



INSTITUT UNIVERSITAIRE
DE CARDIOLOGIE
ET DE PNEUMOLOGIE
DE QUÉBEC
UNIVERSITÉ LAVAL

 CIRRUS

CADRE DE GOUVERNANCE

Centre d'intégration et de régie des
renseignements de santé pour utilisation
secondaire (CIRRUS)

Version 1
28 MAI 2024

Ce document a été réalisé grâce à la collaboration du Centre d'intégration et d'analyse des données médicales (CITADEL) du Centre hospitalier de l'Université de Montréal (CHUM). Il est adapté du cadre de gestion de CITADEL préparé originalement par Camille Craig, Marie-Josée Bernardi, Michaël Chassé et Carole Jabet.

CIRBUS est financé en partie par une subvention du ministère de l'Économie, de l'Innovation et de l'Énergie (MEIE), et est piloté conjointement par la Direction de la qualité, de l'évaluation, de la performance, de l'éthique, de la transformation et de l'innovation (DQEPETI) ainsi que la Direction de la recherche universitaire (DRU).

Document préparé par :

Mylène Bertrand, responsable des opérations CIRBUS – gestion

Félix Gélinas-Gascon, responsable des opérations CIRBUS – technologie

Philippe Després, chercheur au Centre de recherche de l'Institut

Caroline Paquin, directrice de la qualité, de l'évaluation, de la performance, de l'éthique, de la transformation et de l'innovation

TABLE DES MATIÈRES

CONTEXTE	1
1. DESCRIPTION ET OBJECTIFS DE CIRRUS	2
2. STRUCTURE ADMINISTRATIVE	2
2.1 CADRE LÉGAL ET RÉGLEMENTAIRE	2
2.2 GOUVERNANCE CIRRUS.....	4
2.2.1 Rôles et responsabilités	5
2.3 PROPRIÉTÉ.....	5
2.4 FINANCEMENT	5
2.5 CHANGEMENT DE VOCATION	6
3. COLLECTE DES DONNÉES	6
3.1 CONDITIONS D’ADMISSIBILITÉ	6
3.2 CONSTITUTION D’UN LAC DE DONNÉES	6
3.2.1 Infrastructures physiques et logicielles.....	7
3.2.2 Ingestion des données	7
3.2.3 Création d’identifiants uniques banalisés.....	7
4. PROTECTION DE LA VIE PRIVÉE ET CONFIDENTIALITÉ	7
4.1 SÉCURITÉ DE L’INFORMATION	8
4.1.1 Mesures physiques	8
4.1.2 Mesures techniques.....	8
4.1.3 Mesures administratives.....	8
4.2 TRANSFERT DES DONNÉES VERS LES REQUÉRANTS.....	8
4.3 RESPONSABILITÉ DES REQUÉRANTS	8
4.4 ENTENTE DE CONFIDENTIALITÉ	9
4.5 FORMATION AU SEIN DE L’ÉQUIPE OPÉRATIONNELLE CIRRUS	9
4.6 CONFORMITÉ	9
5. GESTION ET UTILISATION DES DONNÉES	9
5.1 OFFRE DE SERVICES	9
5.2 TYPES D’UTILISATION.....	10
5.3 APPARIEMENT DES DONNÉES	10
5.4 CONDITIONS D’ACCÈS	11
5.5 DÉLAIS D’ACCÈS.....	11
5.6 PROCESSUS D’ACCÈS AUX DONNÉES	12
5.6.1 Soumission d’une demande d’accès	13

5.6.2	Évaluation de la demande par le comité d'accès.....	13
5.6.3	Rencontre de précision des besoins	13
5.6.4	Signature de l' <i>Entente de services</i>	13
5.6.5	Création des ensembles de données	13
5.6.6	Mise à disposition ou transfert des données.....	14
5.6.7	Fin de projet.....	14
5.7	REGISTRE DES PROJETS.....	14
6.	COMMERCIALISATION ET PROPRIÉTÉ INTELLECTUELLE.....	14
6.1	RECONNAISSANCE DES AUTEURS.....	14
	GLOSSAIRE	15
	ANNEXE 1 : MANDAT ET ORGANIGRAMME	17
	ANNEXE 2 : RÈGLEMENTS, POLITIQUES ET PROCÉDURES.....	18
	ANNEXE 3 : CELLULE D'INNOVATION ET DÉVELOPPEMENT DE LA RELÈVE	19
	BIBLIOGRAPHIE	20

Liste des figures ou des illustrations

Figure 1	- Représentation de la hiérarchie de la documentation au sein de CIRRUS.	3
Figure 2	- Organigramme CIRRUS.	4
Figure 3	- Flux de données pour utilisation secondaire.	6
Figure 4	- Cheminement des demandes d'accès.....	12

Liste des sigles et des abréviations

Institut	Institut universitaire de cardiologie et de pneumologie de Québec – Université Laval
CIRRUS	Centre d'intégration et de régie des renseignements de santé pour utilisation secondaire
MSSS	Ministère de la Santé et des Services sociaux
DRI	Direction des ressources informationnelles
CD	Comité de direction
CHU	Centre hospitalier universitaire
HL7	Consortium Health Level Seven International
CAI	Commission d'accès à l'information du Québec
CRCHUM	Centre de recherche du Centre hospitalier de l'Université de Montréal
CHUM	Centre hospitalier de l'Université de Montréal
CITADEL	Centre d'intégration et d'analyse des données médicales du CHUM
CVD	Centre de valorisation de données
FRQS	Fonds de recherche du Québec – Santé
TNDR	Table nationale des directeurs de la recherche

CONTEXTE

La *Stratégie québécoise des sciences de la vie (SQSV) 2022-2025* [1] prévoit, dans l'axe « Générer des synergies pour relever les grands défis de santé », une mesure qui vise à innover grâce à la valorisation des renseignements de santé. De plus, dans son document *Plus humain, plus performant : Plan pour mettre en œuvre les changements nécessaires en santé* [2], le ministère de la Santé et des Services sociaux (MSSS) fait de l'accès aux données une de ses principales priorités. Dans ce contexte, l'Institut universitaire de cardiologie et de pneumologie de Québec - Université Laval (Institut) a créé le Centre d'intégration et de régulation des renseignements de santé pour utilisation secondaire (CIRRUS) qui vise à encadrer la valorisation des renseignements de santé et de services sociaux ainsi qu'à faciliter l'accès aux données à des fins de gestion (qualité, performance), d'innovation, de recherche, d'enseignement, d'évaluation et d'amélioration des modes d'intervention en santé.

Ce document aborde les six éléments qui devraient se retrouver dans le cadre de gestion d'une banque de données, comme suggéré par le MSSS dans son *Guide d'élaboration des cadres de gestion des banques de données et de matériel biologique constituées à des fins de recherche* [3], soit :

- la description de la banque;
- la structure de la gestion administrative;
- la collecte des données;
- la gestion des données;
- la protection de la vie privée et la confidentialité;
- la commercialisation et la propriété intellectuelle.

La portée de ce document dépasse cependant celle associée au cadre de gestion d'une banque de données, en touchant de façon plus globale à la gouvernance de l'information au sein de l'établissement. La gouvernance informationnelle, telle que définie par la norme ISO 24143, est un ensemble de « politiques, processus, procédures, rôles et contrôles mis en place dans le but de répondre aux exigences réglementaires, légales, opérationnelles et relatives aux risques » [4]. De façon encore plus large, ce document contient des éléments touchant à la gouvernance CIRRUS et à son rôle au sein de l'Institut. Le contenu de ce cadre est inspiré du *Guide pour la mise en œuvre et le fonctionnement d'un lac de données dans un établissement de santé et de services sociaux* de l'initiative « Accès aux données » de la Table nationale des directeurs de la recherche (TNR) [5]. Il s'inspire aussi du cadre de gouvernance du Centre d'intégration et d'analyse des données médicales (CITADEL) du Centre hospitalier de l'Université de Montréal (CHUM).

Le présent document décrit les modalités, les exigences et les processus permettant une utilisation secondaire des renseignements de santé et de services sociaux à l'Institut.

1. DESCRIPTION ET OBJECTIFS DE CIRRUS

CIRRUS est une plateforme créée pour encadrer, baliser, normer et surveiller l'accès aux données pour des utilisations secondaires à l'Institut. Cette plateforme offre des services à divers secteurs d'affaires (par ex. recherche, administration, clinique), avec l'objectif principal de valoriser des renseignements de santé. Cette valorisation peut prendre différentes formes, comme celles énoncées dans le document de la TNDR [5] :

- Acquérir et lier les données pour améliorer les soins aux patients et augmenter la performance du système;
- Fournir un accès facile, sécurisé, approprié, dans un temps raisonnable aux données, pour faciliter la recherche, l'évaluation, l'innovation et l'enseignement;
- Appuyer les décisions par l'analyse et la visualisation de données de haute qualité obtenues en temps réel.

CIRRUS permet d'exposer des données de façon sécuritaire et responsable aux utilisateurs et utilisatrices du réseau de la santé ou du secteur privé, selon les lois, règlements et autorisations d'usage en vigueur [6]. CIRRUS vise à centraliser les accès vers les renseignements de santé pour utilisation secondaire, afin notamment de faciliter la reddition de comptes et la journalisation.

Pour remplir sa mission sans affecter les opérations du secteur clinique, CIRRUS gère un lac de données institutionnel où sont versées les informations de divers systèmes d'information. Cette composante technologique, qui héberge des données nominatives, réside sur le réseau conforme de l'Institut et profite à cet égard de la même protection que les actifs informationnels de la part de la Direction des ressources informationnelles (DRI). Dans le cadre des opérations, les données sont extraites de ce lac de données, dépersonnalisées, transformées et agrégées au besoin, et mises à disposition des requérants et requérantes.

2. STRUCTURE ADMINISTRATIVE

2.1 CADRE LÉGAL ET RÉGLEMENTAIRE

De façon générale, le cadre de gouvernance CIRRUS vise à assurer la protection de la vie privée et à réduire au minimum les risques reliés à l'utilisation secondaire de renseignements de santé et de services sociaux. Les principes de protection de la vie privée énoncés dans ce cadre de gouvernance se conforment au *Code civil du Québec* [7], à la *Loi sur les services de santé et les services sociaux* [8], à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* [9], à la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* [10] à la *Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives* [11] (loi 5 – sanctionnée le 4 avril 2023) et à la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (loi 25)[12].

Le cadre de gouvernance CIRRUS a été développé en cohérence avec les règlements, politiques et procédures en vigueur à l'Institut et de son Centre de recherche (annexe 2).

La politique des trois organismes sur la gestion des données de recherche [13] a également servi de référence à l'élaboration du présent document, notamment quant à l'application des principes FAIR (données Facilement repérables, Accessibles, Interopérables, Réutilisables) [14].

La figure 1 suivante illustre la hiérarchie des différents documents CIRRUS. Le cadre de gouvernance CIRRUS s'inscrit plus largement dans les documents institutionnels existants (politiques et procédures à l'Institut et à son Centre de recherche).

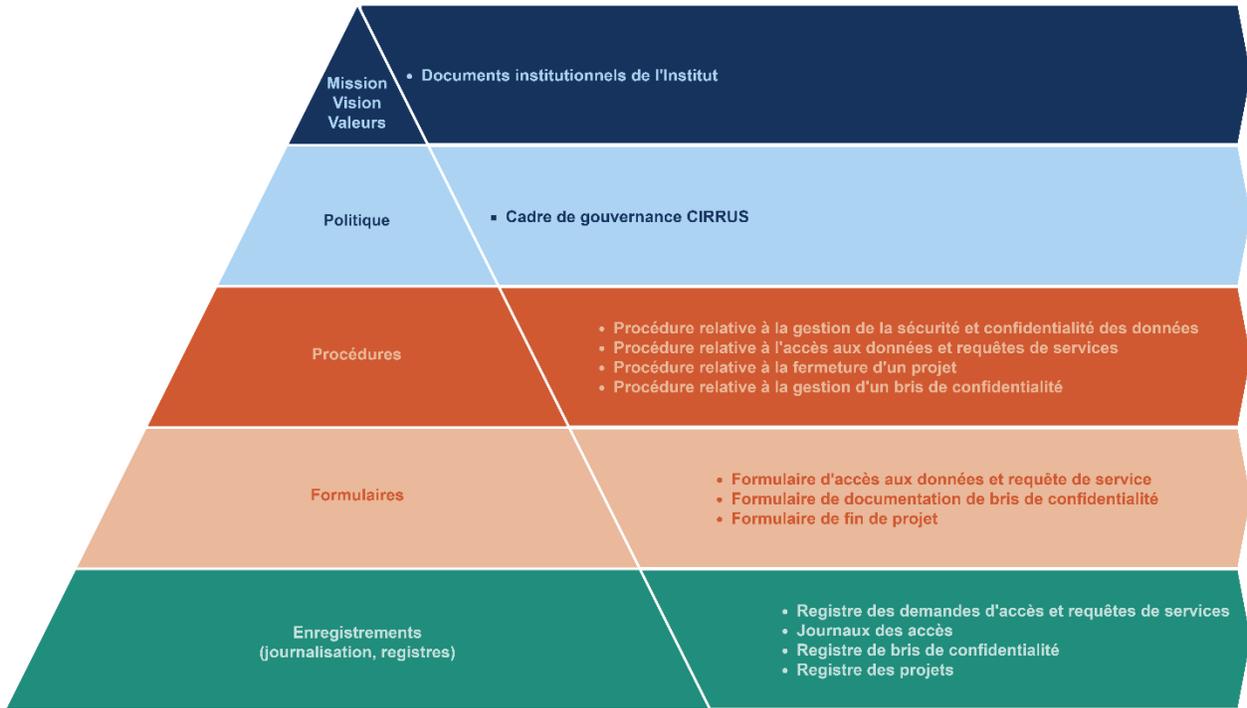


FIGURE 1 - REPRÉSENTATION DE LA HIÉRARCHIE DE LA DOCUMENTATION AU SEIN DE CIRRUS.

2.2 GOUVERNANCE CIRRUS

Les liens hiérarchiques de la gouvernance CIRRUS ont été définis dans son mandat (annexe 1), adopté par le comité de direction de l’Institut et illustré dans l’organigramme suivant (figure 2).

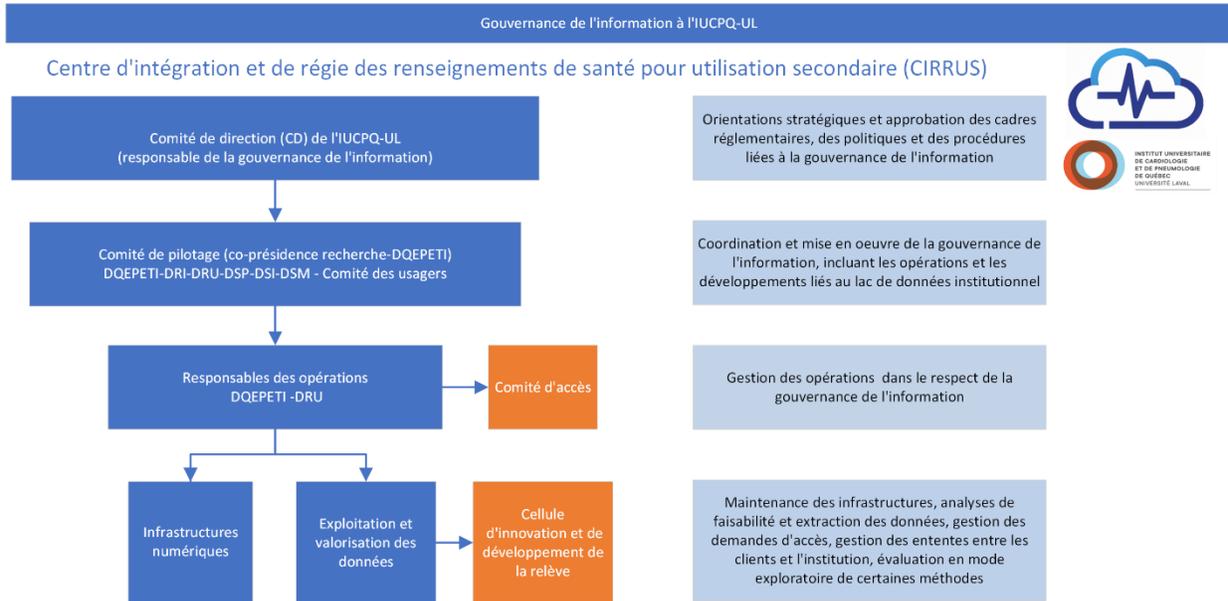


FIGURE 2 – ORGANIGRAMME CIRRUS.

2.2.1 Rôles et responsabilités

Le **comité de direction** (CD) de l'Institut a la responsabilité de déterminer les orientations stratégiques et d'approuver le cadre de gouvernance et les procédures de CIRRUS.

Le **comité de pilotage** assure la coordination et la mise en œuvre de CIRRUS, incluant les opérations et les développements liés au lac de données institutionnel.

Les **responsables des opérations** de CIRRUS relèvent hiérarchiquement des co-responsables CIRRUS et collaborent avec le personnel de la DRI, de l'équipe informatique du Centre de recherche de l'Institut et l'équipe du volet performance de la DQEPETI. Ils ont le mandat de s'assurer du respect des politiques, procédures et meilleures pratiques mises en place au sein de CIRRUS. Ils assurent la gestion de projets, l'administration financière et logistique, la gestion des ententes, des contrats, des registres de suivi et la conformité éthique et juridique des demandes d'accès.

Un **comité d'accès** évalue, approuve et priorise selon les critères en vigueur les demandes d'accès, dont la faisabilité, les synergies possibles et les ressources requises.

Une **cellule d'innovation et de développement de la relève**, sous la responsabilité du représentant de la communauté de la recherche, est un espace consacré à la formation de la relève et aux expérimentations au sein de CIRRUS (p. ex. évaluation en mode exploratoire de certaines méthodes numériques).

Les **équipes des infrastructures numériques et valorisation des données** réunissent des expertises techniques (p. ex. serveurs, machines virtuelles), de gestion, de protection et d'analyse de données. Elles assurent, de concert avec les responsables des opérations et la DRI :

- le déploiement et la maintenance des infrastructures numériques;
- l'application de la stratégie de sécurité informationnelle, incluant la journalisation des accès;
- les analyses de faisabilité technologique;
- l'extraction et la mise en forme des données;
- les processus de dépersonnalisation des données.

2.3 PROPRIÉTÉ

Les actifs informationnels sous le contrôle de CIRRUS appartiennent à l'Institut.

2.4 FINANCEMENT

Les opérations de CIRRUS sont initialement financées par le ministère de l'Économie, de l'Innovation et de l'Énergie par l'entremise du programme de soutien à l'organisation et à la valorisation des renseignements de santé (mesure de la *Stratégie québécoise des sciences de la vie 2022-2025*). L'Institut contribue aussi au financement.

2.5 CHANGEMENT DE VOCATION

Tout changement de vocation de CIRBUS doit être approuvé par le comité de direction de l'Institut.

3. COLLECTE DES DONNÉES

3.1 CONDITIONS D'ADMISSIBILITÉ

Il n'y a pas de restriction quant aux types et à l'origine des données pouvant être gérés par CIRBUS. En plus des renseignements de santé et de services sociaux, CIRBUS peut accueillir des données clinico-administratives et des données collectées dans un contexte de recherche selon les lois et règlements en vigueur.

3.2 CONSTITUTION D'UN LAC DE DONNÉES

CIRBUS a recours à un lac de données pour remplir sa mission. Cette approche consiste à verser, le plus souvent telles quelles, les données contenues dans divers systèmes d'information (par ex. laboratoires, médicaments, sommaires d'hospitalisation). Ces données, souvent sous forme brute, ne peuvent typiquement pas être consommées sans des étapes préalables de transformation. L'approche du lac de données permet de faciliter les utilisations secondaires tout en évitant de mettre en péril les systèmes d'information critiques dans le fonctionnement des opérations hospitalières; les pipelines d'extraction sont connectés au lac et non aux systèmes en production (figure 3).

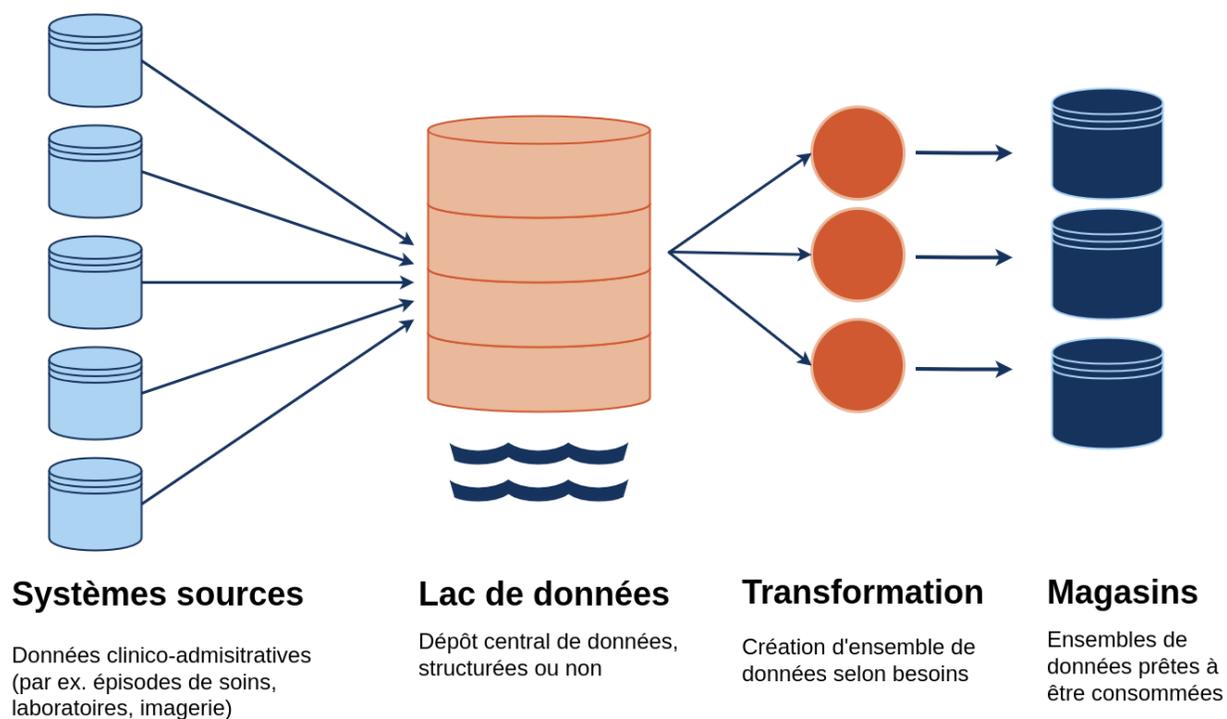


FIGURE 3 – FLUX DE DONNÉES POUR UTILISATION SECONDAIRE.

3.2.1 Infrastructures physiques et logicielles

Le lac de données CIRRUS, qui contient des renseignements de santé et de services sociaux, est hébergé au sein du réseau conforme à l'Institut. Les serveurs physiques et les composantes logicielles de base (par ex. virtualisation) sont gérés par la DRI. Le matériel est situé dans une zone sécurisée à accès restreint. Les machines virtuelles créées pour répondre aux besoins d'affaires de CIRRUS sont gérées par l'équipe CIRRUS, en collaboration avec la DRI.

3.2.2 Ingestion des données

La fréquence et la stratégie (incrémentale ou complète) de chargement des données vers le lac sont déterminées conjointement par la DRI, l'équipe CIRRUS et les pilotes des systèmes concernés. La capture de transactions (typiquement messages HL7) entre systèmes d'information peut aussi être appropriée pour certains projets nécessitant des données en temps réel.

3.2.3 Création d'identifiants uniques banalisés

Au sein de l'institution, les individus sont identifiés par leur numéro de dossier hospitalier. Ce numéro permet de retracer les individus dans différents systèmes d'information, par l'entremise de l'index patient (système d'admission, départ et transfert - ADT). Les données qui sont exposées aux requérants contiendront une version banalisée de cet identifiant, pour faciliter d'éventuels échanges en lien avec les données fournies. La version banalisée est produite par une fonction de hachage salée, opération mathématique unidirectionnelle qui empêche la reconstitution de l'information originale. Des sels différents seront utilisés pour chaque projet.

Pour certains projets, les requérants fournissent une liste d'identifiants permettant de retrouver les bonnes informations; dans ces cas, ces identifiants sont retournés avec les données demandées (voir scénarios d'utilisation et détails à la section 5).

4. PROTECTION DE LA VIE PRIVÉE ET CONFIDENTIALITÉ

CIRRUS se conforme à l'ensemble des règlements, politiques et procédure en vigueur à l'Institut concernant la confidentialité et les renseignements personnels.

De façon générale, CIRRUS s'assure de maintenir un niveau de risque de réidentification acceptable pour les ensembles de données dépersonnalisés qui seront produits. Des manipulations telles que le masquage des résultats d'analyse avec cellules contenant moins de cinq individus [15], la généralisation (ex. : création de catégories pour l'âge, année de diagnostic au lieu de date complète) et la suppression ou la substitution de valeurs (ex. : suppression ou remplacement d'une valeur extrême ou marginale permettant d'identifier potentiellement un individu), pour n'en nommer que quelques-unes, peuvent être employées.

4.1 SÉCURITÉ DE L'INFORMATION

Des mesures rigoureuses – *physiques, techniques, administratives* – pour protéger la vie privée et assurer la confidentialité à tous les niveaux du cycle de vie des données sont mises en œuvre au sein de CIRRUS. Ces mesures sont conformes avec les politiques et procédures en vigueur à l'Institut.

4.1.1 Mesures physiques

Les actifs informationnels de CIRRUS sont entreposés sur des serveurs dédiés et protégés au sein des infrastructures de l'Institut. Ces serveurs physiques sont gérés par l'équipe de la DRI. Ils sont soumis aux mêmes standards de sécurité que les autres actifs contenant des données clinico-administratives de l'Institut. L'accès à l'espace des serveurs physiques est contrôlé.

4.1.2 Mesures techniques

L'infrastructure numérique CIRRUS est constituée de serveurs virtuels déployés sur le réseau conforme [16] et isolés dans un premier temps d'un point de vue réseautique. Les ouvertures réseau sont faites à la pièce pour chaque service nécessaire aux opérations. L'administration des serveurs virtuels est assurée par un nombre limité de personnes au sein de CIRRUS et de la DRI.

4.1.3 Mesures administratives

Un système assure la journalisation des accès aux données de CIRRUS. Seuls les utilisateurs CIRRUS détenant le privilège peuvent accéder aux actifs CIRRUS. Les utilisateurs secondaires accèdent aux ensembles de données créés pour eux et entreposés séparément des actifs CIRRUS, via des espaces de stockage dédiés à cette fin. Les journaux de connexion et d'accès pourront être consultés en tout temps par les responsables de CIRRUS ou par le comité de pilotage.

4.2 TRANSFERT DES DONNÉES VERS LES REQUÉRANTS

Les données dépersonnalisées sont transférées aux requérants par l'entremise d'un espace sécurisé à accès contrôlé. Les requérants deviennent responsables de ces données dès leur accession et doivent les gérer selon les autorisations obtenues des instances concernées (par ex. comité d'éthique de la recherche (CER), CAI, plus haut dirigeant de l'établissement). Pour les ensembles de données contenant des renseignements identificatoires (par ex. numéro de dossier), l'espace sécurisé à accès contrôlé est situé sur le réseau conforme de l'Institut.

4.3 RESPONSABILITÉ DES REQUÉRANTS

En tout temps, les requérants s'engagent à respecter les bonnes pratiques, les lois et les règlements quant à l'accès, l'utilisation, la conservation, la manipulation et la destruction des renseignements de santé et de services sociaux. Pour le secteur de la recherche, s'applique également la conduite responsable [17] telle

que définie par les établissements académiques et les organismes de financement. Les requérants doivent respecter ses règles pendant et après l'utilisation des renseignements.

4.4 ENTENTE DE CONFIDENTIALITÉ

Le personnel CIRRUS s'engage à respecter les politiques mises en place à l'Institut et à son Centre de recherche quant à la protection de la vie privée et à la sécurité de l'information. Cet engagement est officialisé par la signature des formulaires destinés au personnel ayant accès aux renseignements de santé et de services sociaux.

4.5 FORMATION AU SEIN DE L'ÉQUIPE OPÉRATIONNELLE CIRRUS

Tous les membres de l'équipe de CIRRUS et les personnes appelées à travailler en collaboration doivent posséder les compétences requises et suivre les formations requises par leur titre d'emploi et leur rôle au sein de l'équipe.

Les exigences quant à la formation sont détaillées dans le document PR-CIRRUS-002 *Procédure relative à la formation de l'équipe opérationnelle CIRRUS*.

4.6 CONFORMITÉ

Des mesures de suivi sont mises en place afin d'assurer la conformité au cadre de gouvernance CIRRUS et des politiques et procédures s'y rattachant. À cet effet, la liste des demandes d'accès aux données incluant le titre du projet et le statut de la demande ainsi que le registre des connexions aux serveurs sont déposés au comité de pilotage. De plus, le comité de pilotage rapporte annuellement au comité de direction de l'Institut la liste des projets ayant obtenu l'autorisation d'utiliser les données de CIRRUS.

Une évaluation des facteurs relatifs à la vie privée, largement inspirée des modèles existants [18] [19], est également réalisée au besoin ou lorsqu'une modification au cadre de gestion ou aux politiques et procédures est effectuée.

5. GESTION ET UTILISATION DES DONNÉES

5.1 OFFRE DE SERVICES

L'équipe CIRRUS peut offrir un ensemble de services relatifs aux données de santé dont :

- **Étude de faisabilité** : identification de la population ciblée par les requérants et/ou extraction de données préliminaires pour estimer la faisabilité d'un projet.
- **Demande impliquant la recherche de profils de participants et participantes** qui répondent à des critères précis.
- **Préparation d'ensembles de données clinico-administratives** : extraction, nettoyage et transformation des données pour obtenir un ensemble de données prêt à l'analyse.

- **Gestion des données en prospectif** : analyse des besoins pour colliger des données en temps réel et mise en place d'infrastructure de collecte et d'analyse.
- **Gestion et entreposage des données de recherche** : construction de schémas de données spécifiques à un projet et services de maintenance.

Outre les services en lien avec les requêtes d'accès aux données formulées par les utilisateurs, l'équipe CIRRU pourrait aussi proposer des services complémentaires en méthodologie et statistiques selon l'expertise disponible, tels que :

- la consultation méthodologique;
- l'analyse des données et l'interprétation des résultats;
- le soutien à la production scientifique;
- la planification d'un projet.

Ces services sont facturables pour les projets qui sont pris en charge par CIRRU (après la signature de l'*Entente de services*).

5.2 TYPES D'UTILISATION

Plusieurs scénarios d'utilisation de données sont possibles au sein de CIRRU; le tableau suivant en rapporte quelques exemples. Toutefois, pour les usages encadrés par un CER, seules les données/variables mentionnées au protocole sont extraites des systèmes d'information. Les données transmises deviennent sous contrôle des requérants, qui doivent les gérer conformément aux autorisations obtenues. Certains scénarios pourraient permettre une réidentification triviale des individus, même dans des jeux de données dépersonnalisés. Dans ces cas, les données pourraient ne pas être transmises pour préserver la confidentialité.

Scénario	Description
Extraction basée sur critères d'inclusion et d'exclusion	Les requérants fournissent des critères d'inclusion et d'exclusion pour identifier des individus. CIRRU produit un ensemble de données dépersonnalisées.
Extraction basée sur une liste de numéros de dossiers hospitaliers	Les requérants fournissent une liste de participants pour lesquels des données doivent être extraites. Ces données alimentent par exemple une base de données ou un registre déjà constitué par les requérants. CIRRU produit un ensemble de données qui contient des identifiants (par ex. numéro de dossier).
Capture de messages transactionnels	Des messages (typiquement HL7) sont collectés, le plus souvent pour alimenter des tableaux de bord ou autres applications en temps réel ou quasi réel. CIRRU collige les transactions et expose les données aux requérants, typiquement via une base de données.

5.3 APPARIEMENT DES DONNÉES

Lorsqu'approprié et seulement pour l'usage spécifié dans un projet approuvé et pour un temps limité, il est possible que les données de CIRRU soient appariées ou mises en commun avec d'autres données. Tout appariement ou combinaison des données de CIRRU avec d'autres sources doit être spécifié dans la

demande d'accès et les autorisations requises doivent être obtenues avant l'obtention de l'accès aux données de CIRRUS.

Certaines bases de données constituées à des fins de recherche sont entreposées au Centre de recherche de l'Institut (par ex. biobanques institutionnelles). Il est à noter que les bases de données constituées à des fins de recherche ont des règles d'accès qui leur sont propres. Aucune liaison entre les données clinico-administratives de l'Institut et les bases de données constituées à des fins de recherche ne peut être effectuée sans l'obtention de tous les accords préalables.

5.4 CONDITIONS D'ACCÈS

Les projets de recherche pour lesquels toutes les autorisations requises ont été obtenues peuvent faire une demande d'accès aux données par l'entremise de CIRRUS. Afin d'accélérer les processus, la demande à CIRRUS peut être déposée pour analyse en même temps que le dépôt au CER. Le demandeur doit avoir des privilèges de recherche à l'Institut. Les projets provenant du milieu académique externe ou les projets provenant de l'industrie doivent inclure une personne qui a un privilège de recherche à l'Institut. Les demandes de données à des fins d'enseignement, de qualité, de performance ou d'évaluation des modes d'intervention de gestion doivent être approuvées et priorisées par les instances responsables.

Les travaux de l'équipe CIRRUS, au-delà de l'évaluation de la faisabilité, peuvent commencer dès la signature de l'*Entente de services*.

5.5 DÉLAIS D'ACCÈS

Une confirmation de la soumission d'une demande d'accès sera envoyée dans les deux jours ouvrables suivant la réception de la demande. Plusieurs facteurs peuvent influencer les délais d'accès, notamment la disponibilité des requérants pour répondre aux questions de l'équipe CIRRUS, la complexité de la demande et l'obtention d'autres autorisations requises.

5.6 PROCESSUS D'ACCÈS AUX DONNÉES

Le cheminement des demandes d'accès est illustré à la figure 4. L'accès à des fins d'évaluation, de qualité, de performance, d'enseignement ou d'amélioration des modes d'intervention en santé ne nécessite pas d'Entente de services, contrairement aux demandes issues du secteur de la recherche qui nécessiteront une Entente de services.



FIGURE 4 - CHEMINEMENT DES DEMANDES D'ACCÈS.

5.6.1 Soumission d'une demande d'accès

Les demandes d'accès sont formulées par l'entremise d'un formulaire Web, qui renseigne sur divers éléments du projet. À cette étape, une vérification de la conformité éthique, juridique et budgétaire de la demande est effectuée. L'équipe CIRRUS peut contacter les demandeurs pour préciser certains éléments, après quoi la demande admissible est transférée au comité d'accès.

5.6.2 Évaluation de la demande par le comité d'accès

Le comité d'accès évalue les projets admissibles et les priorise selon différents critères dont :

- la nature des projets (par ex. gestion, reddition de comptes, priorités organisationnelles, caractère stratégique);
- la faisabilité technique;
- les ressources requises et le financement disponible;
- la considération des dates de soumission aux organismes subventionnaires;
- les synergies avec d'autres projets et le potentiel de réutilisation.

À cette étape, le comité d'accès peut décider de refuser une demande d'accès. Dans tous les cas, une justification de la décision sera transmise par écrit aux demandeurs. Le comité d'accès vise une décision dans un délai de 10 jours ouvrables.

5.6.3 Rencontre de précision des besoins

Une rencontre initiale est prévue entre le requérant et l'équipe CIRRUS afin de préciser le mandat et les attentes. Le requérant doit avoir en sa possession toute information relative au projet, comme le protocole de recherche, la fiche mandat de son projet, une liste de participants ou des critères d'identification de sa population cible, une liste de variables d'intérêts incluant les codes normés ou internes utilisés pour créer ces variables lorsque disponibles. À la suite de cette rencontre, l'équipe CIRRUS produit une estimation des coûts et une évaluation des délais. Il est possible que, à la suite de cette étape, un projet se révèle trop complexe ou comporte des contraintes trop grandes pour être accepté par CIRRUS. Les requérants pourraient alors être redirigés vers d'autres ressources.

5.6.4 Signature de l'Entente de services

Les services CIRRUS pour les projets de recherche sont sujets à un recouvrement de coût selon le modèle des plateformes du Centre de recherche de l'Institut. L'évaluation de la faisabilité détaillée permet de quantifier les coûts qui seront spécifiés dans l'*Entente de services*. Les estimations sont sujettes à changement advenant que des modifications soient apportées au projet.

5.6.5 Création des ensembles de données

L'équipe CIRRUS est responsable de créer et de déployer les pipelines d'extraction des données, et de constituer des ensembles de données prêts à l'emploi pour les requérants. Les scripts ayant permis les extractions et les transformations des données seront conservés dans un dépôt `git`. Ces scripts

permettent de reconstruire les ensembles de données au besoin. Sauf exception, il n'est pas prévu de conserver une copie des ensembles de données produits au sein de CIRRUS.

5.6.6 Mise à disposition ou transfert des données

Les ensembles de données sont livrés aux requérants via des espaces sécurisés à accès contrôlé. Dans certains cas, ce sont des pipelines d'alimentation en données qui sont livrés.

5.6.7 Fin de projet

Le statut du projet passe à “ *Terminé* ”.

5.7 REGISTRE DES PROJETS

Un registre des projets faisant usage des données est tenu par l'équipe CIRRUS. Ce registre est publié pour informer les communautés et le public des projets de valorisation en cours dans l'établissement.

6. COMMERCIALISATION ET PROPRIÉTÉ INTELLECTUELLE

Dans le cas où une collaboration de recherche est établie autour d'un projet utilisant les services CIRRUS, l'utilisateur secondaire s'engage à respecter les règles applicables en matière de propriété intellectuelle et de commercialisation selon la collaboration établie.

6.1 RECONNAISSANCE DES AUTEURS

L'utilisateur secondaire s'engage à reconnaître la contribution éventuelle des membres de l'équipe CIRRUS selon la taxonomie CRediT¹, notamment en ce qui a trait au rôle de curateur de données. Toute publication ou présentation utilisant les données ou des services CIRRUS doit inclure une référence au site Web de CIRRUS et la mention suivante :

Cette étude/présentation a été rendue possible par la contribution du Centre d'intégration et de régie des renseignements de santé pour utilisation secondaire (CIRRUS) de l'Institut universitaire de cardiologie et de pneumologie de Québec – Université Laval (Institut).

¹ <https://credit.niso.org/>

GLOSSAIRE

Lac de données : Dépôt centralisé qui regroupe des données structurées ou non structurées.

Entrepôt de données : Ensemble de données ayant subi certaines transformations pour répondre à des besoins d'exploitation spécifiques. Les termes comptoir, cube ou magasin de données sont parfois utilisés de façon équivalente.

Base de données : Collection de données structurées pour permettre des opérations, parfois très complexes, de lecture, de suppression, de déplacement, de tri, de comparaison ou autres opérations. Lorsque plusieurs bases de données sont constituées sous forme de collection, on parle alors d'une banque de données.

Sous-ensemble de données d'analyse : Ensemble de données extrait à partir d'un schéma de données pour répondre à une question précise. Un sous-ensemble a généralement une portée finie dans le temps et ne requiert pas de mise à jour systématique et récurrente.

Élément : Unité de donnée élémentaire définie par plusieurs attributs ou métadonnées (ex. : contexte, nom d'élément, définition, unité de mesure, format, etc.) [8]. Un élément peut être, par exemple, mais sans y être restreint, une unité de donnée en format numérique ou texte, une image numérique, un son.

Anonymisation : Procédure qui consiste à remplacer les informations nominatives contenues dans un document par un code d'identification, avant de les supprimer définitivement, de manière à rendre virtuellement impossible l'identification des individus auprès desquels elles ont été recueillies.

Dépersonnalisation (aussi nommé dénominalisation ou pseudo-anonymisation – pseudonymisation (RGPD)) : Procédure qui consiste à remplacer les informations nominatives contenues dans un document par un code d'identification, de manière à empêcher l'identification des individus auprès desquels elles ont été recueillies.

Dé-identification : L'action de transformer les données individuelles pour diminuer la probabilité de révéler l'identité d'un individu. Cela implique de retirer les identifiants directs (ex. : nom, numéro de téléphone, adresse) ainsi que de transformer les identifiants indirects pouvant être utilisés seuls ou en combinaison pour identifier un individu (ex. : dates de naissance, informations géographiques, dates d'événements) [20]

Réidentification : Tout processus rétablissant le lien entre l'information et l'identité d'un individu.

Utilisateur de la donnée : Corresponds à la personne physique ou morale qui a été autorisée à accéder à la donnée afin d'accomplir une tâche donnée ou dans l'exercice des rôles ou fonctions qui lui sont attribués. L'utilisateur de la donnée est responsable de suivre les lois, politiques, procédures et standards associés à la donnée qu'il utilise et d'utiliser cette dernière uniquement aux fins auxquelles il a été autorisé. L'utilisateur de la donnée a également la responsabilité de signaler à l'intendant de la donnée tout accès non autorisé, utilisation abusive ou problème de qualité de la donnée.

Utilisateur principal : Individu ayant obtenu l'autorisation d'accéder à des données comprises dans le lac de données. Un niveau de permission est attribué à ce type d'utilisateur qui lui donne le privilège d'accéder

à certaines données sensibles ou non sensibles, selon le niveau de permission, dans le cadre des opérations de CIRBUS.

Utilisateur secondaire : Individu ayant obtenu l'autorisation d'accéder à un entrepôt de données ou à un sous-ensemble de données d'analyse dans le cadre d'un projet spécifique.

Renseignements personnels : Renseignements portant sur un individu et permettant d'établir son identité.

Appariement de données : Opération consistant à jumeler des données sur la base de renseignements identificatoires ou dépersonnalisés à partir d'au moins deux bases de données différentes. Il s'agit donc de combiner de l'information provenant de deux bases de données différentes pour les mêmes individus.

Mise en commun de données sans appariement : Opération consistant à combiner des informations de deux bases de données différentes provenant d'individus différents.

Variables avec identifiants directs : Une ou plusieurs variables utilisées seules ou en combinaison permettant l'identification d'un individu en particulier.

Variables avec identifiants indirects : Variables utilisées seules ou en combinaison permettant d'identifier un individu en ayant connaissance du contexte.

Variable non identificatoire : Variable ne permettant pas la réidentification d'un individu.

Utilisation secondaire : Utilisation, en recherche, de renseignement ou de matériel biologique humain recueillis dans un but autre que celui de la recherche actuelle. [21, Paragr. Utilisation secondaire]

ANNEXE 1 : MANDAT ET ORGANIGRAMME

[CD 2023-10-17_Mandat CIRRUS_vf.pdf](#)

ANNEXE 2 : RÈGLEMENTS, POLITIQUES ET PROCÉDURES

Le cadre de gouvernance CIRRUS a été développé en cohérence avec les règlements, politiques et procédures en vigueur à l'Institut et de son Centre de recherche notamment :

- **DSM-024** - Politique relative à la sécurité de l'information (en refonte, nouvelle formulation à venir, sera remplacée par une future Politique et cadre de gestion en matière de sécurité de l'information et des ressources informationnelles et les procédures associées);
- **DTI-009 et DTI-009.1** - Politique de l'IUCPQ en matière de gestion des accès aux données et produits informationnels (en refonte, nouvelle formulation à venir, sera remplacée par une future Politique et cadre de gestion en matière de sécurité de l'information et des ressources informationnelles et les procédures associées);
- **PR-DSM-024-01** - Procédure concernant les règles d'utilisation des systèmes d'information (en refonte, nouvelle formulation à venir, sera remplacée par une future Politique et cadre de gestion en matière de sécurité de l'information et des ressources informationnelles et les procédures associées);
- **DRU-008** - Politique relative à la Biobanque institutionnelle et aux répertoires de matériel biologique (en révision);
- **DRU-013** - Politique relative à la gestion des banques de données de la recherche (en révision);
- **R-45** - Règlement relatif à la gestion des dossiers des usagers;
- **MON10** - Protection des participants et de leurs droits et suivi des participants à la recherche;
- **MON23** - Gestion des données et sécurité informationnelle;
- Règles de fonctionnement du comité d'éthique de la recherche (CER) de l'Institut.

ANNEXE 3 : CELLULE D'INNOVATION ET DÉVELOPPEMENT DE LA RELÈVE

L'informatique médicale est une discipline en émergence, à l'intersection de la médecine, du génie logiciel, des sciences de l'information et de la science des données entre autres. Ce domaine est appelé à prendre de l'ampleur avec le virage vers la santé numérique et le déploiement de projets d'envergure, mais est ralenti par une rareté de main-d'œuvre qualifiée. Cette main-d'œuvre doit non seulement posséder des compétences techniques avancées en informatique, mais aussi des connaissances sur le cadre éthique et légal en vigueur, ainsi que sur les terminologies, ontologies et protocoles d'échange d'information utilisés en santé. De plus, cette main-d'œuvre doit avoir une certaine compréhension des activités cliniques et administratives d'un établissement de santé afin de bien aligner les développements avec les besoins.

Dans le cadre de CIRRUS, l'Institut mettra en place une cellule d'innovation en informatique médicale. Cette cellule sera :

- un lieu d'exploration et d'expérimentation (pilotes, preuves de concept), dans un environnement contrôlé et sécuritaire;
- un lieu de formation de personnel hautement qualifié;
- un centre de ressources et de connaissances au service de l'ensemble des secteurs ayant des besoins en informatique médicale.

La cellule d'innovation est une zone virtuelle dans laquelle évolue du personnel ayant reçu la formation nécessaire pour accéder à des renseignements de santé et les manipuler. Ce personnel, typiquement des étudiants et étudiantes, provient de disciplines variées (par ex. informatique, génie logiciel, physique médicale, administration, archivistique) et est autorisé à accéder à certaines ressources (humaines ou informationnelles) dans le cadre des activités de la cellule. Celle-ci est animée par le personnel encadrant (p. ex. professeur.e.s) et dans une moindre mesure par du personnel de l'Institut.

La cellule s'inscrit dans la gouvernance informationnelle de l'Institut et profitera aussi du lac de données qui sera constitué au sein de CIRRUS. Il est convenu, comme dans toute démarche d'innovation, que certains projets mèneront à des culs-de-sac ou à des échecs. Cependant, il est aussi possible de générer des réussites sans que l'établissement prenne de grands risques (ressources humaines et financières minimales). Dans tous les cas – échecs ou réussites – la cellule permet de former du personnel avec des compétences très recherchées et peut devenir une filière de recrutement très efficace pour l'Institut.

BIBLIOGRAPHIE

- [1] « Stratégie québécoise des sciences de la vie (SQSV) 2022-2025 », Ministère de la Santé et des Services sociaux du Québec, 2022.
- [2] « Plan pour mettre en oeuvre les changements nécessaires en santé », Ministère de la Santé et des Services sociaux du Québec, 2022. [En ligne]. Disponible sur: <https://publications.msss.gouv.qc.ca/msss/document-003355>
- [3] « Guide d'élaboration des cadres de gestion des banques de données et de matériel biologique constituées à des fins de recherche ».
- [4] « ISO 24143:2022(fr), Information et documentation — Gouvernance de l'information — Concept et principes », Organisation internationale de normalisation. Consulté le: 17 janvier 2023. [En ligne]. Disponible sur: <https://www.iso.org/obp/ui/#iso:std:iso:24143:ed-1:v1:fr>
- [5] I. « A. aux données » de la T. nationale des directeurs de la recherche (TNR), C. de recherche du C. hospitalier de l'Université de Montréal (CRCHUM), F. de recherche du Q.- Santé (FRQS), C. d'Intégration et d'Analyse en D. médicales (CITADEL) du C. hospitalier de l'Université de Montréal (CHUM), C. S. N. de l'Université de Montréal, et U. informationnel du C. Ste-Justine (UniC), « Guide pour la mise en œuvre et le fonctionnement d'un lac de données dans un établissement de santé et de services sociaux », 17 octobre 2022. doi: 10.5281/zenodo.7218119.
- [6] « Autorisation des projets de recherche par l'établissement - Éthique de la recherche - Professionnels de la santé - MSSS ». Consulté le: 30 octobre 2023. [En ligne]. Disponible sur: <https://www.msss.gouv.qc.ca/professionnels/ethique/ethique-de-la-recherche/autorisation-des-projets-de-recherche-par-l-etablissement/>
- [7] « CCQ-1991.pdf ». Consulté le: 19 octobre 2023. [En ligne]. Disponible sur: <https://www.legisquebec.gouv.qc.ca/en/pdf/cs/CCQ-1991.pdf>
- [8] « 2023 - Éditeur officiel du Québec.pdf ». Consulté le: 8 décembre 2023. [En ligne]. Disponible sur: <https://www.legisquebec.gouv.qc.ca/fr/pdf/lc/S-4.2.pdf>
- [9] « 2023 - LOI SUR L'ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS.pdf ». Consulté le: 19 octobre 2023. [En ligne]. Disponible sur: <https://www.legisquebec.gouv.qc.ca/fr/pdf/lc/A-2.1.pdf>
- [10] « LOI SUR LA GOUVERNANCE ET LA GESTION DES RESSOURCES INFORMATIONNELLES DES ORGANISMES PUBLICS ET DES ENTREPRISES DU GOUVERNEMENT.pdf ». Consulté le: 8 décembre 2023. [En ligne]. Disponible sur: <https://www.legisquebec.gouv.qc.ca/fr/pdf/lc/G-1.03.pdf>
- [11] « Projet de loi no 3 (2023, chapitre 5) Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives ». Consulté le: 21 novembre 2023. [En ligne]. Disponible sur: https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/fr/2023/2023C5F.PDF
- [12] « 2021C25F.pdf ». Consulté le: 17 janvier 2024. [En ligne]. Disponible sur: https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/fr/2021/2021C25F.PDF
- [13] I. Gouvernement du Canada, « Politique des trois organismes sur la gestion des données de recherche - Foire aux questions ». Consulté le: 30 mai 2024. [En ligne]. Disponible sur: <https://science.gc.ca/site/science/fr/financement-interorganismes-recherche/politiques-lignes-directrices/gestion-donnees-recherche/politique-trois-organismes-gestion-donnees-recherche-foire-aux-questions>
- [14] M. D. Wilkinson *et al.*, « The FAIR Guiding Principles for scientific data management and stewardship », *Sci Data*, vol. 3, n° 1, Art. n° 1, mars 2016, doi: 10.1038/sdata.2016.18.

- [15] « researcher-rechercheur-guide-eng.pdf ». Consulté le: 19 octobre 2023. [En ligne]. Disponible sur: <https://cdn.dal.ca/content/dam/dalhousie/pdf/faculty/ardc/researcher-rechercheur-guide-eng.pdf>
- [16] « DG036-Gestion intégrée des risques ». Consulté le: 20 décembre 2023. [En ligne]. Disponible sur: https://intranet.ss.hlaval.reg03.rtss.qc.ca/sites/default/files/dg-036_politique_gestion_integree_des_risques_2018-08-28_jh_vf.pdf
- [17] « dru-014_politique_et_procrdure_2015.pdf ». Consulté le: 4 janvier 2024. [En ligne]. Disponible sur: https://intranet.ss.hlaval.reg03.rtss.qc.ca/sites/default/files/dru-014_politique_et_procrdure_2015.pdf
- [18] « Canadian-Assessment-Framework-w-CA-organizations.pdf ». Consulté le: 19 octobre 2023. [En ligne]. Disponible sur: <https://secureservercdn.net/192.169.221.188/b1f.827.myftpupload.com/wp-content/uploads/2020/04/Canadian-Assessment-Framework-w-CA-organizations.pdf>
- [19] « Planning-for-Success-PIA-Guide.pdf ». Consulté le: 19 octobre 2023. [En ligne]. Disponible sur: <https://www.ipc.on.ca/wp-content/uploads/2015/05/Planning-for-Success-PIA-Guide.pdf>
- [20] « anonymization.pdf ». Consulté le: 27 octobre 2023. [En ligne]. Disponible sur: <https://www.csri.info/wp-content/uploads/2012/08/anonymization.pdf>
- [21] G. consultatif interagences en éthique de la recherche Gouvernement du Canada, « Énoncé de politique des trois conseils : Éthique de la recherche avec des êtres humains – EPTC 2 (2018) – Glossaire ». Consulté le: 23 octobre 2023. [En ligne]. Disponible sur: https://ethics.gc.ca/fra/tcps2-eptc2_2018_glossary-glossaire.html#u