doit être en mesure de comprendre et de choisir les fins pour lesquelles elle donne ou non son consentement, par exemple en cochant des cases dans un formulaire électronique.
5. Être demandé en termes simples et clairs : Le consentement doit être obtenu de manière compréhensible. Cela signifie que les informations fournies doivent être formulées dans un langage simple, sans jargon technique ou ambigu. Si les explications sont trop complexes ou obscures, la personne peut ne pas saisir pleinement ce à quoi elle consent.
6. Avoir une durée : le consentement ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé, sous réserve des périodes minimales requises par les lois applicables. Ce consentement s'évalue donc au cas par cas. Cette durée peut être un nombre de jours, de mois ou d'années, ou alors faire référence à un événement déterminé ou à une situation précise.
7. Être donné par une personne apte à consentir : Un consentement libre et éclairé doit être

obtenu d'une personne apte, sauf exceptions prévues par les lois applicables. En cas d'inaptitude, le consentement peut être donné par le mandataire ou le tuteur légal de l'utilisateur. En ce qui concerne le mineur de moins de 14 ans, le consentement doit être donné par le titulaire de l'autorité parentale ou le tuteur.

Conformément aux lois applicables, l'Établissement obtient le consentement exprès de la personne concernée ou de l'utilisateur, lorsque requis. La manifestation du consentement est dite « expresse » ou « explicite » lorsque la personne démontre sa volonté d'une manière apparente, sous forme verbale ou écrite, notamment quand elle appose sa signature sur un document ou qu'elle effectue une déclaration en public ou devant un témoin. Le consentement exprès exige un acte positif de la personne concernée ou de l'utilisateur, soit une action volontaire, comme le fait de remplir un formulaire, de répondre par l'affirmative à une question ou de cocher une case.

L'Établissement conserve la preuve de tout consentement qu'il reçoit. Lorsque le consentement est donné verbalement, celui-ci est consigné au dossier de la personne concernée ou de l'utilisateur.

Pour les éléments spécifiques relatifs au consentement aux soins, veuillez consulter la *Politique sur le consentement aux soins – DSP-002* ([Annexe 2](#)) de l'Établissement.

10 COLLECTE ET CONSERVATION DES RP-RS

10.1 PRINCIPES GÉNÉRAUX

L'Établissement recueille uniquement les RP-RS nécessaires à la réalisation de ses différentes missions. La collecte de RP-RS s'effectue avec transparence. L'information transmise à l'utilisateur ou à la personne concernée doit lui permettre de savoir comment ses RP-RS seront utilisés et circuleront afin qu'il puisse exercer un contrôle à ce sujet ou faire valoir ses droits en toute connaissance de cause.

10.2 NÉCESSITÉ DE LA COLLECTE

La collecte doit s'avérer nécessaire avant même d'obtenir le consentement valide des personnes concernées et des usagers et l'évaluation de la nécessité de recueillir des RP-RS doit prédominer en toute circonstance. La nécessité s'évalue en fonction de la finalité de la collecte et de sa proportionnalité. Une collecte sera nécessaire si les conditions suivantes sont toutes réunies :

1. L'objectif poursuivi est légitime, important et réel : Il est crucial que l'objectif pour lequel le consentement est demandé soit justifié et significatif. Cela signifie que l'intention derrière la demande doit être honnête et respectueuse des droits et des besoins de la personne concernée ou de l'utilisateur.
2. L'atteinte à la vie privée est proportionnelle à cet objectif (la collecte des RP-RS est rationnellement liée aux objectifs) : Cela signifie que la portée de l'atteinte à la vie privée doit être limitée et justifiée par la nécessité d'atteindre l'objectif visé. Une collecte excessive ou intrusive de RP-RS peut nuire à la confiance de la personne concernée ou de l'utilisateur et soulever des préoccupations éthiques. Ainsi, il est important de s'assurer que chaque RP-RS collecté a un lien clair et rationnel avec les objectifs, garantissant ainsi une approche équilibrée et respectueuse des droits individuels.
3. L'atteinte au droit à la vie privée est minimisée (il n'existe pas d'autres moyens d'atteindre les mêmes objectifs d'une façon qui porte le moins atteinte à la vie privée) : Il est primordial que la collecte de RP-RS soit réalisée de la manière la moins intrusive

possible. Cela implique d'évaluer si d'autres méthodes ou approches pourraient atteindre les mêmes objectifs sans compromettre la vie privée des individus. En démontrant qu'il n'existe pas d'autres moyens moins intrusifs, on assure une approche respectueuse et éthique envers la confidentialité.

4. La collecte, l'utilisation ou la communication du RP-RS est nettement plus utile à l'Établissement que préjudiciable à la personne concernée ou à l'utilisateur : Une approche équilibrée doit être adoptée, garantissant que la protection des droits des personnes concernées et des usagers est une priorité tout en visant des résultats positifs pour l'Établissement.

10.3 INFORMATIONS À FOURNIR PRÉALABLEMENT À UNE COLLECTE D'UN RP-RS

10.3.1 Collecte d'un RS

Toute personne visée par la présente politique qui recueille un RS auprès d'un usager doit, lors de sa collecte et par la suite, sur demande, l'informer, en termes simples et clairs, des éléments suivants :

1. Du fait que ce RS est recueilli pour et au nom de l'Établissement;
2. Des fins pour lesquelles ce RS est recueilli (sauf exception prévue à la LRSSS);
3. Des moyens par lesquels ce RS est recueilli;
4. De son droit d'avoir accès à ce RS et de le faire rectifier;
5. De la possibilité de restreindre ou de refuser l'accès à ce RS ainsi que des modalités selon lesquelles il peut manifester sa volonté à cet effet;
6. De la durée de conservation de ce RS.

La personne visée par la politique n'est pas tenue d'informer l'utilisateur des éléments 1 à 6 si ceux-ci ont déjà été mentionnés durant le même épisode de soins.

Tout usager qui fournit un RS le concernant conformément à la présente section consent à son utilisation aux fins visées.

L'Établissement s'assure du respect de ce principe à travers la mise en place de processus de travail qui s'y conforment.

10.3.2 Collecte d'un RP

Toute personne visée par la présente politique qui recueille un RP auprès de toute autre personne qu'un usager doit, lors de sa collecte et par la suite, sur demande, l'informer, en termes simples et clairs, des éléments suivants:

1. Du fait que ce RP est recueilli pour et au nom de l'Établissement;
2. Des fins pour lesquelles ce RP est recueilli;
3. Des moyens par lesquels ce RP est recueilli;
4. Du caractère obligatoire ou facultatif de la demande;
5. Des conséquences d'un refus de répondre à la demande ou, si cela s'applique, d'un retrait de son consentement à la communication ou à l'utilisation du RP;
6. De son droit d'avoir accès à ce RP et de le faire rectifier;
7. Du nom du tiers ou des catégories de tiers à qui il est nécessaire de communiquer le RP pour atteindre les objectifs justifiant la collecte;
8. De la possibilité que le RP soit communiqué à l'extérieur du Québec, le cas échéant.

Lorsque des RP sont recueillis auprès d'un tiers, et non directement auprès de la personne concernée, ce tiers doit être informé des éléments suivants :

1. Du fait que ce RP est recueilli pour et au nom de l'Établissement;
2. Des conséquences d'un refus de répondre à la demande ou, si cela s'applique, d'un retrait de son consentement à la communication ou à l'utilisation du RP;
3. Des droits d'accès et de rectification prévus à la Loi sur l'accès.

Toute personne concernée qui fournit ses RP conformément à la présente section consent à leur utilisation aux fins pour lesquelles ils ont été recueillis. De même, elle consent à leur communication à des tiers aux fins pour lesquelles ils ont été recueillis, à condition que lors de la collecte, la personne concernée ait été informée du nom du tiers à qui il est nécessaire de les communiquer.

L'Établissement s'assure du respect de ce principe à travers la mise en place des processus de travail qui s'y conforment.

10.3.3 Collecte d'un RP dans le cadre d'une collaboration avec un autre organisme public

L'Établissement peut recueillir un RP si cela est nécessaire à l'exercice des attributions ou à la mise en œuvre d'un programme d'un autre organisme public avec lequel il collabore pour la prestation de services ou pour la réalisation d'une mission commune.

Cette collecte de RP est conditionnelle à ce qu'une ÉFVP soit réalisée.

De plus, cette collecte doit être précédée d'une entente écrite qui doit être transmise à la CAI. L'entente entre en vigueur 30 jours après sa réception par la CAI.

Cette entente contient les éléments suivants :

1. L'identification des deux organismes publics : celui par lequel la collecte est faite et celui pour lequel la collecte est effectuée;
2. Les fins auxquelles le RP est recueilli;
3. La nature ou le type du RP recueilli dont notamment une liste de l'ensemble des RP qui seront recueillis et communiqués à l'autre organisme public;
4. Les moyens par lesquels le RP est communiqué et recueilli;
5. Les mesures propres à assurer la protection du RP;
6. La périodicité de la collecte incluant la fréquence de la collecte ainsi que la fréquence de la communication;
7. La durée de l'entente.

L'Établissement s'assure du respect de ce principe à travers des processus de travail qui s'y conforment.

10.4 INFORMATIONS ADDITIONNELLES À FOURNIR PRÉALABLEMENT À UNE COLLECTE D'UN RP-RS À L'AIDE DE CERTAINES TECHNOLOGIES

En plus des informations à fournir préalablement à toute collecte de RP-RS, l'Établissement fournit des informations additionnelles aux personnes concernées et aux usagers si les RP-RS sont recueillis en utilisant une technologie comprenant des fonctions permettant :

1. D'identifier ces personnes;
2. De les localiser;

3. D'effectuer un profilage à leur sujet.

Dans un tel cas, les personnes concernées et les usagers sont informés de l'utilisation de cette technologie et des moyens offerts pour activer les fonctions d'identification, de localisation ou de profilage. Ces fonctions ne peuvent pas être activées par défaut et la personne concernée ou l'utilisateur doit pouvoir le faire elle-même, volontairement.

10.5 CONSERVATION DES RP-RS

L'Établissement ne conserve pas de RP-RS qu'il détient au-delà de la durée nécessaire à la réalisation des fins pour lesquelles il l'a recueilli ou utilisé, sous réserve des délais prévus par les lois applicables. En ce sens, l'Établissement s'est doté d'un *Calendrier de conservation des documents* ([Annexe 3](#)) conformément aux lois applicables. À noter qu'à compter de la fusion de l'Établissement dans Santé Québec au 1^{er} décembre 2024, la référence à ce calendrier de conservation sera remplacée par celui de Santé Québec.

Les RP sont conservés conformément à la *Politique de gestion intégrée des documents administratifs* ([Annexe 4](#)) et à la *Procédure de gestion des documents semi-actifs sous format papier* ([Annexe 5](#)).

Les RS sont conservés conformément à la *Politique d'accès, de gestion, de conservation des dossiers des usagers* ([Annexe 6](#)).

Les RP-RS conservés sont à jour, exacts et complets.

11 RS DES USAGERS DE L'ÉTABLISSEMENT: ACCÈS, UTILISATION ET COMMUNICATION

Dans le cadre de ses différentes missions, dont celle d'offrir aux usagers l'ensemble des services sociaux et des soins de santé, il est nécessaire pour l'Établissement de collecter, utiliser ou autrement traiter les RS des usagers. Dans l'esprit de la LRSSS, qui a comme ambition de simplifier la circulation des RS et d'optimiser leur utilisation et leur communication afin d'améliorer la qualité des services offerts à la population, la présente section vise à encadrer cette circulation, permettant d'atteindre l'objectif tout en s'assurant de la protection adéquate des RS.

En ce sens, même si l'accessibilité aux RS se verra élargie, chaque personne qui consultera le dossier des usagers et/ou qui aura accès aux RS devra le faire uniquement si les critères détaillés dans la présente politique sont rencontrés, **en s'attardant particulièrement à la nécessité de cet accès ou de cette utilisation.**

Tout RS des usagers est confidentiel, et sous réserve du consentement exprès de l'utilisateur, ne peut être utilisé ou communiqué que conformément à la présente section.

11.1 CATÉGORIES DE PERSONNES POUVANT UTILISER LES RS DANS L'EXERCICE DE LEURS FONCTIONS

11.1.1 Catégorisation et types d'accès établis par l'Établissement

Les catégories de personnes pouvant avoir accès aux RS sont déterminées par l'Établissement. Cette catégorisation doit assurer la prestation de services de santé et de services sociaux adéquats, continus et sécuritaires, le tout dans le respect du droit à la vie privée des usagers.

La catégorisation des personnes doit prévoir le type d'accès aux RS auxquels ces personnes ont droit. Suivant le processus de catégorisation, l'Établissement a établi une liste des catégories de personnes pouvant utiliser les RS dans l'exercice de leurs fonctions, laquelle se trouve au *Cadre de gestion de l'accès* ([Annexe 7](#)).

Cette catégorisation est mise à jour par l'Établissement, au moins une fois l'an, et en fonction de l'évolution des services de santé et des services sociaux qui sont prodigués, de même qu'en fonction de l'évolution des actifs informationnels utilisés par l'Établissement. Par conséquent, et sous réserve de l'approbation de la Responsable de la protection des RP-RS, il sera possible pour l'Établissement de donner accès à une personne ne faisant pas partie des catégories établies par le *Cadre de gestion de l'accès* ([Annexe 7](#)), mais qui aurait dû l'être, afin de s'assurer que la prestation des services à l'utilisateur ne soit en aucun temps compromise.

11.1.2 Catégorisation et types d'accès établis par le ministre

Dans la mesure où un règlement du gouvernement est établi afin de définir certaines catégories de personnes pouvant avoir accès aux RS ou de définir des profils d'accès types par catégorie de personnes, cette catégorisation aura préséance sur la catégorisation de l'Établissement.

De plus, dans la mesure où un règlement du gouvernement est établi afin de déterminer les catégories de RS qui, en raison du fait que le risque de préjudice qu'entraînerait leur divulgation serait nettement supérieur aux bénéfices escomptés pour l'utilisateur, l'Établissement mettra en place des restrictions d'accès conformes aux conditions déterminées par ce règlement.

11.1.3 RS obtenus en application de la *Loi sur la protection de la jeunesse*

La catégorisation des personnes prévoit que les RS obtenus en application de la *Loi sur la protection de la jeunesse* ne peuvent être accessibles qu'aux personnes agissant dans le cadre de l'application de cette loi.

Malgré l'alinéa précédent, ces RS peuvent toutefois être accessibles à certaines personnes lorsque le directeur de la protection de la jeunesse de l'Établissement juge que cet accès est dans l'intérêt de l'enfant.

11.1.4 RS obtenus en application de la *Loi sur la santé publique*

La catégorisation des personnes prévoit que les RS obtenus en application de la *Loi sur la santé publique* et visant les éléments suivants ne peuvent être accessibles qu'avec l'autorisation du directeur de santé publique de l'Établissement :

1. Les intoxications, les infections et les maladies à déclaration obligatoire;
2. Le traitement obligatoire et les mesures de prophylaxie à respecter pour certaines maladies ou infections contagieuses;
3. Les enquêtes épidémiologiques et les autres pouvoirs des autorités de santé publique et du gouvernement en cas de menace à la santé de la population;
4. Les manifestations cliniques inhabituelles temporellement associées à une vaccination.

11.2 RESTRICTION D'ACCÈS PAR L'USAGER

11.2.1 Restriction d'accès à un intervenant ou une catégorie d'intervenants

L'utilisateur peut déterminer qu'un intervenant ou une catégorie d'intervenants ne puisse avoir accès à un ou plusieurs RS le concernant. Pour faire une demande de droit de restriction d'accès aux RS, l'utilisateur doit faire sa demande par écrit, par courriel ou par la poste aux coordonnées suivantes :

Responsable de l'accès aux documents et de la protection des renseignements de santé et de services sociaux pour les dossiers usagers et pour les informations cliniques:

Cheffe de service des archives

Direction des services multidisciplinaires

3120, boulevard Taschereau

Greenfield Park (Québec) J4V 2H1

HCLM: archivesmedicales.hclm.ci:sssmc16@ssss.gouv.qc.ca

HHR: corr.hrr.ci:sssmc16@ssss.gouv.qc.ca

Autres sites :

<https://www.santemonteregie.qc.ca/services/archives#installation-33>

Cette demande doit inclure :

1. Les coordonnées de l'utilisateur ou les coordonnées de la personne titulaire de l'autorité parentale, du tuteur, de la tutrice ou de la personne mandataire, le cas échéant;
2. La date de la demande de restriction;
3. Le nom de l'intervenant ou de la catégorie d'intervenants dont l'utilisateur veut restreindre l'accès aux RS;
4. Une description des RS visés par la restriction;
5. La signature de l'utilisateur.

L'Établissement communiquera avec l'utilisateur afin de l'informer des modalités et des conséquences possibles que la restriction de RS peut entraîner dans son dossier.

11.2.2 Exceptions à la restriction d'accès

La restriction de l'accès peut être levée dans les cas suivants :

1. Lorsqu'il y a risque de mettre en péril la vie ou l'intégrité de l'utilisateur et qu'il est impossible d'obtenir à temps son consentement pour lever la restriction d'accès;
2. Lorsque la communication des RS est exigée par la loi.

11.2.3 Autres types de restriction d'accès

L'utilisateur peut également restreindre l'accès à ses RS aux personnes suivantes :

1. Son conjoint ou un proche parent, si l'accès envisagé s'inscrit dans un processus de deuil;

2. Son conjoint, son ascendant direct ou son descendant direct, s'il s'agit d'un RS relatif à la cause de son décès;
3. Un chercheur, si l'accès envisagé est à des fins de sollicitation en vue de sa participation à un projet de recherche;
4. Un chercheur qui n'est pas lié à un établissement public ou à toute autre catégorie prévue en annexe de la LRSSS.

Pour ce faire, l'utilisateur doit adresser sa demande par écrit aux coordonnées mentionnées au point 11.2.1. Cette demande doit contenir :

1. Les coordonnées de l'utilisateur ou les coordonnées de la personne titulaire de l'autorité parentale, du tuteur, de la tutrice ou de la personne mandataire, le cas échéant;
2. La date de la demande de restriction;
3. Le nom de la ou des personnes mentionnées aux points 1 à 3 précédents, dont l'utilisateur veut restreindre l'accès aux RS;
4. Dans le cas d'une restriction au point 4, les RS, les thématiques de recherche ou les catégories d'activités de recherche visés par le refus;
5. La signature de l'utilisateur.

11.2.4 Modification à la restriction d'accès

L'utilisateur peut en tout temps retirer ou modifier une demande de restriction d'accès, et retirer ou modifier une restriction active. Pour ce faire, l'utilisateur doit adresser sa demande par écrit aux coordonnées mentionnées au point 11.2.1. Cette demande doit contenir :

1. Le nom et les coordonnées de l'utilisateur ou les coordonnées de la personne titulaire de l'autorité parentale, du tuteur, de la tutrice ou de la personne mandataire, le cas échéant;
2. S'il s'agit d'une modification, les RS qui doivent être modifiés par cette modification;
3. S'il s'agit d'un retrait de la restriction, cette information doit être inscrite;
4. La signature de l'utilisateur.

11.3 ACCÈS AUX RS PAR L'UTILISATEUR OU CERTAINES PERSONNES LIÉES

Toute personne qui veut demander l'accès ou la rectification d'un RS en fonction des éléments visés à cette section 11.3 doit suivre la procédure détaillée à la [section 23](#) de la présente politique.

11.3.1 L'utilisateur de 14 ans et plus

L'utilisateur a le droit, sauf exceptions prévues par la loi:

1. D'être informé de l'existence de tout RS le concernant et détenu par l'Établissement et d'y avoir accès;
2. D'être informé du nom de toute personne ou de tout groupement qui a accédé, utilisé ou reçu communication à un RS détenu par l'Établissement le concernant;
3. D'être informé de la date et de l'heure de cet accès, utilisation ou communication;

4. De demander la rectification d'un RS détenu par l'Établissement et le concernant s'il est inexact, incomplet ou équivoque ou s'il a été recueilli ou est conservé en contravention à la loi.

Toutefois, cet accès pourrait lui être refusé dans les cas suivants :

1. Si, de l'avis d'un intervenant professionnel, il en découlerait vraisemblablement d'un préjudice grave pour sa santé;
2. Si le RS de l'utilisateur provient d'un tiers, autre qu'un intervenant dans l'exercice de ses fonctions, lorsque cette divulgation permettrait d'identifier ce tiers, à moins du consentement écrit de ce dernier.

Dans le cas du point 1, si le préjudice grave pour la santé de l'utilisateur est temporaire, l'utilisateur sera informé du moment où son droit d'accès pourra être exercé.

Le mineur de moins de 14 ans n'a pas le droit d'être informé de l'existence d'un RS le concernant et détenu par l'Établissement ni d'y avoir accès, sauf par l'intermédiaire de son avocat dans le cadre d'une procédure judiciaire.

11.3.2 Personnes liées à un majeur inapte

À condition que:

1. L'évaluation conclut à l'inaptitude de l'utilisateur à prendre soin de lui-même et à administrer ses biens ou à accomplir un acte déterminé;
2. La personne liée à l'utilisateur majeur inapte atteste sous serment qu'elle entend demander, à l'égard de ce dernier, l'ouverture ou à la révision d'une tutelle, l'homologation d'un mandat de protection ou la représentation temporaire. (La personne liée peut consulter le *Modèle d'attestation sous serment* ([Annexe 8](#))).

La personne liée à l'utilisateur majeur inapte a le droit :

1. D'être informée de l'existence d'un RS contenu dans les rapports d'évaluation médicale et psychosociale de l'utilisateur, détenus par l'Établissement;
2. D'avoir accès à un tel renseignement.

Le tuteur ou le mandataire en règle d'un majeur inapte a le droit :

1. D'être informé de l'existence de tout RS détenu par l'Établissement concernant ce majeur et d'y avoir accès;
2. De demander la rectification de tout RS détenu par l'Établissement concernant un majeur inapte s'il est inexact, incomplet ou équivoque ou s'il a été recueilli ou est conservé en contravention à la loi.

11.3.3 Personnes liées à un défunt

Une personne liée à un défunt a le droit :

1. D'être informée de l'existence d'un RS détenu par l'Établissement concernant le défunt et d'y avoir accès, à condition que cela soit nécessaire à l'exercice de ses droits et de ses obligations à ce titre (par exemple, à titre de liquidateur de la succession);
2. De demander la rectification d'un RS détenu par l'Établissement concernant le défunt s'il est inexact, incomplet ou équivoque ou s'il a été recueilli ou est

conservé en contravention à la loi, à condition que cette rectification mette en cause ses intérêts ou ses droits à titre d'héritier, de légataire particulier, de liquidateur de la succession ou de bénéficiaire.

11.3.4 Conjoint ou proche parent d'une personne décédée

Le conjoint ou un proche parent d'une personne décédée a le droit d'être informé de l'existence d'un RS concernant la personne décédée et d'y avoir accès lorsque ce renseignement est susceptible de l'aider dans son processus de deuil, à moins que la personne décédée n'ait refusé l'accès à ce RS conformément aux dispositions légales applicables et à la [section 11.2.3](#).

Le conjoint, l'ascendant direct ou le descendant direct d'une personne décédée a le droit d'être informé de l'existence d'un RS relatif à la cause du décès détenu par l'Établissement et d'y avoir accès, à moins que la personne décédée n'ait refusé l'accès à ce renseignement conformément aux dispositions légales applicables et à la [section 11.2.3](#).

Les personnes liées génétiquement à une personne décédée ont le droit d'être informées de l'existence d'un RS détenu par l'Établissement concernant la personne décédée et d'y avoir accès, à condition que cela soit nécessaire à la vérification de l'existence d'une maladie génétique ou d'une maladie à caractère familial. Ce droit s'exerce même si la personne décédée avait refusé l'accès à un RS relatif à la cause de son décès conformément aux dispositions légales applicables et à la [section 11.2.3](#).

11.3.5 Titulaire de l'autorité parentale ou tuteur d'un mineur

Dans le cas d'un mineur de moins de 14 ans, vivant ou décédé, sauf exceptions prévues par la loi, le titulaire de l'autorité parentale ou le tuteur a le droit :

1. D'être informé de l'existence de tout RS détenu par l'Établissement concernant ce mineur et d'y avoir accès;
2. De demander la rectification de tout RS détenu par l'Établissement concernant ce mineur s'il est inexact, incomplet ou équivoque ou s'il a été recueilli ou est conservé en contravention à la loi.

Toutefois, il ne sera pas possible pour le titulaire de l'autorité parentale ou le tuteur d'avoir accès à ces RS:

1. Si un directeur de la protection de la jeunesse détermine qu'il en découlerait vraisemblablement un préjudice pour la santé ou la sécurité du mineur dans l'une des situations prévues à la LRSSS et à la *Loi sur la protection de la jeunesse*;
2. Si le mineur de moins de 14 ans est décédé et que le RS est de nature psychosociale.

Dans le cas d'un mineur de 14 ans et plus, si (i) après avoir consulté le mineur; et (ii) après avoir consulté le directeur de la protection de la jeunesse, le cas échéant, l'Établissement est d'avis qu'il ne découlerait vraisemblablement pas de préjudice pour la santé et la sécurité de celui-ci, le titulaire de l'autorité parentale ou le tuteur a le droit :

1. D'être informé de l'existence de tout RS détenu par l'Établissement concernant

- ce mineur et d'y avoir accès, sauf certains RS visés à la *Loi sur la protection de la jeunesse*;
2. De demander la rectification de tout RS détenu par l'Établissement concernant ce mineur s'il est inexact, incomplet ou équivoque ou s'il a été recueilli ou est conservé en contravention à la loi.

11.4 ACCÈS AUX RS PAR LES INTERVENANTS EXTERNES À L'ÉTABLISSEMENT

Afin de clarifier les procédures en place, l'Établissement a élaboré un schéma illustrant les différentes situations d'accès et d'utilisation des RS de l'Établissement. Veuillez consulter le *Schéma d'accès aux RS par les intervenants internes et externes* ([Annexe 9](#)).

Prendre note que dès la fusion de l'Établissement dans Santé Québec au 1^{er} décembre 2024, les autres établissements publics de santé du Québec ne seront plus considérés externes à l'Établissement. Les sections [11.5](#) et [11.6](#) seront alors applicables à ceux-ci.

11.4.1 Intervenant professionnel

Un intervenant professionnel externe à l'Établissement peut demander l'accès aux RS détenus par l'Établissement :

1. S'il lui est nécessaire pour offrir à l'utilisateur des services de santé ou des services sociaux;
- ou
2. Si l'accès ou l'utilisation est requise à des fins d'enseignement, de formation et de pratiques réflexive (par exemple, pour une évaluation de la qualité de l'acte médical).

Cet accès pourrait toutefois lui être refusé si des restrictions d'accès ont été demandées par l'utilisateur, sous réserve des conditions établies aux sections [11.1.3](#), [11.1.4](#) et [11.2](#).

11.4.2 Intervenant non-professionnel

Un intervenant non-professionnel externe à l'Établissement peut demander l'accès aux RS détenus par l'Établissement:

1. S'il lui est nécessaire pour offrir à l'utilisateur des services de santé ou des services sociaux;
- ou
2. S'il lui est nécessaire pour fournir du soutien technique ou administratif à un autre intervenant qui offre des services de santé ou de services sociaux;
- et**
3. S'il a obtenu une autorisation d'accès de l'organisation pour lequel il exerce.

Cet accès pourrait toutefois lui être refusé si des restrictions d'accès ont été demandées par l'utilisateur, sous réserve des conditions établies aux sections [11.1.3](#), [11.1.4](#) et [11.2](#).

11.5 UTILISATION, AU SEIN DE L'ÉTABLISSEMENT, DES RS DÉTENUS PAR L'ÉTABLISSEMENT

Afin de clarifier les procédures en place, l'Établissement a élaboré un schéma illustrant les différentes situations d'accès et d'utilisation des RS au sein de l'Établissement : *Schéma d'accès aux RS par les intervenants internes et externes* ([Annexe 9](#)).

Prendre note que dès la fusion de l'Établissement dans Santé Québec au 1^{er} décembre 2024, les autres établissements publics de santé du Québec seront considérés comme étant internes à l'Établissement. Les sections 11.5 et 11.6 seront alors applicables à ceux-ci.

11.5.1 Intervenant professionnel

Un intervenant professionnel qui exerce au sein de l'Établissement peut utiliser les RS détenus par l'Établissement :

1. S'il fait partie d'une catégorie de personnes identifiées au *Cadre de gestion de l'accès* ([Annexe 7](#)) ou à un règlement;
et
2. S'il a complété une formation sur la protection des RP-RS;

et s'il répond à l'un des critères suivants:

3. S'il lui est nécessaire pour offrir à l'utilisateur des services de santé ou des services sociaux;
ou
4. Si l'accès ou l'utilisation est requise à des fins d'enseignement, de formation et de pratiques réflexive (par exemple, pour une évaluation de la qualité de l'acte médical);
ou
5. Si l'utilisation est nécessaire aux fins pour lesquelles les RS ont été recueillis;
ou
6. L'accès est nécessaire à l'exercice des fonctions de l'Établissement relatives à l'organisation ou à l'évaluation des services de santé et services sociaux (ex : audits internes).
ou
7. Si l'utilisation est nécessaire à d'autres fins si l'une des conditions suivantes est remplie :
 - a. Les fins sont compatibles avec celles pour lesquelles il a été recueilli (lien pertinent et direct) : par exemple, le lien entre les antécédents médicaux et le suivi de l'utilisateur est direct, comme les antécédents peuvent influencer le traitement et les soins de l'utilisateur; ou
 - b. Manifestement au bénéfice de l'utilisateur : l'utilisation des RS peut aller au-delà des finalités initiales, tant que cela sert le bien-être et la santé de l'utilisateur; ou
 - c. Nécessaire à l'application d'une loi au Québec (que cette utilisation soit ou non prévue expressément par la loi) : par exemple, le signalement d'un potentiel abus aux autorités compétentes.

Malgré les points ci-dessus, il se pourrait que l'accès ou l'utilisation ne soit pas possible pour l'intervenant professionnel interne si des restrictions d'accès ont été demandées par l'utilisateur, sous réserve des conditions établies aux sections [11.1.3](#), [11.1.4](#) et [11.2](#).

11.5.2 Intervenant non-professionnel

Un intervenant non-professionnel qui exerce au sein de l'Établissement pourra utiliser les RS détenus par l'Établissement :

1. S'il fait partie d'une catégorie de personnes identifiées au *Cadre de gestion de l'accès* ([Annexe 7](#)) ou à un règlement;

et

2. S'il obtient une autorisation d'accès de la personne déléguée selon le processus de délégation prévu au *Cadre de gestion de l'accès* ([Annexe 7](#)) après avoir rempli toutes les conditions suivantes:
 - a. Être un membre du personnel, un étudiant ou un stagiaire sous supervision d'un professionnel œuvrant dans un établissement d'enseignement collégial ou universitaire, un bénévole exerçant les activités visées aux articles 39.7 et 39.8 du *Code des professions*, ou un salarié d'une agence de placement, une personne qui est de la main-d'œuvre indépendante visée à l'article 338.2 de la *Loi sur les services santé et les services sociaux*; et
 - b. Avoir complété une formation sur la protection des RP-RS; et
 - c. S'engager par écrit à faire preuve de discrétion et à ne pas divulguer les RP-RS.

et s'il répond à l'un des critères suivants:

3. S'il lui est nécessaire pour offrir à l'utilisateur des services de santé ou des services sociaux;
ou
4. S'il lui est nécessaire pour fournir du soutien technique ou administratif à un autre intervenant qui offre des services de santé ou de services sociaux;
ou
5. Si l'utilisation est nécessaire aux fins pour lesquelles les RS ont été recueillis;
ou
6. L'accès est nécessaire à l'exercice des fonctions de l'Établissement relatives à l'organisation ou à l'évaluation des services de santé et services sociaux.
ou
7. Si l'utilisation est nécessaire à d'autres fins si l'une des conditions suivantes est remplie :
 - a. Les fins sont compatibles avec celles pour lesquelles il a été recueilli (lien pertinent et direct); ou
 - b. Manifestement au bénéfice de l'utilisateur; ou
 - c. Nécessaire à l'application d'une loi au Québec (que cette utilisation soit ou non prévue expressément par la loi).

Malgré les points ci-dessus, il se pourrait que l'accès ou l'utilisation ne soit pas possible pour l'intervenant non-professionnel interne si des restrictions d'accès ont été demandées par l'utilisateur, sous réserve des conditions établies aux sections [11.1.3](#), [11.1.4](#) et [11.2](#).

11.5.3 Tout autre membre du personnel

Tout autre membre du personnel de l'Établissement, qu'il soit professionnel ou non-professionnel, et qui ne correspond pas à la définition d'intervenant peut utiliser les RS :

1. S'il fait partie d'une catégorie de personnes identifiées au *Cadre de gestion de l'accès* ([Annexe 7](#)) ou à un règlement;
et
2. S'il a complété une formation sur la protection des RP-RS.

et s'il répond à l'un des critères suivants:

3. Si l'utilisation est nécessaire aux fins pour lesquelles les RS ont été recueillis;
ou
4. L'accès est nécessaire à l'exercice des fonctions de l'Établissement relatives à l'organisation ou à l'évaluation des services de santé et services sociaux;
ou
5. Si l'utilisation est nécessaire à d'autres fins si l'une des conditions suivantes est remplie :
 - a. Les fins sont compatibles avec celles pour lesquelles il a été recueilli (lien pertinent et direct); ou
 - b. Manifestement au bénéfice de l'utilisateur; ou
 - c. Nécessaire à l'application d'une loi au Québec (que cette utilisation soit ou non prévue expressément par la loi).

Malgré les points ci-dessus, il se pourrait que l'accès ou l'utilisation ne soit pas possible pour ce membre du personnel si des restrictions d'accès ont été demandées par l'utilisateur, sous réserve des conditions établies aux sections [11.1.3](#), [11.1.4](#) et [11.2](#).

11.6 UTILISATION ET COMMUNICATION DE RP-RS À DES FINS DE RECHERCHE

11.6.1 Utilisation des RP-RS avec consentement

La section 11.6 n'est pas applicable à une recherche dont il est possible d'obtenir le consentement du participant (par exemple, les essais cliniques). Veuillez consulter la [section 12](#) – RP-RS concernant les participants d'une recherche.

11.6.2 Utilisation des RS sans consentement

Un chercheur lié à un établissement public ou à l'une ou l'autre des catégories en annexe de la LRSSS peut avoir accès à un RS si celui-ci est nécessaire à la réalisation d'un projet de recherche. Le chercheur doit démontrer qu'il est nécessaire pour le projet de recherche d'obtenir des RS qui permettent d'identifier l'utilisateur, plutôt que des renseignements anonymisés ou agrégés. La forme dépersonnalisée (c'est-à-dire qui ne permet pas l'identification directe de la personne concernée) doit toujours être favorisée.

Malgré le paragraphe ci-dessus, il se pourrait que l'accès ou l'utilisation ne soit pas possible pour ce chercheur si des restrictions d'accès ont été demandées par l'utilisateur conformément à la [section 11.2.3](#).

11.6.3 Demande d'autorisation et ÉFVP

Une ÉFVP doit être effectuée pour toute demande d'autorisation du chercheur à être informé de l'existence d'un RS et d'y avoir accès, sans le consentement de l'utilisateur.

L'ÉFVP doit conclure que :

1. Il est déraisonnable d'exiger l'obtention du consentement de l'utilisateur;
2. L'objectif du projet de recherche l'emporte, eu égard à l'intérêt public, sur l'impact de l'utilisation ou de la communication du RS sur la vie privée de l'utilisateur;
3. Les mesures de sécurité qui seront en place pour la réalisation du projet de recherche sont propres à assurer la protection du RS et sont conformes à la

présente politique et aux règles particulières définies par le dirigeant réseau de l'information;

4. Lorsque le projet de recherche implique la communication d'un RS à l'extérieur du Québec, l'ÉFVP doit démontrer que le RS bénéficierait d'une protection adéquate, notamment au regard des principes de protection des RP-RS généralement reconnus.

Une fois les documents reçus et l'ÉFVP favorable réalisée, l'Établissement signe avec le chercheur une *Entente de communication* ([Annexe 10](#)). Cette entente est ensuite transmise à la CAI.

Pour plus d'informations concernant le processus d'ÉFVP au sein de l'Établissement, veuillez consulter la *Procédure concernant les évaluations des facteurs relatifs à la vie privée* ([Annexe 11](#)), le *Processus organisationnel de demande d'évaluation et d'avis de protection des renseignements personnels et des renseignements de santé et de services sociaux* ([Annexe 12](#)) et le *Formulaire de demande d'autorisation à être informé de l'existence de renseignements de santé et de services sociaux nécessaires à la réalisation d'un projet de recherche et d'y avoir accès, sans le consentement des personnes concernées par ces renseignements* ([Annexe 13](#)).

11.6.4 Responsabilité du chercheur lors des projets de recherche sans consentement

Les obligations du chercheur envers les RS sont plus amplement détaillées à l'*Entente de communication* ([Annexe 10](#)). Dans l'éventualité où le chercheur s'adjoint d'un tiers pour la réalisation du projet de recherche, le chercheur doit communiquer avec le cr-info@rrsss16.gouv.qc.ca afin de mettre en place le processus applicable. Le chercheur doit s'assurer que le tiers respecte l'ensemble des obligations qui incombent au chercheur en vertu de l'entente de communication.

11.6.5 Recherche multicentrique ou impliquant l'accès aux RS détenus par plusieurs établissements

Lorsqu'un projet de recherche nécessite l'utilisation de RS dans plusieurs établissements du réseau de la santé du Québec, le chercheur dépose sa demande d'autorisation dans l'établissement auquel il est lié. La personne ayant la plus haute autorité au sein de cet établissement (ou toute personne déléguée) est celle responsable d'autoriser l'accès et la communication des RS de tous les établissements visés par la demande d'accès. Avant de faire droit à la demande, la personne ayant la plus haute autorité au sein de cet établissement doit consulter chacun des autres établissements détenteurs de RS visés par la demande, qui disposent alors de 10 jours pour présenter leurs observations.

Une entente de transfert de données ou de collaboration sera effectuée entre les établissements. Pour plus d'information concernant cette entente, veuillez communiquer avec: cr-info@rrsss16.gouv.qc.ca

11.6.6 Révocation des accès

L'Établissement peut révoquer l'autorisation qu'elle a octroyée au chercheur en vertu de la [section 11.6.3](#) dès qu'il a des raisons de croire que les normes d'éthique et d'intégrité scientifique généralement reconnues, les mesures de sécurité ou toute autre mesure prévue par l'entente ne sont pas respectées ou que la protection des RS est autrement compromise.

11.6.7 Rapport annuel

L'Établissement transmet annuellement au ministre et à la CAI un rapport qui concerne les projets de recherche pour lesquels une demande d'autorisation lui a été adressée. Ce rapport est produit par le Comité ÉFVP - Volet recherche.

11.7 COMMUNICATION DE RS À DES TIERS

11.7.1 Communication nécessaire à l'application d'une loi au Québec

L'Établissement peut communiquer un RS qu'il détient à une personne ou à un groupement dans la mesure où ce RS est nécessaire à l'application d'une loi au Québec et qu'une communication, une transmission, une divulgation ou toute autre action permettant de prendre connaissance de ce RS est prévue expressément par la loi.

11.7.2 Communication nécessaire pour prévenir un acte de violence dont un suicide

Un RS détenu par l'Établissement peut être communiqué sans le consentement de l'utilisateur en vue de protéger une personne ou un groupe de personnes identifiables lorsqu'il existe un motif raisonnable de croire qu'un risque sérieux de mort ou de blessures graves, lié notamment à une disparition ou à un acte de violence, dont une tentative de suicide, menace cette personne ou ce groupe et que la nature de la menace inspire un sentiment d'urgence.

Les RS peuvent alors être communiqués à la ou aux personnes exposées à ce risque, à leur représentant ou à toute personne susceptible de leur porter secours. Seuls les RS nécessaires aux fins poursuivies par la communication peuvent leur être communiqués.

Les RS peuvent être communiqués par les personnes autorisées en fonction des processus établis par la *Directive sur les conditions et les modalités de divulgation de renseignements confidentiels pour prévenir un acte de violence dont un suicide* ([Annexe 14](#)).

Toute divulgation de RS doit être rapportée à la Responsable de la protection des RP-RS et sera consignée au dossier de l'utilisateur selon les modalités établies par [l'Annexe 14](#).

11.7.3 Communication au Directeur des poursuites criminelles et pénales

L'Établissement peut communiquer un RS qu'il détient au Directeur des poursuites criminelles et pénales ou à une personne ou à un groupement qui, en vertu de la loi, est chargé de prévenir, de détecter ou de réprimer le crime ou les infractions aux lois lorsque le RS est nécessaire aux fins d'une poursuite pour une infraction à une loi applicable au Québec.

11.7.4 Communication à un corps de police

L'Établissement peut communiquer un RS qu'il détient à un corps de police lorsqu'il est nécessaire à la planification ou à l'exécution d'une intervention adaptée aux caractéristiques d'une personne ou de la situation, dans l'un ou l'autre des cas suivants :

1. Le corps de police intervient, à la demande de l'Établissement, pour lui apporter de l'aide ou du soutien dans le cadre des services qu'il fournit à une personne;
2. L'Établissement et le corps de police agissent en concertation ou en partenariat dans le cadre de pratiques mixtes d'interventions psychosociales et policières.

Le RS communiqué ne peut être utilisé qu'aux fins de la planification ou de l'intervention pour laquelle il est communiqué.

11.7.5 Communication nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de services ou d'entreprise

L'Établissement peut communiquer un RS qu'il détient à un fournisseur ou un prestataire de services à qui il confie l'exercice d'un mandat ou avec qui il conclut un contrat de services, d'entreprise ou d'approvisionnement autre que celui visant la prestation de services de santé ou de services sociaux, lorsque ce RS est nécessaire à l'exercice de ce mandat ou à l'exécution de ce contrat.

Un tel mandat ou un tel contrat doit être, selon le cas, confié ou conclu par écrit et, lorsque le fournisseur ou le prestataire de services à qui il est confié ou avec qui il est conclu n'est pas un organisme au sens de la LRSSS, prévoir, sous peine de nullité, toutes les exigences prévues à la LRSSS visant la conclusion d'un tel mandat ou contrat.

Le fournisseur et le prestataire de services devra transmettre à l'Établissement, avant toute communication, un engagement de confidentialité complété par toute personne à qui le RS peut être communiqué ou qui peut l'utiliser dans l'exercice du mandat ou pour l'exécution du contrat. À ce titre, voir l'*Engagement de confidentialité dans le cadre d'un mandat ou à l'exécution d'un contrat de service, d'entreprise ou d'approvisionnement* ([Annexe 15](#)). L'engagement est collecté par la direction concernée.

Le fournisseur et le prestataire de services qui s'adjoit d'un tiers pour exercer un mandat ou pour exécuter un contrat de services ou d'entreprise doit obtenir l'autorisation préalable de l'Établissement. Le tiers est soumis aux mêmes obligations que celles qui sont imposées au fournisseur ou prestataire de services à l'exception de l'engagement de confidentialité et de l'avis de violation ou de tentative de violation

12 RP-RS CONCERNANT LES PARTICIPANTS D'UNE RECHERCHE

12.1 RECHERCHE AVEC CONSENTEMENT

L'Établissement, par le biais d'un chercheur, procède à la collecte, à l'utilisation et à la communication de RP-RS concernant des participants ayant consenti expressément à participer à la recherche menée à l'Établissement. Tout RP-RS recueilli et traité à cette fin le sera conformément aux modalités et précisions fournies au formulaire de consentement approuvé par le Comité d'éthique de la recherche de l'Établissement (« **CÉR** »), et signé par chaque participant, ainsi que les autres documents applicables, dont, le protocole de recherche approuvé par le CÉR (collectivement, les « **documents de recherche** »).

Les documents de recherche détaillent également les fins auxquelles ces RP-RS seront utilisés et les circonstances dans lesquelles les RP-RS pourront être communiqués à des tiers. Ces documents de recherche prévoient également les processus de conservation et de

destruction des RP-RS des participants. Les documents de recherche ont préséance sur la présente politique.

12.2 RECHERCHE IMPLIQUANT UNE BANQUE DE DONNÉES OU UNE BIOBANQUE

L'Établissement procède également, par le biais d'un chercheur, à la collecte, l'utilisation et la communication de RP-RS concernant des participants ayant consenti expressément à ce que leurs RP-RS soient conservés dans des banques de données ou des biobanques de recherche. Tout RP-RS sera recueilli et traité conformément aux modalités et précisions fournies au formulaire de consentement approuvé par le CÉR et signé par chaque participant à la banque de données ou à la biobanque, ainsi que les autres documents applicables, dont, notamment, le cadre de gestion applicable à chaque banque de données ou biobanque approuvé par le CÉR (collectivement, les « **documents de la banque de données/biobanque** »).

Les documents de la banque de données/biobanque détaillent les fins auxquelles ces RP-RS seront utilisés et les circonstances dans lesquelles ils pourront être communiqués à des tiers. Finalement, les documents de la banque de données/biobanque prévoient les processus de conservation et de destruction des RP-RS. Les documents de la banque de données/biobanque ont préséance sur la présente politique.

Pour plus d'informations concernant les règles en matière de recherche au sein de l'Établissement, veuillez consulter le *Cadre réglementaire sur l'organisation et les bonnes pratiques de la recherche au CISSS de la Montérégie-Centre* ([Annexe 16](#)), la *Politique sur la conduite responsable et l'intégrité scientifique en recherche* ([Annexe 17](#)), la *Procédure d'évaluation de la convenance institutionnelle de la recherche au CISSS de la Montérégie-Centre* ([Annexe 18](#)) et les MON du CISSS de la Montérégie-Centre.

13 RP DES MEMBRES DU PERSONNEL ET DES PERSONNES AFFILIÉES À L'ÉTABLISSEMENT

13.1 UTILISATION ET COMMUNICATION DES RP

Il est nécessaire pour l'Établissement de collecter divers RP des membres de son personnel afin de gérer adéquatement sa relation d'emploi avec son personnel. De même, il est nécessaire pour l'Établissement de collecter des RP auprès des personnes affiliées à l'Établissement, lui permettant ainsi de gérer le lien d'affiliation avec celles-ci. Les RP collectés sont spécifiés au calendrier de conservation. Ces RP sont colligés et autrement traités avec le consentement des membres du personnel ou des personnes affiliées, sauf dans les cas prévus à la Loi sur l'accès.

Sauf exceptions prévues par la Loi sur l'accès :

1. L'Établissement obtient le consentement du membre du personnel ou de la personne affiliée lorsqu'il collecte, utilise, divulgue ou traite autrement des RP qui ne sont pas nécessaires à la gestion de la relation d'emploi ou d'affiliation. Cela s'applique également lorsque l'Établissement souhaite utiliser ou divulguer ces RP à d'autres fins.
2. Les RP collectés pour la gestion de l'emploi ou de l'affiliation ne seront accessibles qu'aux membres du personnel de l'Établissement dont les fonctions l'exigent. Dans le cas d'un dossier de cadre, l'Établissement s'est doté d'une *Politique sur le dossier du cadre – DRHDO-AJ-012* ([Annexe 19](#)).
3. Les RP sont utilisés uniquement pour les fins pour lesquelles ils ont été recueillis, sauf lorsque:

- a. Leur utilisation est à des fins compatibles avec celles pour lesquelles ils ont été recueilli, soit lorsqu'il existe un lien pertinent et direct;
 - b. Leur utilisation est manifestement au bénéfice de la personne concernée;
 - c. Leur utilisation est nécessaire à l'application d'une loi au Québec.
4. L'Établissement peut communiquer les RP sans le consentement du membre du personnel ou de la personne affiliée dans les cas suivants :
- a. Aux prestataires de services, fournisseurs ou sous-traitants et uniquement s'ils en ont besoin pour remplir leurs obligations contractuelles envers l'Établissement. Ces tiers seront liés par des obligations de confidentialité strictes.
 - b. Si l'Établissement est légalement tenu de le faire (par exemple, auprès des autorités fiscales) ou pour protéger ses intérêts, ses biens ou ceux de ses membres du personnel ou personnes affiliées (par exemple, assurer la sécurité des personnes concernées en situations d'urgence).

De plus, l'Établissement met à la disposition de ses membres du personnel et des personnes affiliées plusieurs actifs informationnels permettant d'échanger des informations entre eux, de communiquer avec des tiers à des fins professionnelles, et d'accéder à Internet ainsi qu'aux documents de l'Établissement. L'utilisation de ces actifs doit être limitée aux fins professionnelles. En ce sens, les membres du personnel et les personnes affiliées ne peuvent pas s'attendre à ce que leurs communications personnelles effectuées via le réseau ou le matériel de l'Établissement demeurent en tout temps confidentielles.

En soumettant des RP à l'Établissement, les membres du personnel et les personnes affiliées reconnaissent avoir consenti aux pratiques de collecte, d'utilisation et de divulgation établies à la présente politique.

14 RP CONCERNANT TOUTE AUTRE PERSONNE

L'Établissement procède également à la collecte de RP des personnes qui interagissent avec lui, que ce soit via son site internet (par exemple, le dépôt d'une candidature à un emploi) ou par courriel (par exemple, pour des questions sur divers sujets). Les détails concernant les RP recueillis sont précisés au calendrier de conservation (notamment le nom, l'adresse courriel, le numéro de téléphone, l'adresse civique, etc.). Ces traitements sont effectués avec le consentement des personnes concernées ou dans les situations prévues par la Loi sur l'accès.

Sauf exception prévue par la Loi sur l'accès :

1. Les RP collectés ne seront accessibles qu'aux membres du personnel de l'Établissement dont les fonctions l'exigent.
2. L'Établissement peut divulguer les RP sans le consentement de la personne concernée dans les cas suivants :
 - a. Aux prestataires de services, fournisseurs ou sous-traitants et uniquement s'ils en ont besoin pour remplir leurs obligations contractuelles envers l'Établissement. Ces tiers seront liés par des obligations de confidentialité strictes.
 - b. Si l'Établissement est légalement tenu de le faire ou pour protéger ses intérêts, ses biens ou ceux de ses membres du personnel ou personnes affiliées (par exemple, assurer la sécurité d'une personne en situations d'urgence).

15 RP RECUEILLIS OU UTILISÉS DANS LE CADRE D'UN SONDAGE

Dans le cadre de ses activités, l'Établissement peut recueillir des RP dans le cadre de la réalisation d'un sondage impliquant des RP.

Dans le cadre de tout sondage visant des RP, l'Établissement :

1. S'assure du respect de la législation applicable en matière de protection des RP;
2. Évalue la nécessité de recourir au sondage;
3. Évalue l'aspect éthique du sondage compte tenu, notamment, de la sensibilité des RP recueillis et de la finalité de leur utilisation;
4. Évite autant que possible la saisie d'informations confidentielles, notamment en privilégiant les sondages anonymes ainsi que les choix de réponses;
5. Consulte le conseiller-cadre en sécurité de la DRIM, afin de s'assurer de la sécurité technologique de l'outil pressenti pour le sondage comportant des RP;
6. Met en place les mesures requises pour préserver la confidentialité des RP des personnes participantes au sondage.

Le Comité ÉFVP – Volet technologiques, ententes, communications et sondages est responsable de ce volet.

16 PROJET TECHNOLOGIQUE IMPLIQUANT DES RP-RS

Afin de respecter les exigences légales applicables et d'assurer la confidentialité et la sécurité des RP-RS, l'Établissement procédera à une ÉFVP de tout projet d'acquisition, de développement et de refonte d'un système d'informations ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation, la destruction ou l'anonymisation de RP-RS. La réalisation de cette évaluation devra être proportionnée à la sensibilité des RP-RS concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support.

Aux fins de l'ÉFVP, tout membre du personnel ou personne affiliée doit consulter, dès le début du projet, le CAI-PRPRS, lequel peut suggérer, à toute étape d'un projet visé :

1. La nomination d'une personne chargée de la mise en œuvre des mesures de protection des RP-RS;
2. Des mesures de protection des RP-RS dans tout document, tels un cahier des charges ou un contrat;
3. Une description des responsabilités des personnes participant au projet, en matière de protection des RP-RS;
4. La tenue d'activités de formation sur la protection des RP-RS pour les personnes participant au projet.

Afin de se conformer à ce qui précède, l'Établissement a élaboré une *Procédure concernant les évaluations des facteurs relatifs à la vie privée* ([Annexe 11](#)).

Pour plus d'informations concernant le processus d'ÉFVP au sein de l'Établissement, voir le *Processus organisationnel de demande d'évaluation et d'avis en protection des RP-RS* ([Annexe 12](#)).

17 COMMUNICATION DE RP-RS À L'EXTÉRIEUR DU QUÉBEC

L'Établissement procède à une ÉFVP avant de communiquer des RP-RS à l'extérieur du Québec ou de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de détenir, d'utiliser ou de communiquer pour son compte des RP-RS.

L'Établissement s'assure que les RP-RS transférés hors du Québec bénéficient d'une protection adéquate, notamment au regard des principes de protection des RP-RS généralement reconnus. De plus, une entente écrite entre l'Établissement et la personne ou l'organisme à l'extérieur du Québec est rédigée et tient compte des résultats de l'ÉFVP et des modalités convenues dans le but d'atténuer les risques identifiés dans le cadre de l'ÉFVP.

Afin de se conformer à ce qui précède, l'Établissement a élaboré une *Procédure concernant les évaluations des facteurs relatifs à la vie privée* ([Annexe 11](#)).

Pour plus d'informations concernant le processus d'ÉFVP au sein de l'Établissement, voir le *Processus organisationnel de demande d'évaluation et d'avis en protection des RP-RS* ([Annexe 12](#)).

18 DÉCISION FONDÉE SUR LE TRAITEMENT AUTOMATISÉ DE RP

L'Établissement veille à informer la personne concernée, au plus tard au moment où elle est informée de la décision, lorsque les RP sont utilisés dans le cadre d'une décision fondée exclusivement sur un traitement automatisé (décision prise sans aucune intervention humaine, par exemple, uniquement à l'aide d'algorithmes). De plus, sur demande, l'Établissement informera la personne concernée :

1. Des RP utilisés pour rendre la décision;
2. Des raisons et des principaux facteurs et paramètres qui ont mené à la décision;
3. De son droit de faire rectifier les RP utilisés pour rendre la décision.

La personne concernée aura alors l'occasion de présenter ses observations à l'Établissement.

19 MESURES VISANT LA PROTECTION DES RP-RS

19.1 PRINCIPES GÉNÉRAUX

L'Établissement met en place des mesures visant à protéger les RP-RS tout au long de leur cycle de vie.

En matière de sécurité technologique de l'information, des mesures de protection - incluant celles exigées par le MSSS, le dirigeant réseau de l'information et le ministre de la Cybersécurité et du Numérique - sont mises en place afin d'assurer la sécurité des infrastructures et des actifs informationnels et de réduire le risque de menaces telles que les cyberattaques, les virus informatiques ainsi que les pannes du réseau et de ces actifs. Une équipe responsable de la cybersécurité veille à la mise en place des mesures et assure la cybersurveillance, afin de sécuriser les infrastructures et les actifs informationnels contenant des RP-RS. Le Chef de la sécurité de l'information organisationnelle et la DRIM ont pour mandat d'assurer la mise en œuvre et l'application de la politique et des directives sous-jacentes applicables en matière de sécurité technologique de l'information. Pour plus d'informations, veuillez consulter la *Politique de sécurité des ressources informationnelles* ([Annexe 20](#)).

En ce qui concerne les RS contenus au dossier d'un usager, les mesures liées à leur protection sont également prévues à la *Politique d'accès, de gestion, de conservation des dossiers des usagers* ([Annexe 6](#)).

19.2 MÉCANISMES DE JOURNALISATION

19.2.1 Obligation relative à la journalisation des accès aux RP-RS détenus par l'Établissement

L'Établissement procède à la journalisation des accès aux RP-RS qu'il détient par toute personne visée par la présente politique. Cette journalisation permet de savoir quel RP-RS a fait l'objet d'un accès, a été utilisé ou a fait l'objet d'une communication, de même que permettre de savoir qui y a accédé, l'a utilisé ou l'a communiqué. L'information journalisée précise la date et l'heure de l'accès, de l'utilisation ou de la communication.

19.2.2 Obligation de journalisation des RP-RS numériques

L'Établissement s'assure également que les actifs informationnels qu'il opère ou utilise permettent de journaliser les RP-RS conformément à l'obligation prévue au point précédent. De plus, lorsqu'il procède à l'acquisition d'un actif informationnel, l'Établissement exige que les capacités de journalisation de cet actif permettent de se conformer à la présente politique.

Dans le cas où l'Établissement détient un actif informationnel ne permettant pas une journalisation conforme à la présente politique, l'Établissement analyse la possibilité de remplacer cet actif par un autre permettant une journalisation conforme à la présente politique.

19.2.3 Obligation de journalisation des RP-RS qui ne sont pas sur support numérique

L'Établissement met en place une procédure visant à journaliser l'accès, l'utilisation ou la communication de RP-RS qui ne sont pas détenus sur un support numérique. Cette procédure prévoit les modalités afin d'assurer le suivi efficace des RP-RS à l'extérieur de leurs lieux d'entreposage ou d'archivage.

19.2.4 Obligation d'auditer la journalisation effectuée

L'Établissement met en place un processus visant à procéder à un audit de la journalisation effectuée. Cet audit doit permettre à l'Établissement de vérifier si l'accès, l'utilisation ou la communication des RP-RS est effectué de manière conforme à la présente politique.

Les résultats d'audit sont communiqués au CAI-PRPRS le 31 mars et le 30 septembre de chaque année.

Tout incident de confidentialité constaté lors d'un audit doit être signalé sans délai au CAI-PRPRS.

19.2.5 Obligation de reddition de compte quant à la journalisation

L'Établissement transmet annuellement au ministre un rapport faisant état des accès, des utilisations ou des communications de RP-RS qui ne sont pas conformes à la présente politique. Ce rapport est produit par le CAI-PRPRS.

Pour plus d'informations concernant la journalisation, veuillez consulter la *Procédure sur la journalisation des accès, l'anonymisation et la destruction des renseignements personnels et des renseignements de santé et de services sociaux* ([Annexe 21](#)).

19.3 ACTIVITÉS DE FORMATION ET SENSIBILISATION EN MATIÈRE DE PROTECTION DES RP-RS

L'Établissement prend les mesures requises pour s'assurer que toutes les personnes visées par la présente politique soient au fait des règles en matière de vie privée prévues aux lois applicables, de même qu'à cette politique. La sensibilisation et la formation de manière continue sont essentielles pour assurer la protection des RP-RS.

19.3.1 Communication de la présente politique

L'Établissement communique la présente politique à l'ensemble des personnes visées par celle-ci. Il s'assure également que ces personnes reçoivent les explications et la sensibilisation requise quant aux principes qu'elle contient.

L'Établissement s'assure que les membres du personnel et les personnes affiliées s'engagent à respecter la présente politique et documente cet engagement par le biais du *Formulaire d'engagement à respecter la politique de gouvernance des RP-RS de l'Établissement* ([Annexe 22](#)). Ce formulaire sera transmis et consigné par l'Établissement par le biais de ses directions concernées.

À ce titre:

1. La DRHDO s'assure de diffuser la politique et de collecter le formulaire d'engagement signé à tout nouveau membre du personnel lors de l'embauche;
2. La DEAU s'assure de diffuser la politique et de collecter le formulaire d'engagement signé à tout étudiant, professeur ou stagiaire sous sa responsabilité;
3. La DR s'assure de diffuser la politique et de collecter le formulaire d'engagement signé à tout chercheur, membre de l'équipe de recherche ou étudiant sous sa responsabilité;
4. La DSP-FH s'assure de diffuser la politique et de collecter le formulaire d'engagement signé à tout membre du CMDP exerçant leur profession au sein de l'Établissement;
5. La DL s'assure de diffuser la politique à tout fournisseur, prestataire de services, sous-traitant ou autre lors de la conclusion du contrat.

La politique est ensuite communiquée de nouveau à chaque personne visée de façon périodique.

19.3.2 Formation obligatoire

L'Établissement s'assure que les membres de son personnel et les personnes affiliées reçoivent une formation en matière de protection des RP-RS reconnue par le MSSS, dès leur entrée en fonction ou le début de l'exercice de leur profession/affiliation au sein de l'Établissement. Cette obligation s'applique également à l'égard des personnes mentionnées par règlement.

En matière de recherche, les formations portant sur les MON de l'Établissement et sur les bonnes pratiques cliniques doivent obligatoirement être complétées par les

chercheurs et les membres de leurs équipes de recherche. Ces formations traitent de la protection des RP-RS.

L'Établissement veille également à ce que ces personnes mettent à jour annuellement leurs connaissances en matière de protection des RP-RS. Cette mise à jour porte sur:

1. Les rôles et les responsabilités des membres du personnel de l'Établissement et des professionnels qui y exercent leur profession, y compris les étudiants et les stagiaires, à l'égard des RP-RS qu'il détient;
2. Les règles et les modalités de conservation, de destruction et d'anonymisation des RP-RS;
3. Les mesures de sécurité propres à assurer la protection des RP-RS que l'Établissement a mises en place, notamment celles visant à minimiser les risques d'incident de confidentialité;
4. Le processus de traitement des incidents de confidentialité;
5. L'utilisation sécuritaire des produits ou services technologiques de l'Établissement.

Le CAI-PRPRS révisé annuellement l'offre d'activités de formation et de sensibilisation en matière de protection de RP-RS et détermine celles qui doivent être obligatoires en tenant compte de la catégorie de personnes exerçant leur profession à l'Établissement et du degré de sensibilité des RP-RS auxquels elles auront accès.

19.3.3 Activités de formation et de sensibilisation

Plusieurs activités de formation et de sensibilisation en matière de protection des RP-RS sont offertes aux membres du personnel et aux personnes affiliées, notamment en lien avec la tenue de dossier et rédaction de notes, la protection des RP-RS, la sécurité de l'information et la cybersécurité.

Des capsules de formation sur la sécurité de l'information sont également disponibles sur la plateforme « Environnement numérique d'apprentissage » (**ENA**) du MSSS, et ce, pour l'ensemble des membres du personnel et des personnes affiliées de l'Établissement (exemples : Cybersécurité, sensibilisation en sécurité informationnelle, confidentialité et sécurité de l'information, etc.).

Enfin, le CAI-PRPRS procède à la rédaction de feuillets d'information à l'égard des bonnes pratiques en matière de protection des RP-RS. Ces feuillets sont diffusés aux membres du personnel et aux personnes affiliées et sont disponibles sur l'intranet de l'Établissement dans la section [Boîte à outils PRP](#).

19.4 MESURES DE SÉCURITÉ SUPPLÉMENTAIRES

L'Établissement déploie divers mécanismes de protection des RP-RS afin d'en assurer la confidentialité.

19.4.1 Accès aux installations et aux actifs informationnels

L'Établissement restreint l'accès aux RP-RS via l'utilisation de cartes d'identité du CISSS ou d'autres dispositifs d'accès tel la clé d'authentification SecurSanté (communément appelée clé DSQ). Ces dispositifs permettent la protection des RP-RS notamment en sécurisant physiquement les entrées dans les bâtiments et les zones

restreintes et en créant une barrière de sécurité numérique (accès aux logiciels, systèmes et autres actifs informationnels informatisés).

Les cartes d'identité du CISSS remises aux membres du personnel et personnes affiliées enregistrent l'heure et les endroits où elles sont utilisées. De plus, des caméras de sécurité installées dans les locaux de l'Établissement enregistrent sur bande vidéo les espaces clés des installations de l'Établissement. L'information tirée des cartes d'identité et des enregistrements des caméras de sécurité est accessible et utilisable à des fins de sécurité ou pour se conformer aux politiques de l'Établissement. Selon l'emplacement du poste de travail, certains RP-RS associés aux cartes d'identité et aux caméras de sécurité peuvent être recueillis, et dans un tel cas, ces RP-RS sont assujettis à la présente politique. Pour plus d'informations concernant la surveillance par caméra de sécurité, veuillez consulter la *Politique sur la vidéosurveillance* ([Annexe 23](#)).

Afin que ces mécanismes soient efficaces, l'Établissement s'assure de diffuser aux membres du personnel et personnes affiliées les bonnes pratiques qui doivent être respectées de tous. La protection des RP-RS s'appuie sur l'implication continue de chaque membre du personnel ou personne affiliée, devant notamment:

1. Ne jamais laisser une carte d'identité ou autre dispositif sans surveillance;
2. Ne pas jumeler la carte d'identité avec un autre dispositif d'accès;
3. Signaler immédiatement toute perte ou vol de la carte d'identité ou autre dispositif afin de permettre à l'Établissement de les désactiver;
4. Ne jamais prêter sa carte d'identité ou autre dispositif à d'autres personnes;
5. Informer immédiatement son gestionnaire si un accès ne fonctionne pas ou si des comportements suspects sont observés;
6. Utiliser un mot de passe fort et unique à chaque logiciel, système ou autres actifs informationnels pour protéger les accès;
7. Modifier régulièrement les mots de passe;
8. Utiliser les actifs informationnels avec discernement aux fins prévues et en se conformant aux politiques, procédures et directives de l'Établissement;
9. Ne pas conserver de RP-RS à l'extérieur des actifs informationnels ou du réseau de l'Établissement;
10. Prendre connaissance et s'approprier les meilleures pratiques en matière de protection des RP-RS.

Pour plus d'informations, veuillez consulter la *Politique de sécurité des ressources informationnelles* ([Annexe 20](#)) et la *Politique sur l'attribution et l'utilisation d'équipements et d'appareils de télécommunication mobile* ([Annexe 24](#)).

19.4.2 Installation de logiciels et d'équipements

Toute installation de logiciel ou d'équipement est effectuée exclusivement sous la supervision ou sur la préapprobation d'une personne compétente en la matière. D'ailleurs, l'Établissement contrôle la circulation et les accès des représentants des fournisseurs, prestataires de service, entrepreneurs et autres à l'intérieur des installations de l'Établissement. Pour plus d'informations, veuillez consulter la *Procédure relative à l'encadrement de la présence des représentants de fournisseurs dans les installations du CISSSMC* ([Annexe 25](#)).

19.4.3 ÉFVP

Tel que mentionné à la présente politique, l'Établissement effectue des ÉFVP afin de mieux protéger les RP-RS :

1. Avant de communiquer ou de confier des RP-RS à une personne à l'extérieur du Québec (voir [section 17](#));
2. En cas de communication de RS sans le consentement des usagers à des fins de recherche (voir [section 11.6.2](#));
3. Dans le cadre de projet d'acquisition, de développement et de refonte d'un système d'informations ou de prestation électronique de services impliquant des RP-RS (voir [section 16](#)).

19.4.4 Transmission d'information

Les communications verbales, de visu ou par téléphone, au sujet d'une personne doivent se faire dans un endroit retiré pour respecter la confidentialité. Tout membre du personnel et toute personne affiliée doivent s'assurer de l'identité de la personne à qui elle communique des RP-RS.

Tout membre du personnel et toute personne affiliée doit également :

1. Récupérer un document imprimé immédiatement après son impression;
2. Utiliser l'impression sécurisée, lorsque disponible, notamment sur les imprimantes multifonctions;
3. Protéger adéquatement un document contenant des RP-RS (par exemple : enveloppe sécurisée, cachetée, courrier recommandé, etc.) lors d'un envoi par courrier interne/externe ou par la poste;
4. Sécuriser physiquement les documents papier dans un lieu sûr et sécuritaire (par exemple : tiroir ou classeur barré, local verrouillé avec accès limité, etc.);
5. Disposer des documents dans un bac verrouillé « confidentiel » prévu à cet effet et non dans la récupération régulière ou dans les corbeilles pour le papier;
6. Récupérer un document immédiatement après l'avoir transmis par télécopie. Le télécopieur doit être situé dans un endroit sûr et ne doit être utilisé que par les personnes autorisées;
7. Aviser le destinataire qu'il y aura transmission et s'assurer qu'il en attendra la réception;
8. Accompagner les envois d'un formulaire de transmission, en indiquant le caractère confidentiel de l'envoi, le nom, l'adresse et le numéro de téléphone du destinataire ainsi que le nom et le numéro de téléphone de l'expéditeur;
9. Vérifier le numéro du télécopieur du destinataire après la composition pour éviter les erreurs;
10. Vérifier le rapport de transmission et le classer au dossier.

En ce qui concerne la transmission par messagerie électronique, tout membre du personnel et toute personne affiliée doivent présumer que toute communication qu'ils créent, envoient, reçoivent ou mémorisent sur les systèmes électroniques d'informations ou les systèmes informatiques de l'Établissement peut être lue par quelqu'un d'autre que le destinataire. Ainsi, tout membre du personnel et toute personne affiliée ne doivent pas envoyer d'information confidentielle, de RP ou de RS par une messagerie électronique autre que celle autorisée par l'Établissement (Outlook du réseau de la santé et des services sociaux (RSSS)) ou par les outils de collaboration fournis par le MSSS (suite Office 365).

Les systèmes tels que Outlook (du RSSS) ou des applications spécialisées comme DSIE, RSIPA, SyMo et autres, comportent les mécanismes garantissant la confidentialité des données transmises à l'intérieur du RSSS. Pour les envois vers l'externe par courriel Outlook du RSSS, les messages et les pièces jointes doivent d'abord être protégés en suivant les règles énoncées par le MSSS sur la plateforme Office 365.

19.4.5 Incident de confidentialité

Tout incident de confidentialité doit être déclaré au CAI-PRPRS selon les procédures suivantes :

1. Si l'incident de confidentialité concerne un RS contenu au dossier de l'utilisateur, selon la *Procédure de déclaration des incidents et des accidents liés à une prestation de soins et de services aux usagers (DQEPEL-206a)* ([Annexe 26](#))
2. Pour tout autre RP, selon la *Procédure de déclaration des incidents de confidentialité impliquant des renseignements personnels reliés aux documents administratifs* ([Annexe 27](#)).

L'Établissement a élaboré une *Procédure en matière de gestion des incidents de confidentialité* ([Annexe 28](#)) laquelle **(i)** énonce les rôles et les responsabilités des membres de son Comité de gestion des incidents de confidentialité, lors de la survenance d'un tel incident; **(ii)** établit les critères applicables pour déterminer si un incident de confidentialité présente un risque qu'un préjudice sérieux soit causé; **(iii)** prévoit les mesures devant être mises en place pour gérer les incidents de confidentialité et **(iv)** prévoit les délais et les seuils de réalisation de chaque mesure.

Cette procédure s'applique à tout incident de confidentialité impliquant des RP-RS détenus par l'Établissement.

20 DESTRUCTION ET ANONYMISATION DES RP-RS

Lorsque les finalités pour lesquelles un RP-RS a été collecté ou utilisé sont accomplies et sous réserve des délais prévus au calendrier de conservation, l'Établissement procède à la destruction ou à l'anonymisation des RP-RS de manière sécuritaire.

20.1 DESTRUCTION

20.1.1 Documents papier

Les documents papier renfermant des RP-RS sont détruits par déchiquetage en respectant les exigences minimales émises par le MSSS et/ou la CAI. Entre autres, les documents papier à détruire et contenant des RP-RS sont placés dans la boîte ou le bac prévu à cet effet dans les services et unités de l'Établissement afin qu'ils soient déchiquetés. Les documents contenant des RP-RS ne doivent jamais être jetés à la poubelle ou au recyclage.

20.1.2 Support informatique

Les RP-RS sur support informatique (notamment les disques durs, les supports amovibles, les appareils mobiles) sont détruits de façon sécuritaire. La DRIM doit être contactée pour du soutien à cet égard.

20.2 ANONYMISATION

L'Établissement peut, au lieu de la destruction, procéder à l'anonymisation d'un RP-RS pour l'utiliser à des fins d'intérêt public. Il s'agit d'une possibilité, et non d'une obligation. L'anonymisation devra respecter les critères et exigences prévus par règlement.

Pour plus d'informations sur le processus de destruction ou d'anonymisation, veuillez consulter la *Procédure sur la journalisation des accès, l'anonymisation et la destruction des renseignements personnels et des renseignements de santé et de services sociaux et (Annexe 21)*.

21 OBLIGATIONS DES PERSONNES VISÉES À LA POLITIQUE À L'ÉGARD DES RP-RS

21.1 OBLIGATIONS RELATIVES AU RESPECT DE LA CONFIDENTIALITÉ DES RP-RS

En plus des obligations susmentionnées, les personnes visées par la présente politique doivent, en tout temps, prendre les mesures permettant de maintenir le caractère confidentiel des RP-RS, le tout dans le respect des procédures, directives ou consignes quant aux lieux où ces RP-RS sont consultés, quant aux actifs informationnels utilisés pour accéder aux RP-RS et quant aux modalités d'entreposage, d'archivage ou de sauvegarde des RP-RS.

Les personnes visées par la politique ne peuvent communiquer les RP-RS auxquels ils ont accès qu'aux personnes y ayant un droit d'accès.

Hormis les personnes spécifiquement autorisées par la présente politique, aucune personne visée n'est autorisée à communiquer un RP-RS à un tiers, ni à communiquer un RS sous forme documentaire à un usager.

En plus des diverses politiques et procédures énumérées ci-dessus et visant les membres du personnel et les personnes affiliées à l'Établissement, ces derniers sont également liés aux obligations contenues aux autres politiques, procédures et directives de l'Établissement visant à assurer la confidentialité des RP-RS dans le cadre de leur fonction, notamment:

1. *Politique d'utilisation des médias sociaux* ([Annexe 29](#));
2. *Politique sur le télétravail* ([Annexe 30](#));
3. *Procédure sur la gestion du télétravail* ([Annexe 31](#));
4. *Procédure sur l'appartenance au système professionnel* ([Annexe 32](#));
5. *Code d'éthique organisationnel* ([Annexe 33](#)).

21.2 OBLIGATIONS RELATIVES À LA DIVULGATION DE TOUT INCIDENT DE CONFIDENTIALITÉ

Tout membre du personnel et toute personne affiliée qui sont avisés ou qui ont connaissance d'une situation mettant en cause un incident de confidentialité sont tenus de signaler l'incident, sans délai, selon les modalités prévues à la [section 19.4.5](#). Ils doivent également collaborer à toute démarche d'analyse, d'enquête ou de divulgation en découlant.

22 REGISTRES DE L'ÉTABLISSEMENT ET INVENTAIRE

22.1 REGISTRE DE PRODUIT OU SERVICE TECHNOLOGIQUE

L'Établissement doit inscrire dans un registre tout produit ou service technologique qu'il utilise. L'Établissement rend accessible ce registre au public par tout moyen approprié.

22.2 REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

L'Établissement tient un registre des incidents de confidentialité, lequel est sous la responsabilité du CAI-PRPRS.

Dans la mesure où l'Établissement comptabilise les incidents de confidentialité dans un ou plusieurs actifs informationnels, le CAI-PRPRS a accès à ces actifs afin d'y constituer le registre mentionné ci-haut.

Le registre des incidents de confidentialité contient les informations prévues par règlement.

Les informations contenues au registre sont tenues à jour et conservées pendant une période minimale de 5 ans après la date ou la période au cours de laquelle l'Établissement a pris connaissance de l'incident.

22.3 REGISTRE DES COMMUNICATIONS

L'Établissement tient à jour un registre de communication de RP-RS sans consentement.

Pour les fins de la tenue de ce registre, le Service de la gestion documentaire doit être avisé de toute transmission de RP-RS faite sans le consentement de la personne concernée ou de l'utilisateur.

Lors de la communication avec le Service de la gestion documentaire, les informations suivantes doivent être transmises :

1. Le type de RP-RS communiqué;
2. La personne ou l'organisme qui reçoit les RP-RS;
3. La fin pour laquelle il y a communication de RP-RS;
4. Les raisons et les dispositions de la Loi sur l'accès ou de la LRSSS qui justifient la communication.

Ce registre contient les informations prévues aux lois applicables.

22.4 INVENTAIRE DE FICHIERS CONTENANT DES RP

Lors de la conservation de RP, l'Établissement verse certains RP dans un fichier de RP (par exemple, les dossiers des employés, les dossiers de paie, etc.).

L'Établissement maintient à jour un inventaire de ses fichiers de RP.

Le Service de la gestion documentaire doit être avisé de toute nouvelle collecte de données ou informations amenant à la création de nouveaux fichiers de RP qui :

1. Sont identifiés ou se présentent de façon à être retrouvés par référence au nom d'une personne ou à un signe ou symbole propre à celle-ci, comme un numéro de dossier par exemple; ou
2. Ont servi ou sont destinés à servir pour une décision concernant une personne.

Les RP qui ne tombent pas dans l'une de ces deux catégories n'ont pas à être versés dans un fichier de RP.

23 DEMANDE D'ACCÈS ET DE RECTIFICATION

23.1 DEMANDE D'ACCÈS ET DE RECTIFICATION PAR L'USAGER OU CERTAINES PERSONNES LIÉES

Les modalités d'accès ou de rectification aux RS contenus au dossier d'emploi ou d'affiliation de la personne concernée sont prévues à la *Procédure sur le traitement d'une demande d'accès ou de rectification à des renseignements personnels ou à des renseignements de santé et de services* ([Annexe 34](#)).

La personne responsable du traitement transmettra à la demanderesse un avis écrit de la date de la réception de sa demande. Cet avis indiquera les délais prescrits pour donner suite à la demande et l'effet que la loi attache à son défaut de les respecter. En outre, l'avis de réception informera la demanderesse du recours en révision prévu à la LRSSS.

La personne responsable du traitement de la demande d'accès ou de rectification y donnera suite au plus tard dans les 30 jours qui suivent la date de sa réception. À défaut de répondre à une demande dans le délai applicable, la personne responsable est réputée avoir refusé d'y faire droit et ce défaut donne ouverture au recours en révision prévu à la LRSSS comme s'il s'agissait d'un refus de faire droit à la demande.

23.2 DEMANDE D'ACCÈS ET DE RECTIFICATION AUX RP CONTENUS À SON PROPRE DOSSIER

Les modalités d'accès ou de rectification aux RP contenus au dossier d'emploi ou d'affiliation de la personne concernée sont prévues à la *Procédure sur le traitement d'une demande d'accès ou de rectification à des renseignements personnels ou à des renseignements de santé et de services* ([Annexe 34](#)).

La personne responsable du traitement de la demande d'accès ou de rectification transmettra à la demanderesse un avis écrit de la date de la réception de sa demande, contenant les délais prescrits pour donner suite à la demande et l'effet que la loi attache à son défaut de les respecter. En outre, l'avis de réception informera la demanderesse du recours en révision prévu à la Loi sur l'accès.

La personne responsable du traitement donnera suite à une demande au plus tard dans les 20 jours qui suivent la date de sa réception. La personne responsable du traitement peut prolonger le délai d'une période supplémentaire de 10 jours si le traitement de la demande nécessite plus de temps, mais elle doit alors donner avis à la personne concernée effectuant la demande par écrit dans le premier délai de 20 jours.

À défaut de répondre à une demande dans le délai applicable, la personne responsable du traitement est réputée avoir refusé d'y faire droit et ce défaut donne ouverture au recours en révision prévu à la Loi sur l'accès comme s'il s'agissait d'un refus de faire droit à la demande.

23.3 MODALITÉ DE COMMUNICATION À LA SUITE D'UNE DEMANDE D'ACCÈS OU DE RECTIFICATION PRÉVUE AUX SECTIONS [23.1](#) ET [23.2](#)

Si la demande d'accès est accordée, l'Établissement communiquera le RP-RS visé et permettra à la personne demanderesse d'en prendre connaissance sur place pendant les heures habituelles de travail ou à distance et d'obtenir une copie des documents. Sur demande, la personne responsable s'assure de fournir à la personne demanderesse l'assistance d'un professionnel qualifié pour l'aider à comprendre le RP-RS.

23.3.1 Format des communications

Si la personne demanderesse le requiert, un RP-RS informatisé doit lui être communiqué sous la forme d'une transcription écrite et intelligible, à moins que cela ne soulève des difficultés pratiques sérieuses (voir [section 24](#)).

23.3.2 Mesures d'accommodement

Lorsque la personne demanderesse est une personne handicapée et que les formes usuelles de transmission ne lui permettent pas de recevoir communication des RP-RS, des mesures d'accommodement raisonnable seront prises par l'Établissement, sur demande, pour lui permettre de recevoir communication des RP-RS auxquels elle a droit.

23.4 DEMANDE D'ACCÈS AUX RS PAR UN INTERVENANT EXTERNE À L'ÉTABLISSEMENT

Les modalités d'accès aux RS par un intervenant externe à l'Établissement sont prévues à la *Procédure sur le traitement d'une demande d'accès ou de rectification à des renseignements personnels ou à des renseignements de santé et de services* ([Annexe 34](#)).

L'intervenant ne conserve le RS ainsi communiqué que si cela est nécessaire aux services de santé ou aux services sociaux qu'il offre ou, le cas échéant, au respect de ses obligations professionnelles. L'organisme au sein duquel l'intervenant offre ces services est alors considéré détenteur du RS conservé.

24 DROIT À LA PORTABILITÉ

24.1 PERSONNES VISÉES

Toute personne peut obtenir, dans un format technologique structuré et couramment utilisé, un RP-RS informatisé qu'elle a fourni ou demandé, que celui-ci soit transmis à une autre personne ou à un organisme autorisé par les lois applicables à les recueillir dans ce même format.

24.2 CAPACITÉ DES SYSTÈMES

L'Établissement s'assure que tout projet d'acquisition, de développement et de refonte d'un système d'informations ou de prestation électronique de services impliquant des RP-RS permet qu'un RP-RS informatisé recueilli auprès de la personne concernée ou de l'utilisateur puisse lui être communiqué dans un format technologique structuré et couramment utilisé.

24.3 FORMAT TECHNOLOGIQUE STRUCTURÉ ET COURAMMENT UTILISÉ

L'Établissement communique les RP-RS dans un format technologique permettant à des applications logicielles d'usage courant de reconnaître et d'extraire les informations qui y sont contenues. L'Établissement privilégie des formats adaptés aux RP-RS demandés, ouverts et interopérables.

24.4 RP-RS VISÉS

Seuls les RP-RS informatisés recueillis auprès de la personne concernée ou de l'utilisateur sont visés par le droit à la portabilité.

Les RP-RS informatisés incluent :

1. Les RP-RS que la personne a fournis directement à l'Établissement;
2. Les RP-RS recueillis indirectement auprès de la personne concernée ou de l'utilisateur et qui sont, notamment, générés par son activité.

24.5 EXCLUSION DE CERTAINS RP-RS

Les RP-RS qui ne sont pas recueillis auprès de la personne concernée ou de l'utilisateur et qui sont créés ou inférés à partir des RP-RS de la personne concernée ou de l'utilisateur ne sont pas visés par la présente section.

24.6 EXERCICE ET MODALITÉ DU DROIT À LA PORTABILITÉ

Le droit à la portabilité peut s'exercer à condition qu'il ne soulève pas de difficultés pratiques sérieuses dont, notamment, des coûts importants pour donner suite à la demande ou la complexité que nécessite le transfert.

Lorsqu'une personne demande la transmission dans un format particulier, l'Établissement en tient compte, sauf si ce choix soulève des difficultés pratiques sérieuses.

La [section 23](#) relative aux demandes d'accès aux RP-RS s'applique au droit à la portabilité.

Lorsque l'Établissement refuse de donner suite à une demande en raison de difficultés pratiques sérieuses, l'Établissement doit être en mesure de fournir les justifications nécessaires lors d'une demande de révision devant la CAI.

Lorsque la demande implique la transmission de RP-RS à un organisme autorisé par la loi, l'Établissement s'assure que le tiers est en droit de recueillir de tels RP-RS et tient compte, selon le cas :

1. Des exigences de l'article 37 du *Code civil du Québec*;
2. Des articles 4 et 5 de la *Loi sur la protection des renseignements personnels dans le secteur privé*;
3. De l'article 64 de la Loi sur l'accès.

24.7 QUALITÉ DES RP-RS

L'Établissement n'a pas l'obligation de vérifier la qualité des RP-RS avant de donner suite à chaque demande. L'Établissement s'assure que les RP-RS qu'il conserve sont à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis ou utilisés.

Pour plus d'informations au sujet de la portabilité, veuillez consulter la *Procédure sur la portabilité* ([Annexe 35](#)).

25 SITE INTERNET

Une politique de confidentialité a été incluse au site Internet de l'Établissement afin de diffuser des précisions quant à ses pratiques, comme l'Établissement recueille, par un moyen technologique, des RP. L'Établissement met à jour cette politique lorsque cela est requis et s'assure que la politique de confidentialité est rédigée en termes simples et clairs. Pour plus d'informations, veuillez consulter la *Politique de confidentialité* disponible sur le Portail Santé Montérégie ([Annexe 36](#)).

26 PROCESSUS DE TRAITEMENT D'UNE PLAINTE RELATIVES À LA PROTECTION DES RP-RS

26.1 PLAINTÉ CONCERNANT LES RS

Toute plainte qui concerne le traitement des RS ou le dossier des usagers doit être déposée auprès de la Commissaire aux plaintes et à la qualité des services ("CPQS") via le formulaire de plainte en ligne: [Formulaire de plainte – CISSS de la Montérégie-Centre | Portail Santé Montérégie \(santemonteregie.qc.ca\)](#).

Toute plainte portant sur des allégations de manquement à l'intégrité scientifique et à la conduite responsable en recherche eu égard aux RS sera traitée en fonction de la *Politique sur la conduite responsable en recherche* ([Annexe 17](#)).

26.2 PLAINTÉ CONCERNANT LES RP

Toute plainte qui concerne le traitement des RP ou le dossier des membres du personnel ou des personnes affiliées doit être adressée à la Responsable de la protection des RP-RS:

Responsable de la protection des renseignements personnels et de santé – services sociaux

Directrice des affaires corporatives et des partenariats

Direction des affaires corporatives et des partenariats

CISSS de la Montérégie-Centre

3141, boulevard Taschereau, bureau 220

Greenfield Park (Québec) J4V 2H2

Courriel: prp.ciSSSmc16@sSSS.gouv.qc.ca

26.3 TRANSFERT DE LA PLAINTÉ

Tout membre du personnel ou toute personne affiliée qui reçoit une plainte relative à la protection des RP-RS doit la transmettre sans délai à la CPQS, ou à la Responsable de la protection des RP-RS, selon le cas. Lorsque la plainte est formulée verbalement, le membre du personnel ou la personne affiliée accompagne la personne concernée en lui remettant les coordonnées ci-dessus mentionnées pour le dépôt de sa plainte.

26.4 TRAITEMENT D'UNE PLAINTE

26.4.1 Plainte à la CPQS

Un accusé de réception est automatiquement transmis lorsque la personne concernée complète le formulaire en ligne. La CPQS examine la plainte pour bien cerner le problème et tenter de le résoudre. À ce moment et au besoin, elle pourra communiquer avec la personne concernée afin de valider sa version des faits.

La CPQS informe la personne concernée des résultats de son enquête dans un délai n'excédant pas 45 jours suivant la réception de la plainte. Ses conclusions sont accompagnées des solutions pour résoudre le problème ou des mesures correctives recommandées à l'Établissement. Les conclusions sont transmises verbalement si la plainte est verbale et par écrit si elle est écrite.

Pour plus d'informations, veuillez consulter: [Plaintes, satisfaction et maltraitance - CISSS de la Montérégie-Centre | Portail Santé Montérégie \(santemonteregie.qc.ca\)](#)

26.4.2 Plainte à la Responsable de la protection des RP-RS

La plainte sera examinée dès que possible. La Responsable de la protection des RP-RS pourra communiquer avec la personne concernée pour obtenir toute autre information requise au traitement. Toute plainte est traitée de façon impartiale et dans le respect de la confidentialité.

La Responsable de la protection des RP-RS informe la personne concernée des résultats de son enquête dans un délai n'excédant pas 45 jours suivant la réception de la plainte. Ses conclusions sont accompagnées des solutions pour résoudre le problème ou des mesures correctives recommandées à l'Établissement.

26.5 PLAINTES À LA CAI

Il est également possible pour la personne concernée de déposer une plainte concernant la protection des RP-RS à la CAI. Pour plus d'informations, veuillez consulter le site internet de la CAI: [Citoyens \(gouv.qc.ca\)](#)

27 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](#)

CHU SAINTE-JUSTINE, Politique de gouvernance des renseignements personnels, 26 mars 2024.

UNIVERSITÉ DE MONTRÉAL, Politique de protection des renseignements personnels (40.29).

CIUSSS DE L'ESTRIE-CHUS, Politique de gouvernance des données, 13 juin 2024.

28 ANNEXES

- Annexe 1:** Structure des comités organisationnels – Protection des RP-RS
- Annexe 2:** CISSSMC – Politique sur le consentement aux soins – DSP-002
- Annexe 3:** CISSSMC – Calendrier de conservation des documents
- Annexe 4:** CISSSMC – Politique de gestion intégrée des documents administratifs – DG-301
- Annexe 5:** CISSSMC – Procédure de gestion des documents semi-actifs sous format papier– DG-301a
- Annexe 6:** CISSSMC – Politique d'accès, de gestion, de conservation des dossiers des usagers – DSM-702 (mise à jour à venir)
- Annexe 7:** CISSSMC – Cadre de gestion de l'accès (à venir)
- Annexe 8:** CISSSMC – Modèle d'attestation sous serment (à venir)
- Annexe 9:** CISSSMC – Schéma d'accès aux renseignements de santé et de services sociaux par les intervenants internes et externes (à venir)
- Annexe 10:** CISSSMC – Entente permettant d'être informé de l'existence de renseignements personnels ou de santé et services sociaux nécessaires à la réalisation d'un projet de recherche et d'y avoir accès, sans le consentement des personnes concernées par ces renseignements
- Annexe 11:** CISSSMC – Procédure concernant les évaluations des facteurs relatifs à la vie privée (à venir)
- Annexe 12:** CISSSMC – Processus organisationnel de demande d'évaluation et d'avis de protection des renseignements personnels et des renseignements de santé et de services sociaux (à venir)
- Annexe 13:** CISSSMC – Formulaire de demande d'autorisation à être informé de l'existence de renseignements de santé et de services sociaux nécessaires à la réalisation d'un projet de recherche et d'y avoir accès, sans le consentement des personnes concernées par ces renseignements
- Annexe 14:** CISSSMC – Directive sur les conditions et les modalités de divulgation de renseignements confidentiels pour prévenir un acte de violence dont un suicide (à venir)
- Annexe 15:** CISSSMC – Engagement de confidentialité dans le cadre d'un mandat ou à l'exécution d'un contrat de service, d'entreprise ou d'approvisionnement (à venir)
- Annexe 16:** CISSSMC – Cadre règlementaire sur l'organisation et les bonnes pratiques de la recherche au CISSS de la Montérégie-Centre – R-2016-07
- Annexe 17:** CISSSMC – Politique sur la conduite responsable et l'intégrité scientifique en recherche – DR-001;
- Annexe 18:** CISSSMC – Procédure d'évaluation de la convenance institutionnelle de la recherche au CISSS de la Montérégie-Centre – DR-003
- Annexe 19:** CISSSMC – Politique sur le dossier du cadre – DRHDO-AJ-012
- Annexe 20:** CISSSMC – Politique de sécurité des ressources informationnelles – DRIM-101
- Annexe 21:** CISSSMC – Procédure sur la journalisation des accès, l'anonymisation et la destruction des renseignements personnels et des renseignements de santé et de services sociaux (à venir)
- Annexe 22:** Formulaire d'engagement à respecter la politique de gouvernance des RP-RS de l'Établissement (à venir)
- Annexe 23:** Politique sur la vidéosurveillance (à venir)

- Annexe 24:** CISSSMC – Politique sur l’attribution et l’utilisation d’équipements et d’appareils de télécommunication mobile – DRIM-201
- Annexe 25:** CISSSMC – Procédure relative à l’encadrement de la présence des représentants de fournisseurs dans les installations du CISSSMC – DL-101
- Annexe 26:** CISSSMC – Procédure de déclaration des incidents et des accidents liés à une prestation de soins et de services aux usagers - DQEPEL-206a
- Annexe 27:** CISSSMC – Procédure de déclaration des incidents de confidentialité impliquant des renseignements personnels reliés aux documents administratifs (à venir)
- Annexe 28:** CISSSMC – Procédure en matière de gestion des incidents de confidentialité (à venir)
- Annexe 29:** CISSSMC – Politique d’utilisation des médias sociaux – DCAP-001
- Annexe 30:** CISSSMC – Politique sur le télétravail - DRHDO-AJ-501
- Annexe 31:** CISSSMC – Procédure sur la gestion du télétravail - DRHDO-AJ-501a
- Annexe 32:** CISSSMC – Procédure sur l’appartenance au système professionnel – DSM-001
- Annexe 33:** CISSSMC – Code d’éthique organisationnel – R-2017-15
- Annexe 34:** CISSSMC – Procédure sur le traitement d’une demande d’accès ou de rectification à des renseignements personnels ou à des renseignements de santé et de services sociaux (à venir)
- Annexe 35:** CISSSMC – Procédure sur la portabilité (à venir)
- Annexe 36:** Les CISSS de la Montérégie – Politique de confidentialité

29 DISPOSITIONS FINALES ET TRANSITOIRES

29.1 RÉVISION

La politique doit faire l’objet d’une révision aux trois (3) ans ou lorsque des modifications le requièrent. Toute modification apportée à la présente politique entre en vigueur le jour de son adoption par le conseil d’administration.

HISTORIQUE DES VERSIONS (du plus ancien au plus récent)		
Numéro et titre	Date d’adoption	Établissement d’origine
DACP-001 – Politique de gouvernance des renseignements de santé et de services sociaux et des renseignements personnels	2024-11-19	CISSS de la Montérégie-Centre

<p>RÉDIGÉE OU RÉVISÉE PAR Me Marie-Claude Boutin, responsable de la protection des RP-RS Me Valérie Marceau Milhomme, conseillère-cadre à la protection des RP-RS Mélissa-Anne Blain, conseillère-cadre à la protection des RP-RS</p>
<p>PERSONNES CONSULTÉES Membres du CAI-PRPRS Cloé Rodrigue, directrice de la recherche</p>