

CISSSMC – Formulaire d’engagement à respecter la politique de gouvernance des renseignements personnels et de santé et de services sociaux de l’Établissement

1. IDENTIFICATION DU SIGNATAIRE

Nom, prénom : _____ Titre : _____

- ☐ **Membre du personnel;** Matricule _____
- ☐ **Personne affiliée à l’Établissement** (membre du CMDPSF, chercheurs(se), étudiant(e), stagiaire, bénévole, etc.);
- ☐ **Prestataire de services, fournisseurs, sous-traitants ou autres**

2. PRÉAMBULE

Toute personne a droit au respect de sa vie privée, de même qu’au respect du secret professionnel. Le CISSS de la Montérégie-Centre (l’« **Établissement** ») est responsable d’assurer la protection des renseignements personnels (« **RP** ») et des renseignements de santé et de services sociaux (« **RS** ») qu’il détient pour Santé Québec et cette responsabilité est partagée par l’ensemble des membres du personnel, des personnes affiliées (membres du CMDPSF, les chercheurs, les étudiants, les stagiaires et les bénévoles), ainsi que toute personne physique ou morale liée à l’Établissement par contrat. Pour ce faire, l’Établissement a adopté une *Politique de gouvernance à l’égard des RP-RS*, laquelle énonce notamment les rôles et responsabilités des personnes visées ci-dessus et des instances appelées à assurer le respect des cadres légaux applicables, les normes assurant la protection des RP-RS et la responsabilité et l’imputabilité de l’Établissement et des personnes visées.

3. ENGAGEMENT

En tant que condition à l’exercice de mes fonctions/mon affiliation/ma prestation contractuelle avec l’Établissement, je comprends la responsabilité qui m’incombe de garantir la confidentialité des RP-RS. Je reconnais que l’Établissement s’est doté d’une *Politique de gouvernance des RP-RS* et je m’engage à respecter les obligations qui en découlent. Par conséquent :

1. Je m’engage à préserver la confidentialité des RP-RS auxquels j’aurai accès ou auxquels je pourrais être exposé, ainsi que la vie privée des usagers, des employés et de toutes autres personnes dans le cadre de l’exercice de mes fonctions/mon affiliation/ma prestation contractuelle et ce, peu importe où ils se trouvent (par exemple: les installations de l’établissement, les GMF dans lesquels je pourrais être appelé à travailler incluant leurs systèmes d’information, le domicile des usagers, etc.);
2. En tant que condition de mes accès à des RP-RS, je comprends et accepte qu’il est de ma responsabilité de me familiariser avec toutes les politiques, procédures et directives de l’Établissement en matière de confidentialité et de sécurité de l’information, dans leur forme actuelle et telles qu’elles pourraient être modifiées à l’avenir, que celles-ci soient annexées ou non à la *Politique de gouvernance des RP-RS*;
3. Si j’ai des questions concernant ces politiques, procédures et directives, y compris leur applicabilité à ma situation et leur impact sur l’exercice de mes fonctions, je contacterai mon supérieur ou la protection des RP-RS de l’Établissement (prp.cisssmc16@ssss.gouv.qc.ca);

4. Dans la mesure où la loi et/ou la *Politique de gouvernance des RP-RS* m'autorise à avoir accès à des RP-RS, je reconnais que le simple fait de pouvoir avoir y accès dans le cadre mes fonctions/mon affiliation/ma prestation contractuelle ne m'autorise pas à y accéder/les utiliser en l'absence d'une raison légitime. **Je limiterai donc l'accès aux RP-RS à ce qui est strictement nécessaire pour accomplir les tâches et responsabilités spécifiques à mes obligations. Par conséquent, je m'engage à ne pas accéder à mes RP-RS ou aux RP-RS de mes connaissances, des membres de ma famille, d'une personnalité publique ou de tout autre usager de l'Établissement au-delà de ce qui est strictement nécessaire pour accomplir mes fonctions/mon affiliation/ma prestation contractuelle;**
5. Je comprends qu'il est strictement interdit de publier sur les médias sociaux des RP-RS ou d'autres informations confidentielles de l'Établissement, de ses employés ou de ses partenaires et des usagers, incluant des photos, vidéos ou enregistrements et que la suppression de l'identité des usagers ou toutes autres personnes ne suffit pas à satisfaire aux exigences des lois applicables en matière d'utilisation et de divulgation des RP-RS sans consentement;
6. Je ne prêterai pas mes codes d'accès ou ma carte d'identité de l'Établissement à qui que ce soit et j'accepte l'entière responsabilité des actions effectuées avec mes accès. À cet égard, je respecterai l'ensemble des obligations mentionnées en **Annexe A** du présent engagement. Si je soupçonne que mes codes d'accès, dispositifs informatiques ou ma carte d'identité de l'Établissement, le cas échéant, ont été compromis ou volés, je contacterai immédiatement le service d'assistance de l'Établissement (demande.acces.service.securite.cisssmc16@ssss.gouv.qc.ca) pour obtenir de nouveaux codes, dispositifs informatiques ou une nouvelle carte;
7. (*Pour les membres du personnel et les personnes affiliées*) : Je m'engage à compléter les formations requises à mes fonctions/mon affiliation en lien avec la protection des RP-RS et à mettre à jour mes connaissances en cette matière tel qu'exigé par l'Établissement. Si mes fonctions/mon affiliation sont en lien avec le secteur de la recherche, je m'engage à compléter les formations portant sur les Modes opératoires normalisés, sur les bonnes pratiques cliniques et à respecter la *Politique sur la conduite responsable et l'intégrité scientifique en recherche*;
8. Je reconnais que toutes les informations et RP-RS présents sur les actifs informationnels de l'Établissement, y compris le contenu du courrier électronique et des outils collaboratifs (dont les échanges Teams), sont la propriété exclusive de l'Établissement. Je reconnais que l'utilisation de ces actifs informationnels est réservée à des fins professionnelles et que je ne peux conséquemment avoir d'expectative de vie privée dans le cadre de cette utilisation. Aussi, je reconnais et j'accepte que mon utilisation de ces actifs informationnels puisse faire l'objet d'un accès ou d'une surveillance de la part de l'Établissement, à des fins légitimes de gestion et/ou de sécurité, notamment conformément à sa *Politique de sécurité des ressources informationnelles*;
9. Je comprends que les RP-RS doivent demeurer sur les systèmes de l'Établissement ou dans ses limites physiques, sauf lorsque cela est expressément requis ou autorisé pour l'accomplissement de mes fonctions/de mon affiliation/de ma prestation contractuelle (par exemple, dans le cadre d'un projet de recherche ou d'un contrat de services). Cela inclut l'interdiction de faire des copies de RP-RS, sauf lorsque cela est expressément requis ou autorisé. **Dans tous les cas, je comprends qu'il est strictement interdit de prendre en photo des documents appartenant à des usagers avec des cellulaires ou avec tout autre appareil électronique ou de les enregistrer sur clé USB;**

10. Je protégerai contre toute utilisation ou divulgation non autorisée tous les RP-RS en ma possession et je veillerai à ce que seules les personnes dûment autorisées y accèdent. Si je prends connaissance d'une perte ou d'une divulgation non autorisée de RP-RS, **je m'engage à signaler l'incident, sans délai, selon les modalités prévues à la section 19.4.5 de la Politique de gouvernance des RP-RS (et reproduites en Annexe A)**, et à collaborer à toute démarche d'analyse, d'enquête ou de divulgation;
11. Indépendamment des changements qui pourraient affecter mon titre, mes fonctions, le statut de mon association ou les modalités contractuelles, je comprends et accepte que les termes du présent engagement continueront de s'appliquer et/ou seront maintenus indéfiniment;
12. **Je reconnais que tout manquement ou violation de la Politique de gouvernance des RP-RS pourrait faire l'objet d'un suivi ou d'une mesure disciplinaire ou administrative ainsi qu'un signalement déontologique ou aux autorités règlementaires compétentes.**
13. Le cas échéant, je reconnais que la signature du présent engagement par le biais d'un logiciel de signature électronique aura la même force et le même effet juridique qu'une signature manuscrite.

Par la présente, je reconnais avoir lu et compris les informations ci-dessus, et ma signature ci-dessous atteste de mon accord pour respecter les termes énoncés.

Nom, prénom : _____

Matricule d'employé, le cas échéant : _____

Signature : _____ Date : _____

RÉFÉRENCE : Entente de confidentialité - CISSSMO

Consultations : CAI-PRPRS – CISSSMC, CODIR-CISSMC, DRHDO, Direction de la recherche, DEAU, CMDPSF

Annexe A : Extraits de la Politique de gouvernance des RP-RS

Pour consulter la politique, veuillez utiliser les liens suivants :

<https://intranetciissmc.rtss.qc.ca/index.php?eID=dumpFile&t=f&f=23102&token=2f75202bc5229007b615ce7e897b22335b5a43ec>

<https://www.santemonteregie.qc.ca/sites/default/files/2024/11/politique-de-gouvernance-cissmc.pdf>

ANNEXE A : EXTRAIT DE LA POLITIQUE DE GOUVERNANCE DES RP-RS

19.4.1 Accès aux installations et aux actifs informationnels

(...)

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. Informar 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.

(...)

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).

(...)

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).