|  |  |
| --- | --- |
|  | **Évaluation des facteurs relatifs à la vie privée (EFVP)**Formulaire de demande de communication de renseignements personnels sans consentement à des fins d’étude, de recherche ou de production de statistiques  |

Informations préalables à l’intention du chercheur

Évaluation des facteurs relatifs à la vie privée (EFVP)

Une évaluation des facteurs relatifs à la vie privée (EFVP) doit être réalisée pour toute proposition de projet d’étude, de recherche ou de production de statistiques (ci-après nommé « projet ») impliquant d’accéder aux renseignements personnels d’usagers, renseignements personnels d’employés ou renseignements clinico-administratifs **sans le consentement** des personnes concernées et sous une forme qui permet leur **identification** ou leur **réidentification**.[[1]](#footnote-2) Tout projet concerné est soumis à une EFVP après sa triple évaluation par le comité d’éthique de la recherche (CER).

Cadre législatif

La Loi 25, soit la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, a été adoptée en septembre 2022. La Loi 25 a modifié plusieurs textes de loi, y compris la Loi sur les services de santé et les services sociaux (ci-après nommée « LSSSS ») et la Loi sur l’accès aux documents des organismes publics et sur la protection des renseignements personnels (ci-après nommée « Loi sur l’accès »). Les articles 67.2.1 à 67.2.3 de la Loi sur l’accès ainsi que l’article 19.2 de la LSSSS témoignent désormais de la nécessité de réaliser une EFVP.

L’EFVP vise à vérifier que le projet proposé est conforme à **cinq critères** (article 67.2.1 de la Loi sur l’accès) :

|  |  |
| --- | --- |
| Critère | Description |
| 1 | Il est déraisonnable d’exiger que la personne ou l’organisme obtienne le consentement des personnes concernées. |
| 2 | Seuls les renseignements nécessaires sont communiqués. |
| 3 | L’objectif de l’étude, de la recherche ou de la production de statistiques ne peut être atteint que si les renseignements sont communiqués sous une forme permettant d’identifier les personnes concernées. |
| 4 | Les renseignements personnels sont utilisés de manière à en assurer la confidentialité. |
| 5 | L’objectif de l’étude, de la recherche ou de la production de statistiques l’emporte, eu égard à l’intérêt public, sur l’impact de la communication et de l’utilisation des renseignements sur la vie privée des personnes concernées. |

En complément, le directeur des services professionnels (DSP) autorise les demandes d’accès aux dossiers des usagers à des fins de recherche (article 19.2 de la LSSSS).

Étapes de l’EFVP

Les tableaux qui suivent décrivent les étapes du processus d’EFVP applicables aux renseignements personnels d’usagers, d’employés et clinico-administratifs.

|  |  |  |
| --- | --- | --- |
| Étape | Description | Délai approximatif[[2]](#footnote-3) |
| 1 | Le chercheur responsable du projet remplit le présent formulaire et le transmet au CER. | ~ 3 semaines |
| 2 | Le CER transmet le formulaire, le protocole et l’approbation éthique du projet à une personne-ressource spécialisée en EFVP.  |
| 3 | La personne-ressource prend connaissance du formulaire EFVP et peut demander au chercheur d’y apporter des précisions et des modifications. |
| 4 | Une fois le formulaire EFVP complété, le comité EFVP évalue le projet.  |
| 5 | La personne-ressource fait un suivi de l’évaluation auprès du chercheur. Si nécessaire, elle lui demande des précisions supplémentaires et lui soumet des mesures de sécurité additionnelles exigées par le comité EFVP. Ces éléments sont ajoutés dans le formulaire EFVP. |
| 6 | Advenant que le projet ait été évalué favorablement et que le chercheur est d’accord avec les propositions additionnelles du comité EFVP, la personne-ressource invite le chercheur et l’établissement à signer une entente de communication des renseignements personnels. Le formulaire EFVP est joint à cette entente. |
| 7 | L’EFVP est transmise à la Commission d’accès à l’information. Celle-ci peut demander que des mesures supplémentaires soient prises en matière de protection des renseignements personnels. | >30 jours à partir de l’accusé de réception de la CAI |
| 8 | La personne formellement mandatée émet une lettre officialisant l’autorisation d’accéder aux renseignements personnels. | 1 journée, à l’issue de la période de >30 jours |
| 9 | Le chercheur accède aux renseignements personnels et en parallèle, le présent formulaire et l’entente sont transmis à la Commission d’accès à l’information. | N/A |

Complétion et transmission du formulaire

Veuillez remplir les sections du formulaire comportant le libellé **demandeur**. Certaines questions du présent formulaire sont redondantes avec des questions de la demande à faire au comité d’éthique de la recherche. Pour des raisons d’assurance de conformité légale, ceci est malheureusement inévitable. Cependant, **veuillez assurer la cohérence des informations fournies dans les deux demandes**.

Advenant que le projet proposé repose sur l’utilisation d’outils informatiques offerts par un établissement autre que le CCSMTL, le demandeur est responsable de fournir des attestations de la part du service informatique offrant ces outils quant à leur sécurité. Des précisions additionnelles sont données à la section 9.

Veuillez joindre le formulaire dûment rempli à l’endroit approprié de votre demande dans Nagano (pour les projets de recherche avec approbation éthique) ou le faire parvenir par courriel à l’adresse suivante : evaluation.projets.recherche.ccsmtl@ssss.gouv.qc.ca.

En cas de questions liées à la complétion du formulaire EFVP, veuillez contacter
Ariane Quintal (ariane.quintal.ccsmtl@ssss.gouv.qc.ca).

Structure du présent formulaire

Le présent formulaire contient les sections suivantes, la plupart devant être remplies par le demandeur.

1. Informations sur le demandeur (demandeur)
2. Informations sur l’EFVP (comité EFVP)
3. Informations générales sur le projet (demandeur)
4. Identification ou réidentification des participants (demandeur)
*Critère 3 de l’article 67.2.1 de la Loi sur l’accès*
5. Chercheurs et membres de l’équipe impliqués (demandeur)
6. Participants au projet (demandeur)
7. Renseignements demandés et justification (demandeur)
*Critère 2 de l’article 67.2.1 de la Loi sur l’accès*
8. Consentement déraisonnable à obtenir (demandeur)
*Critère 1 de l’article 67.2.1 de la Loi sur l’accès*
9. Protection de la confidentialité des renseignements (demandeur)
*Critère 4 de l’article 67.2.1 de la Loi sur l’accès*
10. Risques liés à la confidentialité des renseignements (demandeur + comité EFVP)
*Suite du critère 4 de l’article 67.2.1 de la Loi sur l’accès*
11. Intérêt public lié au traitement des renseignements (demandeur)
*Critère 5 de l’article 67.2.1 de la Loi sur l’accès*
12. Respect des critères de l’article 67.2.1 de la *Loi sur l’accès* (comité EFVP)
13. Signatures (comité EFVP et établissement)

# Informations sur le demandeur (demandeur)

## Identification du demandeur

|  |  |
| --- | --- |
| Nom |  |
| Fonction |  |
| Établissement(s) affiliés |  |
| Service/département |  |
| Adresse professionnelle |  |
| Courriel |  |
| Numéro de téléphone |  |

# Informations sur l’EFVP (comité EFVP)

## Numéro EFVP du projet

|  |
| --- |
|  |

## Date de l’évaluation

|  |
| --- |
|  |

## Évaluateurs

|  |  |  |  |
| --- | --- | --- | --- |
| Nom | Titre(s)  | Direction ou service | Rôle dans l’EFVP |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Directions de l’établissement concernées par la demande

|  |  |
| --- | --- |
| Direction  | Rôles et responsabilités |
|  |  |
|  |  |
|  |  |
|  |  |

# Informations générales sur le projet (demandeur)

## Titre du projet

|  |
| --- |
|  |

## Fins du projet

[ ]  Étude (p. ex. : qualité de l’acte)

[ ]  Enseignement

[ ]  Production de statistiques

[ ]  Recherche (avec approbation éthique)

[ ]  Vérification de l’éligibilité à des fins de recrutement

### S’il s’agit d’un projet de recherche :

Veuillez indiquer le numéro Nagano du projet.

|  |
| --- |
|  |

### Si le projet vise à vérifier l’éligibilité à des fins de recrutement :

Est-ce que les renseignements seront utilisés pour rejoindre les personnes concernées en vue de solliciter leur participation au projet? Si oui, veuillez préciser les informations qui seront communiquées à ces personnes.

|  |
| --- |
|  |

## Est-ce qu’il s’agit d’une nouvelle demande?

[ ]  Nouvelle demande

[ ]  Modification d’une demande existante

S’il s’agit d’une modification d’une demande existante, veuillez remplir uniquement les sections du formulaire visées par la modification.

## Autres EFVP

Veuillez mentionner tous les organismes ayant reçu une demande similaire **aux fins du même projet**, y compris le CCSMTL.

À titre indicatif, ces organismes peuvent inclure un établissement du réseau de la santé et des services sociaux, un organisme relevant du ministère de la Santé et des Services sociaux (p. ex., INSPQ), un ministère ou un organisme relevant du gouvernement du Québec ou une université.

|  |
| --- |
|  |

## Contexte et description du projet

Veuillez décrire les grandes lignes du projet, incluant le contexte justifiant sa réalisation. S’il y a lieu, veuillez distinguer le projet faisant l’objet de l’EFVP (p. ex., étude préliminaire) du projet plus large dans lequel il s’inscrit.

|  |
| --- |
|  |

## Objectifs du projet

Veuillez préciser les objectifs du projet et s’il y a lieu, les distinguer de ceux du projet plus large.

|  |
| --- |
|  |

# Identification ou réidentification des participants (demandeur)Critère 3 de l’article 67.2.1 de la Loi sur l’accès

## Niveau d’identification des renseignements

Veuillez cocher **le niveau le plus identifiable** de renseignements que vous traiterez lors du projet.[[3]](#footnote-4)

Par exemple, si vous traitez **des renseignements nominaux** lors de la consultation desdossiers, même si ceux-ci sont ensuite dépersonnalisés ou anonymisés, vous devez cocher **« renseignements nominaux »**.

[ ]  Renseignements nominaux

[ ]  Renseignements dénominalisés

[ ]  Renseignements anonymisés

[ ]  Renseignements agrégés

En cas de difficultés dans la détermination du niveau d’identification, veuillez communiquer avec : evaluation.projets.recherche.ccsmtl@ssss.gouv.qc.ca.

## Renseignements personnels

Conformément à la question précédente, veuillez indiquer si vous traiterez des renseignements personnels. À titre indicatif, « (…) sont personnels les renseignements qui concernent une personne physique et permettent de l’identifier » *(Loi sur l’accès, article 54)*.

|  |
| --- |
|  |

Si vous traitez uniquement des renseignements **anonymisés** ou **agrégés** (c.-à-d., qui ne sont pas des renseignements personnels), vous n’avez pas besoin de remplir le présent formulaire.

## Niveau d’identification des renseignements personnels[[4]](#footnote-5)

Veuillez expliquer en quoi l’objectif de l’étude, de la recherche ou de la production de statistiques ne peut être atteint que si les renseignements sont communiqués sous une forme permettant d’identifier les personnes concernées.

|  |
| --- |
|  |

# Chercheurs et membres de l’équipe impliqués (demandeur)

## Personnes qui traiteront les renseignements sous leurs différentes formes

Veuillez indiquer les informations des chercheurs et des membres de l’équipe de recherche qui traiteront les renseignements.[[5]](#footnote-6)

Note : Pendant la réalisation du projet, si la liste de personnes qui traitent les renseignements change, veuillez faire parvenir la mise à jour de la liste par courriel à evaluation.projets.recherche.ccsmtl@ssss.gouv.qc.ca.

|  |  |  |
| --- | --- | --- |
| Nom | Titre(s) d’emploi et affiliation(s)  | Rôle(s) lié(s) aux renseignements  |
|  |  |  |
|  |  |  |
|  |  |  |

# Participants au projet (demandeur)

## Personnes concernées par le projet

Veuillez indiquer le nombre de personnes dont les renseignements seront traités dans le cadre du projet ou un ordre de grandeur général. Veuillez également préciser les caractéristiques générales de ces personnes (p. ex., clientèle de quel service).

|  |
| --- |
|  |

## Critères d’inclusion

Veuillez indiquer les critères d’inclusion qui seront utilisés pour identifier les personnes dont les renseignements seront traités dans le cadre du projet (p. ex., âge, sexe, diagnostic, traitement).

|  |
| --- |
|  |

## Période couverte

Veuillez indiquer la période couverte par les renseignements que vous traiterez (p. ex., dossiers des usagers XYZ du 1er janvier 2000 au 31 décembre 2005).

|  |
| --- |
|  |

# Renseignements demandés et justification (demandeur) Critère 2 de l’article 67.2.1 de la Loi sur l’accès

## Source des renseignements

De quelle(s) source(s) proviendront les renseignements? Veuillez cocher toutes les sources applicables.

[ ]  Biobanque (données d’analyses d’échantillons)

Veuillez identifier et décrire la ou les biobanque(s), s’il y a lieu :

|  |
| --- |
|  |

[ ]  Registre de patients (p. ex., registre québécois du cancer)

Veuillez identifier et décrire le(s) registre(s), s’il y a lieu :

|  |
| --- |
|  |

[ ]  Systèmes d’information de l’établissement ou bases de données de services cliniques colligées ou non dans un formulaire de collecte ou Case Report Form (CRF) (p. ex., Oacis, I-CLSC, SIC-SRD, SIPAD, PIJ, etc.)

Veuillez identifier et décrire le(s) système(s) d’information ou base(s) de données, s’il y a lieu :

|  |
| --- |
|  |

[ ]  Dossiers des usagers disponibles en format papier seulement et conservés au service des archives et information clinique

Veuillez préciser, s’il y a lieu :

|  |
| --- |
|  |

[ ]  Dossiers des employés ou systèmes d’information du CCSMTL contenant des informations sur les employés

Veuillez préciser, s’il y a lieu :

|  |
| --- |
|  |

[ ]  Autre(s)

Veuillez préciser, s’il y a lieu :

|  |
| --- |
|  |

## Directions, services, pilotes ou personnes-ressources donnant accès aux renseignements

Veuillez nommer les directions, les services, les pilotes ou les personnes-ressources qui donneront accès aux renseignements compris dans les sources décrites à la question précédente.

|  |
| --- |
|  |

## Inventaire de renseignements et justification

Afin de réduire les risques associés à l’accès aux renseignements, il est essentiel d’accéder uniquement aux renseignements nécessaires.

Ainsi, dans cette section, veuillez fournir la liste des renseignements qui seront traités dans le cadre du projet. Cette liste doit être complète, valide, justifiée et cohérente pour répondre aux exigences du cadre législatif :

* **Complète**:La liste doit comprendre *tous* les renseignements qui seront traités ;
* **Valide**: Les renseignements énumérés dans cette liste doivent être véritablement disponibles dans le système d’information concerné. À cette fin, veuillez valider, corriger et enrichir cette liste auprès des directions, des services, des pilotes ou des personnes-ressources concernés du CCSMTL ;
* **Justifiée**: La collecte des renseignements énumérés dans la liste doit être justifiée. Plus spécifiquement, une justification doit être fournie pour chaque renseignement *nominal[[6]](#footnote-7)* ou *sensible* (c.-à-d., de nature délicate ou intime). Une justification doit être fournie pour chaque *catégorie* de renseignements semblables (p. ex., plusieurs renseignements sur la composition d’une famille).

|  |  |  |
| --- | --- | --- |
| Catégories et exemples de renseignements  | Renseignements visés  | Justifications appropriées |
| NomExemples :* Prénom et nom
* Initiales
 | *
*
*
 |  |
| Codes d’identificationExemples :* Numéro de dossier médical
* Numéro de bénéficiaire du plan de santé
* Numéro de certificat/licence
 | *
*
*
 |  |
| CoordonnéesExemples :* Adresse postale
* Adresse courriel
* Numéro de téléphone
* Ville, comté, quartier, code postal complet
 | *
*
*
 |  |
| DatesExemples :* Date de naissance
* Date de décès
* Dates liées à la prise en charge médicale (p. ex., date d’admission, date de diagnostic, date de décès)
 | *
*
*
 |  |
| Renseignements sociodémographiques* Classe d’âge
* Sexe/genre
* Statut conjugal
* Revenu
* Occupation
* Ethnicité
* Religion
 | *
*
*
 |  |
| Renseignements médicauxExemples :* Diagnostic ou code diagnostique
* Résultat de prise de sang
* Intervention médicale reçue
* Classement sur une échelle liée à la condition médicale
* Résultats de tests d’évaluation réalisés par un professionnel de la santé (p. ex., ergothérapie, physiothérapie, psychologie, psychiatrie, travail social)
* Tout autre renseignement concernant une maladie, une affectation, un problème ou un besoin lié à la santé physique, psychologique et développementale
 | *
*
*
 |  |
| Renseignements psychosociauxExemples :* Composition de la famille
* Antécédents de problématiques présentes dans la famille
* Qualité des liens entre les membres de la famille
* Événements dans la trajectoire de placement
* Renseignements liés à une démarche d’adoption
 | *
*
*
 |  |
| Renseignements scolairesExemples:* Écoles fréquentées
* Résultats scolaires
* Difficultés scolaires
* Classes spéciales fréquentées
 | *
*
*
 |  |
| Renseignements d’emploiSurtout en cas de renseignements provenant d’employésExemples :* Matricule
* Titre d’emploi
* Formation et diplômes
* Ancienneté
* Quart de travail
 | *
*
*
 |  |
| Renseignements phénotypiquesExemples :* Identifiants biométriques (incluant empreintes digitales et vocales)
* Photographies de face et toutes images comparables
 | *
*
*
 |  |
| Renseignements technologiquesExemples :* Localisateur universel de ressource Web (URL)
* Adresse de protocole internet (IP)
 | *
*
*
 |  |
| Autres renseignements  |  |  |

# Consentement déraisonnable à obtenir (demandeur) Critère 1 de l’article 67.2.1 de la Loi sur l’accès

## Déraisonnable d’obtenir le consentement

Veuillez donner toutes les raisons pour lesquelles il est déraisonnable d’obtenir le consentement des personnes concernées dans le cadre du projet.

Veuillez noter que des raisons comme la facilité du processus d'accès sans consentement via la présente procédure d’EFVP, la lourdeur administrative liée à l'obtention du consentement, la crainte d'un refus (ou toute autre justification similaire) **ne sont pas suffisantes** pour justifier l'impossibilité d'obtenir le consentement.

|  |
| --- |
|  |

# Protection de la confidentialité des renseignements (demandeur) Critère 4 de l’article 67.2.1 de la Loi sur l’accès

Dans cette section, veuillez décrire :

* Les **approches** dont vous vous servirez pour traiter les renseignements tout au long de leur cycle de vie (collecte, utilisation, communication, conservation, destruction) ;
* Les **mesures de sécurité** que vous mettrez en place lors de chacune de ces étapes pour assurer la confidentialité des renseignements.

Plusieurs questions et exemples vous guideront à fournir ces informations.

Astuces pour bien remplir cette section

* Veuillez fournir des explications détaillées et vulgarisées pour permettre aux membres du comité EFVP dotés de profils diversifiés de bien comprendre la manière dont les renseignements seront traités tout au long de leur cycle de vie.
* Veuillez valider préalablement l’approche prévue auprès des directions, des services, des pilotes ou des personnes-ressources concernés pour assurer qu’elle soit cohérente avec le soutien et les renseignements qu’ils peuvent offrir. En cas de doute, veuillez contacter le comité d’éthique pour être dirigé vers la bonne personne-ressource.
* Si cette approche implique d’avoir recours à un outil informatique qui n’est pas offert par le CCSMTL, veuillez fournir une attestation écrite de la part du service informatique qui en est responsable confirmant qu’il est sécuritaire et qu’il protège les renseignements selon les lois en vigueur. Cette attestation doit être transmise en accompagnement au formulaire.

En plus des mesures de sécurité spécifiques à ce projet, des mesures organisationnelles visant à sécuriser les renseignements qui sont sous la responsabilité du CCSMTL et à protéger la vie privée des personnes sont mises en place en tout temps au sein de l’établissement. Veuillez consulter l’annexe 2 pour une description plus détaillée de ces mesures.

Enfin, le comité EFVP se réserve le droit de demander que des mesures de sécurité supplémentaires soient prises au cours du cycle de vie des renseignements personnels. Le cas échéant, il en vous fera part.

Les questions suivent à la prochaine page.

## Collecte des renseignements

La collecte de renseignements peut désigner deux cas de figure, soit : (1) l’accès aux renseignements et leur extraction par **le chercheur**; ou (2) l’extraction et le transfert des renseignements **par l’établissement** vers le chercheur.

### Veuillez indiquer qui réalisera la collecte de renseignements, ce qui inclut leur consultation et leur extraction.

[ ]  Chercheur et son équipe de recherche (→ veuillez répondre à la question)

[ ]  Directions, services, pilotes ou personnes-ressources du CCSMTL (→ veuillez répondre à la question d’après sur l’*établissement*)

### Veuillez fournir des informations sur la collecte escomptée des renseignements par le *chercheur et son équipe de recherche* (c.-à-d., accès et extraction) ainsi que les mesures de sécurité qui seront mises en place.

|  |  |  |  |
| --- | --- | --- | --- |
| # | Questions | Mesures de sécurité attendues, lorsqu’applicables | Réponses aux questions et mesures de sécurité qui seront mises en place |
| 9.1.1 | L’accès aux renseignements s’effectuera-t-il sur place ou à distance?* S’ils seront sur place, dans quelle installation du CCSMTL se trouveront-ils?
 | * Consulter les renseignements avec/sur une ressource sécurisée accessible par authentification avec un nom d’utilisateur et un mot de passe
* Consulter et collecter uniquement les renseignements nécessaires pour répondre aux objectifs du projet
* Anonymiser ou dépersonnaliser les renseignements autant que possible lors de la collecte
* Collecter les renseignements dans un fichier chiffré et protégé par un mot de passe qui est entreposé sur une ressource informatique sécurisée
* Dans le cas de renseignements dénominalisés, conserver la clé de correspondance sur une ressource informatique sécuriséeet différente de l’endroit où les renseignements dénominalisés sont entreposés
 |  |
| 9.1.2 | Quels sont le matériel et les ressources informatiques qui seront utilisés pour extraire les renseignements?* Exemples : VPN, authentification sécurisée par nom d’utilisateur et mot de passe, ordinateurs du CCSMTL, serveur du CCSMTL ou d’un autre établissement, ordinateur d’un autre établissement, etc.
 |
| 9.1.3 | Dans quel(s) type(s) de fichier les renseignements seront-ils extraits? |
| 9.1.4 | Qui sont les personnes-ressources du CCSMTL qui donneront accès aux locaux, au matériel et aux ressources informatiques nécessaires à la collecte? | * Signature d’un engagement à la confidentialité et à la protection des renseignements par le chercheur et tous les membres de son équipe
* Limiter le nombre de membres de l’équipe qui consultent ou collectent des renseignements.
* Utiliser une authentification par nom d’utilisateur et mot de passe pour limiter et contrôler l’accès à l’environnement et au poste de travail
* Limiter l’accès à la clé de correspondance au chercheur responsable du projet ou à une personne-ressource précise
 |  |
| 9.1.5 | Qui seront les membres de l’équipe de recherche qui seront impliqués dans la collecte des renseignements et quels seront leurs rôles et leurs responsabilités? |
| 9.1.6 | Des autorisations légales sont-elles nécessaires pour débuter la collecte?* Si oui, quelles sont-elles?
* Ces autorisations ont-elles déjà été obtenues? Sinon, à quel moment seront-elles obtenues?
 | * Disposer des autorisations légales nécessaires pour réaliser la collecte de données
 |  |
| 9.1.7 | Quelle est la période prévue pour la collecte des renseignements? | * N/A
 |  |
| 9.1.8 | Autres précisions sur la méthodologie de collecte de renseignements (accès et extraction) | * N/A
 |  |

### Veuillez fournir des informations sur la collecte escomptée des renseignements par l’établissement (c.-à-d., extraction et transfert) ainsi que les mesures de sécurité qui seront mises en place.

|  |  |  |  |
| --- | --- | --- | --- |
| # | Questions | Mesures de sécurité attendues, lorsqu’applicables | Réponses aux questions et mesures de sécurité qui seront mises en place |
| 9.1.9 | Dans quel type de fichier les renseignements seront-ils extraits? | * Collecter uniquement les renseignements nécessaires pour répondre aux objectifs du projet
* Anonymiser ou dépersonnaliser les renseignements autant que possible lors de la collecte
* Collecter les renseignements dans un fichier chiffré et protégé par un mot de passe qui est entreposé sur une ressource informatique sécurisée
* Dans le cas de renseignements dénominalisés, conserver la clé de correspondance sur une ressource informatique sécuriséeet différente de l’endroit où les renseignements dénominalisés sont entreposés
 |  |
| 9.1.10 | Qui sont les personnes-ressources qui superviseront ou qui réaliseront l’extraction et le transfert des renseignements ? Quels sont les rôles exacts de chacune de ces personnes? | * N/A
 |  |
| 9.1.11 | Quelle est la méthodologie qui sera utilisée par une direction ou un service du CCSMTL pour transférer les renseignements au chercheur?Voici quelques exemples de méthodes qui peuvent être utilisées :* Protocole de communication sécurisé pour transférer des renseignements cryptés
* Plateforme collaborative accessible par le Web dont l’accès est régi par une authentification par nom d’utilisateur et mot de passe (p. ex., RedCap)
* Système informatique sécurisé du CCSMTL ou d’un autre établissement auquel le chercheur est affilié

Si l’utilisation d’un outil collaboratif M365 (p. ex., OneDrive ou Teams) du réseau de la santé est incontournable pour le transfert des renseignements, veuillez expliquer pourquoi d’autres alternatives ne peuvent pas être adoptées.[[7]](#footnote-8) |  |
| 9.1.12 | Autres précisions sur la méthodologie de collecte de renseignements | N/A |  |

## Utilisation des renseignements

L’utilisation des renseignements réfère à leur transformation à des fins d’analyse pour répondre à l’objectif du projet.

### Veuillez fournir des informations concernant l’utilisation escomptée des renseignements ainsi que les mesures de sécurité qui seront mises en place.

|  |  |  |  |
| --- | --- | --- | --- |
| # | Questions | Mesures de sécurité attendues, lorsqu’applicables | Réponses aux questions et mesures de sécurité qui seront mises en place |
| 9.2.1 | Quelles opérations seront effectuées sur les renseignements (p. ex., statistiques descriptives, tests statistiques, analyses thématiques et qualitatives)? Un aperçu général est suffisant. | * Signature d’un engagement à la confidentialité et à la protection des renseignements par le chercheur et tous les membres de son équipe
* Utilisation des renseignements qu’aux seules fins du projet, tel qu’indiqué dans l’engagement à la confidentialité et à la protection des renseignements que signeront le chercheur et les membres de son équipe
* Limiter le nombre de membres de l’équipe qui utilisent les renseignements
* Renseignements analysés dans un fichier chiffré et protégé d’un mot de passe
 |  |
| 9.2.2 | En quoi cette utilisation des renseignements permettra-t-elle d’atteindre les objectifs du projet? | * Analyser uniquement les renseignements nécessaires pour répondre aux objectifs du projet
 |  |
| 9.2.3 | Veuillez indiquer quelles seront la ou les plateforme(s) qui seront utilisées pour manipuler les renseignements.Si l’utilisation d’un outil collaboratif M365 (p. ex., OneDrive ou Teams) du réseau de la santé est incontournable pour manipuler les renseignements, veuillez expliquer pourquoi d’autres alternatives ne peuvent pas être adoptées. | Voici quelques exemples de plateformes recommandées pour la manipulation des renseignements :* Système informatique sécurisé du CCSMTL
* Systèmes informatiques sécurisés d’un autre établissement auquel vous êtes affilié
* Services infonuagiques offrant un hébergement de données au Canada reconnus par des établissements, des universités ou des institutions québécois (p. ex., Redcap, UdeM, LimeSurvey)
* Outils collaboratifs (p. ex., M365) du réseau de la santé et des services sociaux, si aucune autre alternative n’existe et que le travail collaboratif sur un document commun en temps réel est incontournable[[8]](#footnote-9)

Mesures de sécurité complémentaires :* Signature d’un engagement à la confidentialité et à la protection des renseignements par le chercheur et tous les membres de son équipe
* Protéger et chiffrer le fichier contenant les renseignements
* Manipuler les renseignements dans un répertoire dont l’accès est limité à un nombre limité de membres de l’équipe de recherche
* Manipuler les renseignements nominaux dans un fichier contenant une clé de correspondance
* Limiter l’accès au fichier contenant la clé de correspondance au chercheur responsable du projet ou à une personne-ressource précise
* Limiter au minimum le nombre de fichiers contenant les renseignements
 |  |
| 9.2.4 | Veuillez préciser la nature du poste de travail qui sera utilisé pour manipuler les renseignements (p. ex., ordinateur de l’établissement, ordinateur d’un autre établissement, ordinateur personnel). S’il y a lieu, veuillez justifier l’utilisation d’un ordinateur personnel.Veuillez indiquer si les renseignements seront manipulés localement sur cet ordinateur et le justifier le cas échéant. | Ordinateurs : * Il est recommandé d’utiliser un ordinateur prêté par l’établissement plutôt qu’un ordinateur personnel.
* Si l’utilisation d’un ordinateur personnel est envisagée, veuillez expliquer pourquoi d’autres alternatives ne peuvent pas être adoptées.
* Il est déconseillé de manipuler les renseignements localement sur l’ordinateur.

Mesures de sécurité complémentaires :* Accéder au poste de travail à l’aide d’une authentification avec un nom d’utilisateur et un mot de passe
 |  |

## Communication de renseignements

La communication de renseignements réfère à l’envoi de renseignements du chercheur vers un ou des collaborateur(s) externe(s) à son établissement.

### Veuillez indiquer si les renseignements seront communiqués à un ou des collaborateur(s) externe(s) sous format nominal ou dénominalisé.

[ ]  Oui (→ veuillez répondre aux questions 9.3.1 à 9.3.3)

[ ]  Non (→ veuillez passer à la question 9.4)

Si les renseignements sont transmis à un ou des collaborateur(s) externe(s) sous forme agrégée ou anonymisée, il n’est pas nécessaire de remplir la présente section.

### Veuillez fournir des informations sur la communication escomptée des renseignements à un ou des collaborateur(s) externe(s) ainsi que les mesures de sécurité qui seront mises en place.

|  |  |  |  |
| --- | --- | --- | --- |
| # | Questions | Mesures de sécurité attendues, lorsqu’applicables | Réponses aux questions et mesures de sécurité qui seront mises en place |
| 9.3.1 | Quelle est l’utilité de communiquer les renseignements à un ou des collaborateur(s) externe(s)? | Mesures de sécurité applicables :* Signature d’un engagement à la confidentialité et à la protection des renseignements par le chercheur et tous les membres de son équipe
* Signature d’une entente de transfert de données (ou *data transfer agreement*) entre l’établissement, le chercheur et le collaborateur externe qui prévoit des mesures de sécurité équivalentes à celles mentionnées plus haut
* Limiter le nombre de collaborateurs externes visés par la communication des renseignements.
 |  |
| 9.3.2 | Qui sont le(s) collaborateur(s) externes vers lesquels le chercheur communiquera les renseignements? |  |
| 9.3.3 | Quelle est la méthodologie qui sera utilisée pour communiquer les renseignements vers un ou des collaborateur(s) externe(s)?Voici quelques exemples de méthodes qui peuvent être utilisées :* Système informatique sécurisé du CCSMTL
* Systèmes informatiques sécurisés d’un autre établissement auquel vous êtes affilié
* Services infonuagiques hébergés au Canada
* Outils collaboratifs M365, incluant OneDrive ou Teams, fournis au personnel du réseau de la santé, si aucune alternative n’est possible

En complément, voici quelques exemples de méthodes déconseillées pour communiquer les renseignements vers un ou des collaborateur(s) externe(s) :* Systèmes informatiques sécurisés personnels
* Courriel envoyé au sein du CCSMTL ou à l’extérieur du CCSMTL[[9]](#footnote-10)
* Services infonuagiques pas hébergés au Canada
* Outils collaboratifs (p. ex., M365, Google Drive) associés à un compte personnel

Si l’utilisation d’un outil collaboratif M365 (p. ex., OneDrive ou Teams) du réseau de la santé est incontournable pour la communication des renseignements personnels, veuillez expliquer pourquoi d’autres alternatives ne peuvent pas être adoptées. |  |

## Conservation des renseignements

La conservation des renseignements réfère à leur entreposage sur un serveur sécurisé pendant la durée du projet, puis pendant le délai de conservation (habituellement de 5 à 7 ans) exigé par l’établissement, l’université ou l’agence subventionnaire.

### Veuillez fournir des informations concernant la conservation escomptée des renseignements ainsi que les mesures de sécurité qui seront mises en place.

|  |  |  |  |
| --- | --- | --- | --- |
| # | Question | Mesures de sécurité attendues, lorsqu’applicables | Réponses aux questions et mesures de sécurité qui seront mises en place |
| 9.4.1 | Veuillez indiquer quelles seront la ou les plateforme(s) qui seront utilisées pour conserver les renseignements.Si l’utilisation d’un outil collaboratif M365 (p. ex., OneDrive ou Teams) du réseau de la santé et des services sociaux est incontournable pour conserver les renseignements, veuillez expliquer pourquoi d’autres alternatives ne peuvent pas être adoptées. | Voici quelques exemples de plateformes recommandées pour la conservation des renseignements:* Système informatique sécurisé du CCSMTL
* Systèmes informatiques sécurisés d’un autre établissement auquel vous êtes affilié
* Services infonuagiques offrant un hébergement de données au Canada reconnus par des établissements, des universités ou des institutions québécois (p. ex., Redcap, UdeM, LimeSurvey)

Voici quelques exemples de plateformes déconseillées pour la conservation des renseignements :* Outils collaboratifs (p. ex., M365) du réseau de la santé et des services sociaux[[10]](#footnote-11)

Voici quelques exemples de plateformes fortement déconseillées pour la conservation des renseignements :* Systèmes informatiques sécurisés personnels
* Outils collaboratifs (p. ex., M365, Google Drive) associés à un compte personnel
* Services infonuagiques n’hébergeant pas les données au Canada

Mesures de sécurité complémentaires :* Signature d’un engagement à la confidentialité et à la protection des renseignements par le chercheur et tous les membres de son équipe
* Protéger et chiffrer le fichier contenant les renseignements
* Conserver les renseignements dans un répertoire dont l’accès est limité à un nombre limité de membres de l’équipe de recherche
* Dépersonnaliser, agréger ou anonymiser autant que possible les renseignements pendant leur durée de conservation
* Conserver les renseignements nominaux dans un fichier contenant la clé de correspondance
* Limiter l’accès au fichier contenant la clé de correspondance au chercheur responsable du projet ou à une personne-ressource précise
* Limiter au minimum le nombre de lieux d’hébergement pour les renseignements
* Limiter au minimum le nombre de fichiers contenant les renseignements
 |  |
| 9.4.2 | Veuillez préciser la nature du poste de travail qui sera utilisé pour conserver les renseignements (p. ex., ordinateur de l’établissement, ordinateur d’un autre établissement, ordinateur personnel). S’il y a lieu, veuillez justifier l’utilisation d’un ordinateur personnel.Veuillez indiquer si les renseignements seront conservés localement sur cet ordinateur et le justifier le cas échéant. | Ordinateurs : * Il est recommandé d’utiliser un ordinateur prêté par l’établissement plutôt qu’un ordinateur personnel.
* Si l’utilisation d’un ordinateur personnel est envisagée pour conserver les renseignements, veuillez expliquer pourquoi d’autres alternatives ne peuvent pas être adoptées.
* Il est déconseillé de conserver les renseignements localement sur l’ordinateur.

Supports amovibles : * L’utilisation de supports amovibles est déconseillée. Si leur utilisation est incontournable, veuillez expliquer pourquoi.
* Advenant qu’un support amovible soit utilisé, il doit être conservé sous clé dans un lieu sécuritaire (p. ex., établissement) lorsqu’il n’est pas utilisé.
* Le fichier enregistré sur le support amovible qui contient les renseignements doit être chiffré et protégé d’un mot de passe.

Mesures de sécurité complémentaires :* Accéder au poste de travail à l’aide d’une authentification avec un nom d’utilisateur et un mot de passe.
 |  |
| 9.4.3 | Qui seront les membres de l’équipe impliqués dans la conservation des renseignements et quels seront leurs rôles et leurs responsabilités? | * Limiter le nombre de membres de l’équipe qui auront accès aux renseignements pendant leur durée complète de conservation.
 |  |
| 9.4.4 | Quelle sera la durée de conservation des renseignements une fois le projet terminé? | * Conserver le fichier maître contenant les renseignements pendant 5 à 7 ans après la fin de l’étude si exigé par l’agence subventionnaire.
 |  |

## Destruction des renseignements

La destruction des renseignements comprend leur suppression à la fin du délai de conservation ainsi que la suppression des renseignements qui ne sont plus utiles au cours de la réalisation du projet (voir question précédente).

### Veuillez fournir des informations sur la destruction des renseignements ainsi que sur les mesures de sécurité qui seront mises en place.

|  |  |  |  |
| --- | --- | --- | --- |
| # | Question | Mesures de sécurité attendues, lorsqu’applicables | Réponses aux questions et mesures de sécurité qui seront mises en place |
| 9.5.1 | De quelle manière les renseignements seront-ils détruits? | * Supprimer les copies du fichier maître utilisées pour réaliser des analyses dès que celles-ci ne sont plus utilisées
* Si les renseignements sont publiés de manière agrégée en soutien à un article scientifique, veiller à ce que tout renseignement nominatif ou dénominalisé soit enlevé du jeu de données.
* Vider la corbeille une fois que les renseignements ont été supprimés.
 |  |

## Stratégies pour minimiser la quantité et la sensibilité des renseignements traités

Tout au long du cycle de vie des renseignements (c.-à-d., collecte, utilisation, communication, conservation et destruction), plusieurs stratégies peuvent être prises pour réduire le nombre, le niveau de précision et le niveau d’identification des renseignements conservés.

En vous inspirant des exemples donnés dans le tableau ci-dessous, veuillez décrire lorsqu’applicable (1) les stratégies qui seront mises en place pour minimiser la quantité et la sensibilité des renseignements conservés ainsi que (2) l’étape ou les étapes du cycle de vie où elles seront mises en place.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Type de stratégie | Exemples | Stratégie(s) qui seront mis(es) en place lorsqu’applicable(s) | Étape(s) du cycle de vie concernée(s), le cas échéant |
| 9.6.1 | Réduction du nombre de renseignements | * Supprimer le numéro de dossier de la base de données : Des renseignements sur les mêmes usagers pourraient être extraits à partir de deux systèmes d’information et le numéro de dossier pourrait être utilisé pour apparier les renseignements. Une fois l’appariement effectué, le numéro de dossier pourrait être supprimé et remplacé par un code d’identification fictif.
 |  |  |
| 9.6.2 | Réduction du niveau de précision | * Supprimer la date de naissance, mais conserver l’âge : La date de naissance pourrait initialement être extraite pour calculer l’âge de l’usager à divers moments de sa trajectoire de soins. Une fois ces calculs effectués, la date de naissance pourrait être supprimée.
 |  |  |
| 9.6.3 | Réduction du niveau d’identification[[11]](#footnote-12) | * Conserver les renseignements nominaux dans un fichier de type « clé de correspondance » : Un code d’identification fictif pourrait être attribué aux usagers dans la base de données. L’association entre le nom et le code d’identification fictif pourrait être conservée dans un fichier de type « clé de correspondance » entreposé dans un autre répertoire que la base de données.
* Anonymisation : Une fois les analyses réalisées, toutes les informations sensibles et permettant la réidentification des usagers pourraient être supprimées. La base de données en découlant serait donc anonymisée. Note : Il est rare qu’une base de données soit parfaitement anonymisée.
* Agrégation : Une fois les analyses réalisées, seuls les résultats agrégés pourraient être conservés.
 |  |  |

# Risques liés à la confidentialité des renseignements (demandeur) Suite du critère 4 de l’article 67.2.1 de la Loi sur l’accès

## Identification et évaluation des risques

Dans le tableau qui suit, veuillez identifier les risques présents à chaque étape du cycle de vie des renseignements personnels. Puis, veuillez attribuer un niveau de risque résiduel à chaque étape du cycle de vie, soit nul, très faible, faible, moyen, élevé ou très élevé. Un niveau de risque résiduel correspond au niveau de risque présent après la prise en compte des mesures de sécurité énoncées à la section 9. Enfin, veuillez indiquer la moyenne du niveau de risque résiduel en vous appuyant sur les niveaux énoncés pour chaque étape du cycle de vie des renseignements.

Ensuite, le comité EFVP révisera cette section et se réserve le droit de modifier les risques identifiés et l’évaluation des risques.

|  |  |  |
| --- | --- | --- |
| Étape du cycle de vie des renseignements | Identification des risques | Évaluation du niveau de risque résiduel |
| Collecte\* | Accès et extraction par le chercheur et l’équipe de recherche | Extraction et transfert par l’établissement |  |
| [ ]  N/A[ ]  Accès ou extraction de renseignements non nécessaires ou non autorisés pour le projet[ ]  Accès ou extraction non autorisés de renseignements[ ]  Identification ou réidentification de personnes[ ]  Perte ou vol de renseignements[ ]  Conflit de rôles | [ ]  N/A[ ]  Extraction ou transfert de renseignements non nécessaires ou non autorisés pour le projet[ ]  Extraction ou transfert non autorisés de renseignements[ ]  Identification ou réidentification de personnes[ ]  Perte ou vol de renseignements |
| [ ]  Autre (veuillez spécifier) : | [ ]  Autre (veuillez spécifier) : |
| Utilisation | [ ]  Utilisation de renseignements non nécessaires ou non autorisés pour le projet[ ]  Utilisation non autorisée de renseignements[ ]  Identification ou réidentification de personnes[ ]  Perte ou vol de renseignements[ ]  Conflit de rôles |  |
| [ ]  Autre (veuillez spécifier) : |
| Communication | [ ]  Communication de renseignements non nécessaires ou non autorisés pour le projet[ ]  Communication non autorisée de renseignements[ ]  Identification ou réidentification de personnes[ ]  Perte ou vol de renseignements[ ]  Conflit de rôles[ ]  Conservation des renseignements au-delà du délai de conservation ou lorsque leur utilité n’est plus démontrée |  |
| [ ]  Autre (veuillez spécifier) : |
| Conservation et destruction | [ ]  Conservation de renseignements non nécessaires ou non autorisés pour le projet[ ]  Conservation non autorisée de renseignements[ ]  Identification ou réidentification de personnes[ ]  Perte ou vol de renseignements[ ]  Conflit de rôles[ ]  Conservation des renseignements au-delà du délai de conservation ou lorsque leur utilité n’est plus démontrée[ ]  Destruction inadéquate ou non définitive des renseignements |  |
| [ ]  Autre (veuillez spécifier) : |
| **Moyenne approximative du niveau de risque résiduel :**  |  |
| \* Collecte : Veuillez seulement remplir la colonne appropriée. Autrement, veuillez cocher N/A. |

# Intérêt public lié au traitement des renseignements (demandeur) Critère 5 de l’article 67.2.1 de la Loi sur l’accès

## Légitimité de l’objectif ou des objectifs

Veuillez expliquer en quoi l’objectif ou les objectifs du projet (ou du sous-projet, le cas échéant) sont légitimes et répondent à des préoccupations ou des besoins d’intérêt public qui sont réels et justifiables.

|  |
| --- |
|  |

## Primauté de l’intérêt public sur l’impact de l’accès aux renseignements

Veuillez également expliquer comment l’intérêt public du projet l’emporte sur l’impact du traitement des renseignements sur la vie privée des personnes concernées, tout en tenant compte de la moyenne du niveau de risque résiduel (voir question 10.1).

|  |
| --- |
|  |

# Respect des critères de l’article 67.2.1 de la *Loi sur l’accès* (comité EFVP)

L’analyse du respect des critères de l’article 67.2.1 de la *Loi sur l’accès* a été effectuée par le comité EFVP en tenant compte :

* Des informations transmises par le chercheur responsable du projet, y compris sur les moyens prévus pour protéger la confidentialité des renseignements;
* Des discussions ayant mobilisé les expertises des membres du comité EFVP;
* Si nécessaire, d’avis sollicités de la part de directions, de services, de pilotes et de personnes-ressources du CCSMTL concernés par la demande.

En s’appuyant sur ces informations, le comité EFVP se prononce comme suit :

|  |  |  |  |
| --- | --- | --- | --- |
| Critère | Section | Description du critère de l’article 67.2.1 | Verdict du comité EFVP |
| Oui | Non |
| 1 | 8 | Il est déraisonnable d’exiger que la personne ou l’organisme obtienne le consentement des personnes concernées. | [ ]  | [ ]  |
| 2 | 7 | Seuls les renseignements nécessaires sont communiqués. | [ ]  | [ ]  |
| 3 | 4 | L’objectif de l’étude, de la recherche ou de la production de statistiques ne peut être atteint que si les renseignements sont communiqués sous une forme permettant d’identifier les personnes concernées. | [ ]  | [ ]  |
| 4 | 9 et 10 | Les renseignements personnels sont utilisés de manière à en assurer la confidentialité. | [x]  | [ ]  |
|  | Étape du cycle de vie des renseignements personnels | Niveau de risque résiduel  |  |
| Collecte |  |
| Utilisation |  |
| Communication |  |
| Conservation et destruction |  |
| Moyenne du niveau de risque résiduel |  |  |
|  |
| 5 | 11 | L’objectif de l’étude, de la recherche ou de la production de statistiques l’emporte, eu égard à l’intérêt public, sur l’impact de la collecte, de l’utilisation, de la communication, de la conservation et de la destruction des renseignements personnels sur la vie privée des personnes concernées. | [ ]  | [ ]  |
| Bilan | **Le comité EFVP estime que le projet répond entièrement aux critères 1 à 5 énoncés dans l’article 67.2.1 de la *Loi sur l’accès*.** | [ ]  | [ ]  |

# Signatures (comité EFVP et établissement)

## Signature de la représentante du comité EFVP

Sur la base des informations qui ont été fournies et après l’évaluation des facteurs relatifs à la vie privée se rapportant à la présente demande, cette dernière est **approuvée conditionnellement à ce que les mesures de sécurité énoncées à la section 9 soient mises en œuvre**.

|  |
| --- |
| Signature de la représentante du comité évaluateur des facteurs relatifs à la vie privée |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Catherine Patenaude**Conseillère cadre en protection des renseignements personnels, CCSMTL \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Date** |

## Signature(s) des directions concernées par la collecte de renseignements

L’évaluation de la demande de communication de renseignements personnels a été faite en considérant, entre autres, les informations contenues dans le présent formulaire ainsi qu’en considérant la conclusion du comité EFVP quant au respect des 5 critères de l’article 67.2.1 de la *Loi sur l’accès*.

|  |
| --- |
| Direction des services professionnels (renseignements d’usagers) |
| **Cette demande est acceptée ou refusée**:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Signature :**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Dr Jean-François Thibert** Directeur des services professionnels et des affaires médicales universitaires par intérim, CCSMTL **Date :**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |
| --- |
| Direction des ressources humaines (renseignements d’employés) |
| **Cette demande est acceptée ou refusée**:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Signature :**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Lyne Ouellette** Chef de service – Avantages sociaux, rémunération et systèmes d'informationDirection des ressources humaines, CCSMTL **Date :**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

# Annexes

## Annexe 1 : Niveaux d’identification des renseignements personnels

Il existe plusieurs niveaux d’identification des renseignements, définis comme suit :

|  |  |
| --- | --- |
| Niveau d’identification | Définition |
| Renseignements nominaux | Renseignements permettant d’identifier une personne en particulier par des identificateurs directs (par exemple, nom, numéro d’assurance sociale ou numéro d’assurance maladie) ou qui peuvent vraisemblablement permettre d’identifier une personne par une combinaison d’identificateurs indirects (par exemple, date de naissance, lieu de résidence ou caractéristique personnelle distinctive). |
| Renseignements dénominalisés | Renseignements dont les identificateurs directs ont été retirés et remplacés par un code. Si ce code est accessible, il peut être possible de réidentifier des participants précis (par exemple, si le responsable du projet ou le chercheur principal conserve une liste permettant d’associer, au besoin, le nom de code des participants à leur vrai nom; EPTC2, chapitre 5A). |
| Renseignements anonymisés | Renseignements 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 restants est faible ou très faible (EPTC2, chapitre 5A). De plus, des renseignements dépersonnalisés pourraient être considérés comme étant anonymisés dans les projets où le chercheur ou le responsable du projet n’a pas accès à la clé du code (EPTC2, art. 5.5B). L’anonymisation est un processus complexe qui doit suivre les meilleures pratiques généralement reconnues et selon les critères et les modalités déterminés par règlement du gouvernement. Selon la Commission d’accès à l’information, il est quasi impossible de garantir l’anonymisation des données de manière irréversible. |
| Renseignements agrégés | Intégration de renseignements concernant de nombreux individus. Il n'est pas possible de retrouver une personne en particulier à partir de renseignements agrégés. |

## Annexe 2 : Mesures organisationnelles de protection des renseignements personnels et de la vie privée s’appliquant à des demandes de communication de renseignements personnels sans consentement à des fins de projets d’étude, de recherche ou de production de statistiques.

**Évaluation des projets de recherche par un comité d’éthique de la recherche :**

L’évaluation des critères et des principes en protection des renseignements personnels fait partie intrinsèque du mandat du comité d’éthique de la recherche qui veille à la protection, à la sécurité et au bien-être de tous les participants impliqués dans une recherche, ce qui inclut le respect de la vie privée des participants et la confidentialité des renseignements personnels. Cette évaluation est faite par l’analyse de l’ensemble de la documentation soumise incluant le protocole de recherche en se basant sur la législation et les normes éthiques applicables.

**Obligations des chercheurs :**

Afin de pouvoir exercer des activités de recherche au sein du CIUSSS du Centre-Sud-de-l’Île-de-Montréal (CCSMTL), le chercheur doit obtenir un statut de chercheur ou des privilèges de recherche. Il est alors obligé de suivre diverses formations et de respecter en tout temps les lois, règlements et bonnes pratiques applicables à la recherche, dont notamment celles découlant de l’Énoncé de politique des trois conseils : éthique de la recherche avec des êtres Humains, des Bonnes pratiques cliniques de la Conférence Internationale d’Harmonisation (ICH), du Cadre de référence ministériel pour la recherche avec des participants humains (MSSS), du Cadre global de gestion des actifs informationnels — volet sécurité (MSSS) et de la Politique sur la conduite responsable en recherche (Fonds de recherche du Québec). Ces documents encadrent notamment l’importance du maintien de la protection des renseignements personnels. Dans les cas de manquement à ces obligations, un chercheur pourrait se voir suspendre ses activités de recherche, voire se faire retirer son statut de chercheur et, par conséquent, son droit de faire de la recherche au sein de l’établissement. De plus, l’établissement se réserve le droit de vérifier de façon aléatoire quelques recherches par année afin de s’assurer de la conformité de celles-ci en regard des informations fournies et approuvées par l’établissement.

**Obligations des médecins/professionnels qui participent à des projets de recherche ou organisationnels :**

Si le responsable du projet ou le chercheur est un médecin ou un professionnel, il est soumis aux mêmes règles de confidentialité, qu’il exerce en clinique ou participe à un projet de recherche ou organisationnel. Le respect du secret professionnel s’impose au médecin ou au professionnel dans l’exercice de ses activités professionnelles, en établissement ou en cabinet privé.

**Cadre réglementaire et politique du CCSMTL en matière de recherche :**

Notre établissement ayant une vocation universitaire importante et dans le but d’assurer la promotion et le développement de recherche de qualité, le CCSMTL met en œuvre les bonnes pratiques en intégrité scientifique et en éthique de la recherche. Les activités de recherche réalisées au CCSMTL ou sous ses auspices sont d’abord encadrées par son [*Cadre réglementaire de la recherche*](https://www.extranetccsmtl.ca/fileadmin/CIUSSSEspacesSecurises/ESPolitiquesProceduresReglements/CIUSSS/3000/RE_3000_002/RE_3000_002.pdf) qui vise à promouvoir une recherche de qualité respectant la dignité des participants et à se doter de mécanismes assurant le respect des règles et principes éthiques de la recherche en vigueur. Le CCSMTL est aussi assujetti à sa [*Politique sur la conduite responsable en recherche*](https://www.extranetccsmtl.ca/fileadmin/CIUSSSEspacesSecurises/ESPolitiquesProceduresReglements/CIUSSS/3000/PO_3000_002/PO_3000_002.pdf) qui décrit le comportement attendu de quiconque mène des activités de recherche ou de soutien à la recherche à quelque étape que ce soit d’un projet de recherche. Cette politique précise notamment que les activités de recherche doivent s’appuyer sur le principe de confidentialité et sur les valeurs d’honnêteté, de responsabilité, de rigueur, d’objectivité et de transparence.

**Lignes directrices du CIUSSS du Centre-Sud-de-l’Île-de-Montréal encadrant les projets organisationnels (projet autre que recherche) :**

Quant aux projets organisationnels autres que ceux de recherche sollicitant la participation des personnes ou l’utilisation de leurs données, ils sont encadrés, sur le plan éthique, par la procédure *Accompagnement éthique de projets impliquant des personnes ou leurs données*. Dans le cadre de cette procédure, un *Comité d’accompagnement éthique de projets impliquant des personnes ou leurs données,* formé d’un cadre-conseil en éthique de la recherche et d’une conseillère en éthique clinique et organisationnelle, et toutes autres personnes qui détiennent une expertise pertinente, analyse le projet soumis en se basant sur les principes éthiques en vigueur au CCSMTL. Le Comité formule des recommandations visant à minimiser les risques éthiques et à maximiser les avantages potentiels pour les personnes, notamment en matière de consentement, de confidentialité, de protection de la vie privée, de mesures de protection des renseignements personnels, etc.

**Procédure et mesures encadrant la destruction sécurisée des renseignements personnels :**

Les renseignements seront détruits dans les délais imposés des lois applicables et politiques internes en vigueur. Le responsable du projet aura la responsabilité de détruire les renseignements conservés sur son espace informatique sécurisé dès qu’ils ne seront plus requis ou au maximum à l’expiration du délai de conservation indiqué au Formulaire EFVP et d’avertir l’établissement de la destruction. Une entente signée entre l’établissement et le responsable du projet (telle que requise par la loi) impose, entre autres, cette obligation au responsable du projet. Du côté du CCSMTL, une procédure de [*Destruction sécuritaire des documents administratifs contenant des renseignements personnels, confidentiels ou sensibles*](https://www.extranetccsmtl.ca/fileadmin/CIUSSSEspacesSecurises/ESPolitiquesProceduresReglements/CIUSSS/6000/PR_6000_012/PR_6000_012.pdf) détermine et vise à faire connaître toutes les mesures appropriées permettant une destruction sécuritaire des documents renfermant des renseignements personnels, confidentiels ou sensibles dans l’ensemble de ses installations. L’établissement a également mis en place un registre listant les demandes de communication visées par l’article 67.2.1 de la *Loi sur l’accès* comme mesure de contrôle. Le registre inclut un calendrier de conservation permettant de faire un rappel au responsable du projet à la fin du délai afin de valider s’il a effectivement détruit les renseignements à l’expiration du délai de conservation indiqué au Formulaire EFVP ou si ce n’est pas fait, alors lui demander de le faire dans les meilleurs délais et d’aviser l’établissement à la suite de la destruction.

1. Les niveaux d’identification des renseignements personnels sont définis en annexe 1. [↑](#footnote-ref-2)
2. Les délais indiqués entre parenthèses peuvent varier selon plusieurs facteurs, y compris l’exhaustivité des informations fournies par le chercheur dans le présent formulaire, les délais de réponse du chercheur, la complexité du projet à évaluer, la familiarité du comité EFVP avec le ou les systèmes d’information visés par le chercheur et la charge de travail du comité EFVP (p. ex., autres EFVP en cours). Le comité EFVP veille toutefois à évaluer les formulaires complets dans les plus brefs délais. [↑](#footnote-ref-3)
3. Les niveaux d’identification des renseignements personnels sont définis en annexe 1. [↑](#footnote-ref-4)
4. Par souci d’alléger le texte, l’expression « renseignements » est utilisée dans le corps du formulaire pour désigner les renseignements personnels. [↑](#footnote-ref-5)
5. Par souci d’alléger le texte, l’expression « chercheur » est utilisée dans le corps du formulaire pour désigner le chercheur responsable du projet et son équipe de recherche, sauf lorsque spécifié autrement. [↑](#footnote-ref-6)
6. Les niveaux d’identification des renseignements personnels sont définis en annexe 1. [↑](#footnote-ref-7)
7. Le document *Termes et conditions d'utilisation des outils de collaboration* publié par le ministère de la Santé et des Services sociaux (MSSS) suggère d’utiliser les outils collaboratifs M365 du réseau de la santé pour le traitement de renseignements confidentiels en dernier recours, soit s'il n'existe pas d'autres solutions disponibles, si les conditions d’utilisation du MSSS sont respectées et si les bonnes pratiques de sécurité et de protection des renseignements personnels sont respectées. [↑](#footnote-ref-8)
8. Les outils collaboratifs M365 du réseau de la santé peuvent être utilisés pour faire des analyses sur des renseignements personnels lorsqu’il n’existe pas d’autres alternatives possibles, notamment lorsque le travail collaboratif est incontournable et doit se faire en temps réel sur un document commun. L’utilisation de ces outils doit s’effectuer conformément aux conditions d’utilisation du MSSS et selon les bonnes pratiques de sécurité et de protection des renseignements personnels. [↑](#footnote-ref-9)
9. Il est fortement déconseillé de communiquer des renseignements personnels par courriel étant donné que ceux-ci peuvent être interceptés contrairement aux autres méthodes énumérées. [↑](#footnote-ref-10)
10. Les outils M365 du MSSS ne devraient pas être utilisés pour la conservation à long terme des renseignements personnels, à moins qu’aucune autre alternative n’existe. [↑](#footnote-ref-11)
11. Les niveaux d’identification des renseignements personnels sont définis en annexe 1. [↑](#footnote-ref-12)