CHU Sainte-Justine
Le centre hospitalier universitaire mère-enfant

Université de Montréal

Univers informationnel (UnIC)

Cadre de gouvernance pour la création et l'exploitation d'un lac de données

CHU Sainte-Justine

Version 2

Novembre 2024

Table des matières

1. Introduction

1.1 Le CHU Sainte-Justine

Mission, vision

Le Centre hospitalier universitaire Sainte-Justine (CHUSJ) est le seul établissement de santé dédié exclusivement aux enfants, aux adolescents et aux mères au Québec. La mission du CHUSJ est d'améliorer la santé des enfants, des adolescents et des mères du Québec, en collaboration avec les partenaires du réseau de santé et ceux des milieux d'enseignement et de recherche. Inspiré par une tradition d'innovation, le CHU Sainte-Justine s'engage à transformer la vie de générations futures.

Le CHUSJ entend assumer pleinement chacun des six mandats découlant de sa mission universitaire :

- Soins spécialisés et ultraspécialisés;
- Recherche fondamentale et clinique en santé de la femme et de l'enfant;
- Enseignement auprès des futurs professionnels de la santé et des intervenants du réseau;
- Promotion de la santé;
- Évaluation des technologies et des modes d'intervention en santé;
- Réadaptation, adaptation et intégration sociale pour les enfants et les adolescents présentant une déficience motrice ou de langage.

Valeurs

Le CHUSJ s'est doté d'un code d'éthique. Les valeurs et la philosophie qui s'y rattachent, présentées dans ce code d'éthique, proviennent de la vision des patients, de leurs proches et de celle des personnes qui y travaillent.

Ainsi les valeurs phares du code sont les suivantes:

- La quête d'excellence;
- La bienveillance;
- Le partenariat;
- L'engagement individuel et collectif.

La philosophie du code s'articule autour d'un concept fondamental pour le CHUSJ, « Tous des soignants! ». Ainsi autant les patients, les familles, les intervenants que les

gestionnaires ont un rôle fondamental et complémentaire à jouer dans la relation au centre de l'action dans nos murs.

1.2 Le Centre de recherche Azrieli

Le Centre de recherche Azrieli du CHUSJ est considéré comme une référence pour la recherche mère-enfant au Canada. Il réunit plus de 295 chercheurs, dont plus de 110 chercheurs cliniciens, ainsi que plus de 450 étudiants de cycles supérieurs et post-doctorants. Le Centre de recherche Azrieli du CHUSJ a démontré son leadership dans plusieurs domaines de recherche. Il poursuit sa mission de faire avancer les connaissances, de développer la santé de précision qui impactera non seulement le diagnostic et la prise en charge des maladies, mais aussi les trajectoires de santé afin de créer un avenir en santé pour les enfants, les adolescents et les mères de l'ensemble du Québec.

1.3 La Direction de la qualité, de l'évaluation, de la performance et de l'éthique (DQEPE)

La Direction de la qualité, évaluation, performance et éthique (DQEPE) a pour mission de soutenir de façon transversale les différentes activités du CHUSJ dans l'éventail des expertises représentées soient notamment la valorisation des données, la protection des renseignements personnels, la qualité, la gestion des risques, le bureau de projet, l'éthique clinique et organisationnelle et le Bureau du partenariat patients-familles-soignants. Pour ce faire, la DQEPE soutient et accompagne de façon personnalisée les différents niveaux de gestion dans la réalisation des activités liées à la mission du CHUSJ.

1.4 La valorisation des données au CHU Sainte-Justine

Dans le cadre de ses missions cliniques, de recherche et d'enseignement, le CHUSJ collecte un volume important de données. La valorisation de ces données est un outil à la disposition du CHUSJ dans une perspective de prise de décisions fondée sur des données probantes, sur l'avancement des connaissances scientifiques, sur le développement des innovations et sur l'amélioration du bien-être de la population du Québec.

Une saine exploitation des sources de données cliniques et clinico-administratives représente un prérequis indispensable pour soutenir le CHUSJ, les gestionnaires, les

cliniciens et les chercheurs dans leurs missions respectives et leurs valeurs communes pour prévenir les maladies et améliorer les pratiques de soins et services.

C'est dans cet optique que le CHUSJ a mis en place une structure de gouvernance des données, dont le Comité stratégique en gouvernance et valorisation des données du CHUSJ (ref. Section 4.1), ainsi que l'infrastructure de l'UnIC.

1.5 Description de l'Univers informationnel (UnIC)

L'Univers informationnel (UnIC) est une infrastructure centralisée du CHUSJ permettant de fournir aux chercheurs, aux cliniciens et aux gestionnaires des données cliniques et clinico-administratives complètes, documentées, organisées et mises à jour afin de promouvoir et faciliter la recherche, l'évaluation et la gestion tout en maximisant la protection de la vie privée et de la confidentialité des renseignements personnels détenus par le CHUSJ. L'UnIC est central pour le développement de la recherche clinique, de l'intelligence d'affaires et de l'intelligence artificielle au CHUSJ et sera la pierre angulaire du nouveau Centre de valorisation des données mère-enfant.

Les données intégrées dans l'UnIC peuvent être utilisées aux fins suivantes :

- Projets de recherche;
- Projets d'amélioration de la qualité;
- Développement d'outils pour la gestion, notamment le développement d'indicateurs de performance et de projets d'intelligence d'affaires.

En tant que centre hospitalier universitaire, le CHUSJ désire être un accélérateur pour la recherche et des pratiques de gestion basées sur des approches en intelligence artificielle. Le CHUSJ souhaite également participer de façon efficiente au processus d'amélioration continue de la qualité des soins et services, en visant notamment la valorisation et l'exploitation des données clinico-administratives dans un contexte de recherche et d'amélioration de la qualité. Contraints par l'absence de solution rapide pour accéder à des données de qualité et par la difficulté de pouvoir transformer et inter relier les systèmes d'information, les chercheurs, les cliniciens et les gestionnaires du CHUSJ demeurent limités dans leur capacité de développer des outils pour la recherche, pour l'aide à la décision clinique et pour la gestion. L'UnIC offre à ces utilisateurs une plateforme intégrée pour soutenir la recherche, la gestion et la prestation de services fondée sur les données massives et des outils informationnels et analytiques, permettant ainsi de répondre à des problèmes complexes inhérents à la santé ainsi qu'à des besoins organisationnels. L'UnIC permet de protéger la confidentialité des renseignements personnels tout en répondant aux besoins des chercheurs, cliniciens et gestionnaires

d’obtenir des données leur permettant d'examiner et de formuler des recommandations sur des questions complexes liées au système de santé et au bien-être des usagers.

L'UnIC est constitué d’un lac de données alimenté systématiquement par les différents systèmes sources du CHUSJ. Ce lac de données inclut une infrastructure d’archivage des données et une série de solutions logicielles qui permettent d’extraire les données des systèmes sources du CHUSJ et de les intégrer dans l’environnement du lac. Les données sources, qu’elles soient de nature clinique, clinico-administrative ou purement administrative, sont comprises dans ce lac de données, organisées dans un entrepôt de données, documentées et rendues accessibles aux chercheurs, aux cliniciens, aux gestionnaires et aux partenaires ayant obtenu les autorisations requises.

Le CHUSJ est fiduciaire des données, incluant les renseignements personnels, intégrées dans le lac de données.

1.6 Portée de ce document

Ce document a notamment pour objectif d’énoncer la structure, les règles et les balises permettant d’encadrer de façon sécuritaire, éthique et efficace le transfert, l’accès, l’utilisation et la communication des données accessibles via l’UnIC. Ce cadre s’articule autour des principes de protection de la vie privée, de quête de l’excellence et de bienfaisance.

Le respect de la vie privée est une valeur fondamentale qui est essentielle à la protection et à la promotion de la dignité humaine. Le non-respect de la vie privée et de la confidentialité peut causer des préjudices à des personnes ou à des groupes de personnes. Ainsi, les renseignements personnels doivent être collectés, utilisés et communiqués de manière à respecter le droit à la vie privée des patients et de leurs proches. Les principes de bienfaisance et de quête de l’excellence, quant à eux, visent l’amélioration des connaissances et le développement de technologies de pointe et collaboratives pour une population en meilleure santé.

Les principes et pratiques de gouvernance rattachées à ce cadre englobent toutes mesures physiques, techniques et organisationnelles permettant d’assurer la sécurité et la confidentialité de l’information tout au long de son cycle de vie.

2. Définitions

Accès aux données : Le droit ou la possibilité de consulter et/ou d'utiliser les données conservées dans une base de données ou un dépôt/un environnement, virtuel ou non.

Chiffrement : Processus de transformation de l'information en un format différent permettant de rendre illisible l'information pour toute personne ne possédant pas la clé de déchiffrement ou le mot de passe.

Couplage : La combinaison ou l'appariement de deux ou de plusieurs ensembles de données possédant des éléments en commun susceptibles de fournir de nouveaux renseignements ou de nouveaux ensembles de données.

Cycle de vie des données : Ensemble des étapes visant le traitement des données soit la collecte, l'utilisation, la communication, la conservation et la destruction ou l'anonymisation de celles-ci.

Dépersonnalisation (brouillage) : Le fait de modifier les renseignements personnels afin de réduire le risque de divulgation de son identité. Cela peut inclure le retrait d'identificateurs directs (ex.: nom, numéro de téléphone, coordonnées géographiques), la transformation (recodage, combinaison) ou la suppression d'identificateurs indirects qui pourraient être utilisés seuls ou en combinaison pour identifier une personne (p. ex. date d'anniversaire, coordonnées géographiques, dates d'événements clés). Lorsque la dépersonnalisation est exécutée convenablement, le risque de réidentification de données partagées ou publiées est atténué[1].

Données brutes : Données présentées sous la forme où elles ont été collectées, avant d'avoir subi un quelconque traitement ou une interprétation. Ces données doivent parfois être soumises à une extraction sélective et requièrent organisation, analyse et formatage avant d'être utilisées[1].

Renseignements confidentiels : Renseignements personnels ou sensibles, dont l'accès, l'utilisation et la communication doivent être restreints et contrôlés.

Fiduciaire des renseignements : Personne physique ou morale qui est responsable de la conservation, de la protection, de l'utilisation et de la saine gestion des renseignements, du respect des droits des personnes dont les renseignements sont conservés et utilisés. À ces fins, il peut élaborer des politiques en lien avec la gestion des renseignements (notamment en ce qui concerne leur accès et leur utilisation). Le fiduciaire applique les exigences légales et réglementaires en lien avec le renseignement et supervise la mise en place de politiques et de processus de gestion des renseignements. À ce titre, le fiduciaire assure notamment les orientations stratégiques et financières liées aux renseignements.

Lac de données : Dépôt de stockage qui contient une vaste quantité de renseignements dans leur format d'origine, y compris des renseignements structurés, semi-structurés et non structurés. À cette fin, tous les renseignements contenus dans le lac de données sont désignés aux fins de ce texte comme étant des "données". La structure des données et les intentions d'utilisation ne sont pas définies tant que les données ne sont pas requises.

Codage : Utilisation d'un code pour désigner une personne, un groupe ou un lieu spécifique afin de supprimer tout lien direct. Le lien ne peut plus être établi en l'absence d'un registre de clé qui permet de faire la correspondance entre le nom fictif ou le code et la personne, groupe ou lieu spécifique. Le codage est un moyen de dépersonnalisation pour protéger l'identité des participants et des organismes impliqués[1].

Renseignement personnel : Renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier, incluant les renseignements de santé et de services sociaux. Le fait qu'une personne soit un usager du CHUSJ constitue un renseignement personnel.

Renseignements d'identification directe : Renseignements permettant d'identifier une personne par des identificateurs directs (ex. : nom, adresse, numéro de téléphone, numéro d'assurance maladie, numéro de dossier CHUSJ, numéro d'employé, photo d'un patient). Certains renseignements en format texte (ex. : notes du médecin) ou des images (ex. : scan d'un patient) peuvent contenir des identifiants directs[1].

Renseignements d'identification indirecte : Renseignements qui peuvent vraisemblablement permettre d'identifier une personne par une combinaison d'identificateurs indirects (ex. : sexe, date de naissance, dates d'évènements (admission, diagnostic, procédure, congé, titre du poste d'un employé), lieux (codes postaux, noms d'établissement de santé, lieu de résidence, caractéristique personnelle distinctive). Certains renseignements en format texte (ex. : notes du médecin) ou des images (ex. : scan d'un patient) peuvent contenir des identifiants indirects[1].

Renseignement anonymisé : Renseignement concernant une personne physique qui ne permet pas d'identifier directement ou indirectement cette personne, et ce, de façon irréversible.

3. Cadre légal

Le cadre légal en matière de protection des renseignements personnels permet, sous certaines conditions, l'utilisation et la communication de ces renseignements à des fins de recherche, de gestion ou d'amélioration de la qualité.

Ce Cadre de gouvernance reconnaît l'importance du droit fondamental au respect de la vie privée inscrit dans la *Charte des droits et libertés de la personne* [3].

Ce Cadre de gouvernance découle des textes législatifs suivants et des règlements qui y sont afférents :

- *Charte des droits et libertés de la personne*;
- *Loi sur les renseignements de santé et de services sociaux*, RLRQ, c. R-22.1;
- *Loi sur la gouvernance du système de santé et des services sociaux,* L. Q. 2023, c. 34;
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1;
- *Loi concernant le cadre juridique des technologies de l'information,* RLRQ, c. C-1.1;
- *Loi sur les archives,* RLRQ, c. A-21.1;
- *Code des professions*, RLRQ, c. C-26 et les codes de déontologie des professionnels du domaine de la santé et des services sociaux.

De plus, il est complémentaire aux politiques et directives internes applicables en matière de protection des renseignements personnels, notamment :

- *Politique de gouvernance des renseignements personnels* (2024-A056-r0);
- *Politique-cadre sur la gouvernance des renseignements cliniques* (POL-2101);
- *Politique sur la confidentialité et l'accès au dossier de l'usager* (POL-2110);
- *Politique de gestion unifiée de l'information et des documents* (2015-A-001-r3);
- *Politique sur le pilotage des systèmes d'information* (2023-A-042-r0);
- *Politique de déclaration et de gestion des incidents et accidents liés aux soins et services* (2011-A-019-r3);
- *Politique et procédure de gestion des événements sentinelles* (2018-A-018-r2);
- *Procédure de gestion des incidents de confidentialité* (2024-A-060-r0);
- *Cadre de référence de l'utilisation des courriels*;
- *Politique générale sur la sécurité de l'information* (2024-A058-r0) ;

- *Cadre réglementaire pour la recherche avec des participants humains* (2021-A-012-r0);
- *Politique relative à l'autorisation et aux autorisations requises pour effectuer de la recherche clinique avec des participants humains sous les auspices du CHU Sainte-Justine* (2021-C-010-r0).

L'architecture, la mise en œuvre et le maintien du fonctionnement de l'UnIC répondent aux directives ministérielles en matière de recherche et de sécurité informatique, incluant :

- La directive sur la cybersécurité [12];
- La directive sur l'utilisation sécuritaire des outils de collaboration par les médecins[13];
- Les termes et conditions d'utilisation des outils de collaboration [14].

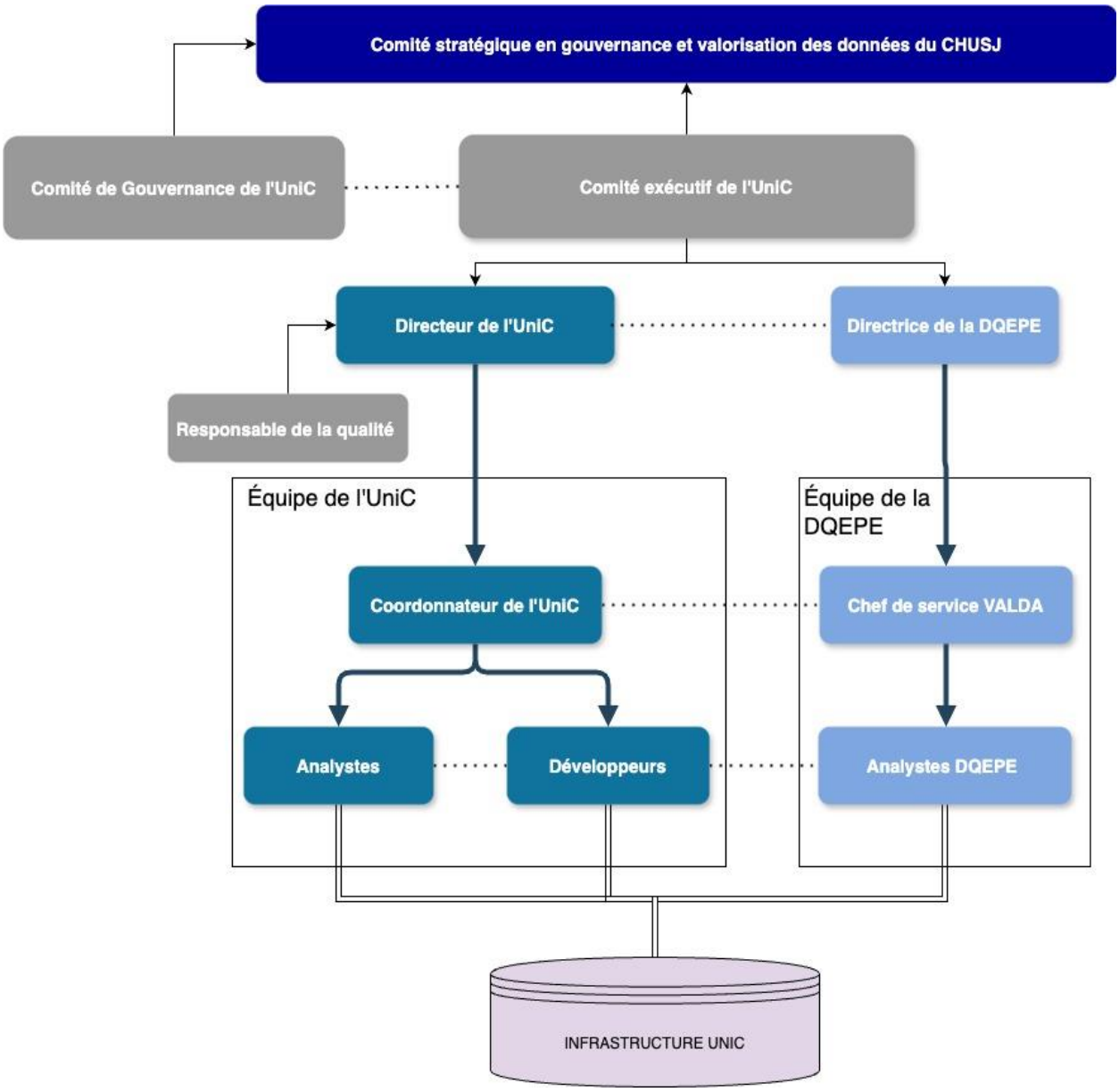
La *Déclaration de principes des trois organismes sur la gestion des données numériques (2016)* [6] a également servi de référence à l'élaboration du présent document.

4. Structure organisationnelle de l'UnIC

La schématisation de la structure de fonctionnement de l'UnIC est présentée sous forme d'organigramme à la figure 1[1].

Figure 1: Structure organisationnelle de l'UnIC

[1] *Dans le présent document, les termes employés pour désigner des personnes sont pris au sens générique; ils ont à la fois valeur d'un féminin et d'un masculin.*



4.1 Comité stratégique en gouvernance et valorisation des données du CHUSJ

Le comité stratégique en gouvernance et valorisation des données du CHUSJ a comme mandat principal de définir la vision, les principes directeurs et les orientations organisationnelles des éléments clés de la gouvernance et de la valorisation des données :

- Le cadre et la définition de la structure et des domaines d'affaires;
- Les rôles et responsabilités de chaque partie prenante;

- Les principes et les politiques organisationnels;
- La stratégie en valorisation des données (ex. : feuille de route, budget, ressources).

Le comité est composé de l'ensemble des directeurs et du président-directeur général adjoint (PDGA). Il est animé par l'adjoint au directeur de la DQEPE.

Le directeur et le coordonnateur de l'UnIC ainsi que les coprésidents du comité de gouvernance de l'UnIC sont présents en tant que membres *ad-hoc* du comité lorsque des sujets en lien avec l'infrastructure de l'UnIC sont à l'ordre du jour.

Le comité stratégique approuve le Cadre de gouvernance selon les recommandations du comité exécutif de l'UnIC.

4.2 Comité exécutif de l'UnIC

Le comité exécutif a comme mandat principal de définir les orientations et les priorités de développement de l'UnIC, notamment en termes d'intégration des systèmes d'information. Le comité exécutif émet des recommandations au comité stratégique en ce qui concerne l'approbation du Cadre de gouvernance et veille à ce que les développements soient conformes aux besoins institutionnels dans le respect des échéanciers et du budget. Dans l'exercice de son mandat, le comité exécutif doit tenir compte des recommandations du comité de gouvernance et du responsable de la qualité et mettre en œuvre les priorités d'action. Le comité exécutif détermine le mandat et la composition du comité de gouvernance de l'UnIC.

Le comité est coprésidé par le directeur de la Recherche (DR) et le directeur de la DQEPE et est composé des membres suivants : le directeur des ressources informationnelles, des stratégies numériques et du génie biomédical (DRISNGBM), le directeur à la gestion des données et infrastructures informatiques de la DR, le directeur de l'UnIC et le coordonnateur de l'UnIC ainsi que l'adjoint au directeur de la DQEPE.

4.3 Comité de gouvernance de l'UnIC

Le comité de gouvernance de l'UnIC a pour mandat de proposer le cadre de gouvernance de l'UnIC et ses mises à jour au comité exécutif en fonction notamment des nouvelles orientations et des nouveaux objectifs institutionnels, des nouvelles pratiques et obligations légales. Il doit, entre autres, offrir son soutien pour le développement des procédures entourant l'accès et définir les modalités d'appariement des données de l'UnIC avec celles des partenaires.

Le comité est coprésidé par le chef du Bureau de l'éthique de la recherche et par le responsable de la protection des renseignements personnels – autre que clinique. Il est composé des membres suivants :

- Un représentant du Bureau de l'éthique de la recherche;
- Un représentant de la DQEPE;
- Un représentant du Service des archives médicales;
- Un représentant du Bureau des affaires juridiques;
- Un représentant de la DRISNGBM;
- Un représentant de la Direction des ressources humaines;
- Le directeur à la gestion des données et infrastructures informatiques de la DR;
- Le directeur de la recherche clinique;
- Un représentant de la pharmacie;
- Un représentant du Bureau du Partenariat Patients-Familles-Soignants ;
- Le directeur de l'UnIC;
- Le coordonnateur de l'UnIC.

D'autres membres peuvent être invités au besoin.

4.4 L'UnIC

4.4.1 Directeur de l'UnIC

Le directeur de l'UnIC assure la direction générale, son suivi régulier, la prise des décisions, la gestion des risques, des finances, des ressources et de l'échéancier de l'UnIC. Ce directeur est nommé par le président-directeur général du CHUSJ. Il veille à ce que tous les membres de l'équipe de l'UnIC respectent les obligations légales et réglementaires, les règles en matière de protection des renseignements personnels et de sécurité de l'information ainsi que les standards de qualité et de rigueur scientifique.

Il a également le mandat de s'assurer que les politiques, les procédures et les pratiques mises en place dans l'équipe de l'UnIC respectent le Cadre de gouvernance établi.

Les tâches ou les responsabilités du directeur de l'UnIC pourraient être déléguées à un membre du personnel si celui-ci possède l'expertise nécessaire pour mener à bien la tâche.

4.4.2 L’équipe de l’UnIC

L’équipe de l'UnIC est constituée d’experts en ingénierie des données massives, en développement d'algorithmes et de solutions en recherche opérationnelle, en gestion des plateformes technologiques et en science de la donnée.

Les scientifiques de la donnée membres de l’équipe de l’UnIC sont responsables de mettre en place les services de traitement, d’extraction, d’analyse des données pour toute demande d’accès pour la recherche et pour les projets d’amélioration de la qualité.

Les membres de cette équipe sont des employés du CHUSJ et travaillent sous la supervision du directeur de l'UnIC.

4.5 La DQEPE

4.5.1 Directeur de la Direction qualité, évaluation, performance et éthique (DQEPE)

Le directeur de la DQEPE s’assure que les membres de son équipe respectent les obligations légales et règlementaires, les règles en matière de protection des renseignements personnels et de sécurité de l’information ainsi que les standards de qualité établis lors de l’exploitation des données de l’UnIC.

Les tâches ou les responsabilités du directeur de la DQEPE pourraient être déléguées à un membre du personnel si celui-ci possède l’expertise nécessaire pour mener à bien la tâche.

4.5.2 L’équipe de la DQEPE

La DQEPE dispose d’une équipe d’experts en valorisation des données incluant des archivistes médicales ayant les compétences d’analyser et d’exploiter les données en fonction des standards et procédures établies. La DQEPE soutient les différentes entités du CHUSJ dans leurs travaux de déploiement d’un système de gestion axé sur les données et la prise de décisions éclairées.

La DQEPE fournit à l’organisation l’expertise en matière d’élaboration et de mise en œuvre de stratégie et de structure de gouvernance visant l’exploitation des données ainsi qu’en matière de protection des renseignements personnels.

Dans le cadre de ces travaux, la DQEPE, en collaboration avec les différentes parties prenantes, s'assure que la confidentialité des renseignements personnels est respectée tout au long du cycle d'exploitation de ces données.

Les membres de la DQEPE sont employés du CHUSJ et travaillent sous la supervision du directeur de la DQEPE. Les scientifiques de la donnée membres de la DQEPE ont un accès à l'UnIC pour assurer la mise en œuvre des projets d'amélioration de la qualité ou de gestion. Ils sont notamment responsables de mettre en place les services de traitement, d'extraction et d'analyse de données en lien avec ces projets.

D'autres scientifiques de la donnée décentralisés œuvrent au sein d'autres directions du CHUSJ, notamment à la direction des ressources humaines et à la direction des ressources financières et de la logistique. Ils ont accès aux données de l'UnIC concernant les activités de leur direction d'appartenance. Ceux-ci sont soumis aux mêmes exigences, règles et responsabilités que les membres de la DQEPE (ex. : formation, engagement de confidentialité.)

4.6 Responsable de la qualité

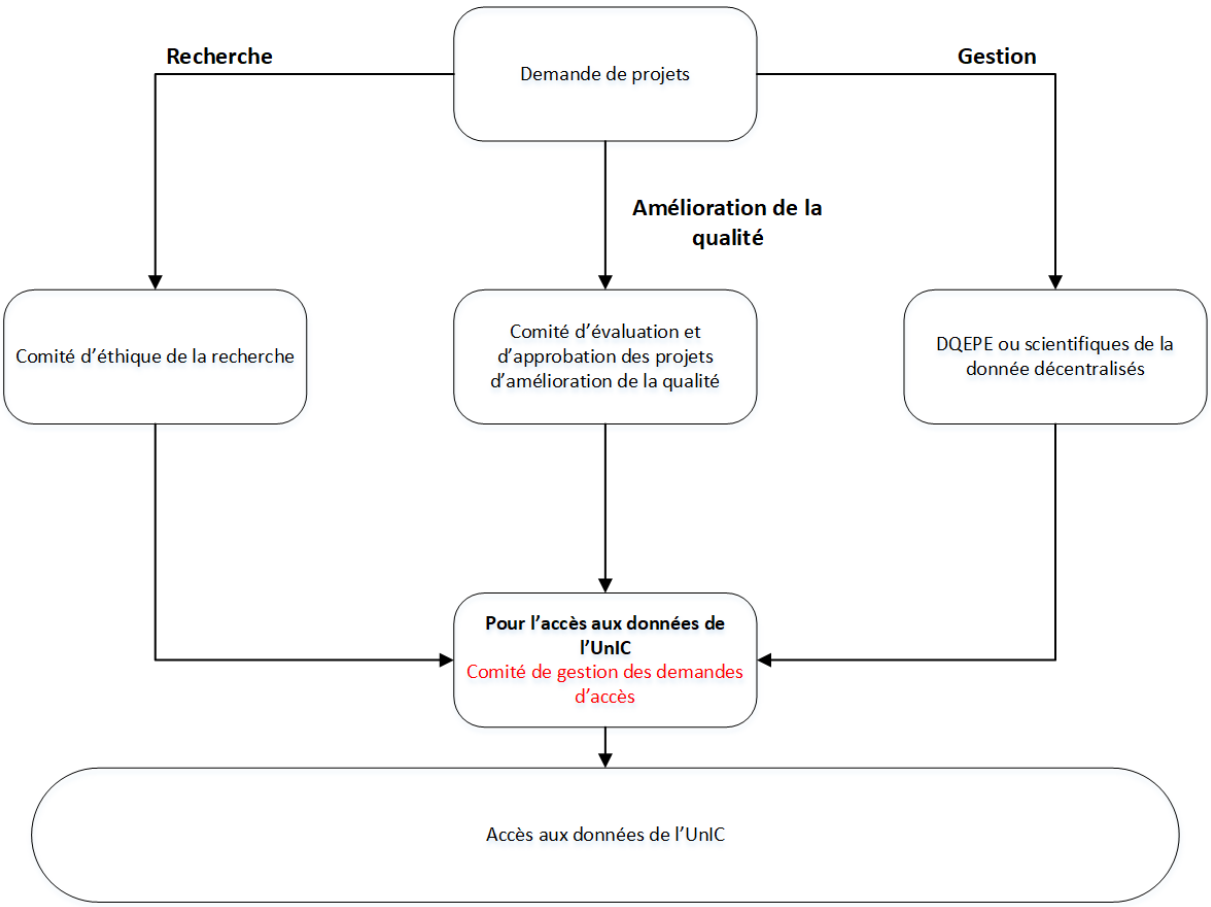
Le responsable de la qualité évalue la qualité et la conformité des services et des processus mis en place par l'UnIC. Dans le cadre de ces fonctions, il doit notamment voir au maintien et à l'organisation des modes opératoires normalisés et effectuer un suivi auprès du comité de gouvernance ainsi qu'auprès du comité exécutif. Le responsable de la qualité effectue toute recommandation qu'il juge pertinente au comité stratégique, au comité exécutif et au comité de gouvernance.

Il s'agit d'un individu employé par le CHUSJ ne faisant pas partie de l'équipe de l'UnIC ou de la DQEPE.

4.7 Les structures encadrant les demandes d'accès

La schématisation de la structure encadrant les demandes d'accès est présentée sous forme d'organigramme à la figure 2.

Figure 2 : Structure organisationnelle encadrant les demandes d'accès



4.7.1 Comité de gestion des demandes d'accès

Le comité de gestion des demandes d'accès au lac de données de l'UnIC veille à la mise en œuvre des accès aux données par les utilisateurs autorisés. Dans l'exercice de ses fonctions, ce comité est appelé à effectuer les tâches suivantes :

- S'assurer que les demandes d'accès aient reçues les autorisations institutionnelles nécessaires.
- Faire une évaluation de la faisabilité des demandes d'accès.
- Faire une évaluation des risques d'identification ou de réidentification des usagers du CHUSJ. Dans certains cas, l'analyse des sous-ensembles de données comportant un risque élevé de réidentification est réalisée par le scientifique de la donnée qui est attitré au projet.

- Déterminer les actions à effectuer sur les données pour réduire le risque d'identification des personnes. Ces actions peuvent inclure, entre autres, le masquage, la suppression, la pondération et l'agrégation des données.
- Proposer des solutions d'accès aux données en fonction des besoins des utilisateurs, tout en prenant en considération les risques.
- Offrir un soutien scientifique aux chercheurs.

Ce comité est composé du coordonnateur de l'équipe de l'UnIC, d'au moins un membre de l'équipe scientifique et, au besoin, d'un administrateur du lac de données et/ou d'un membre de la DQEPE. L'identification des données requises peut nécessiter l'expertise de d'autres professionnels dont les archivistes médicales et les pilotes de système d'information. Toute information relative à une demande d'accès communiquée par le demandeur au personnel de l'UnIC ou à la DQEPE est confidentielle.

4.7.2 Comité d'éthique de la recherche

Le comité d'éthique de la recherche a le mandat d'évaluer l'acceptabilité éthique des recherches qui se déroulent sous les auspices ou l'autorité du CHU Sainte-Justine et qui font appel à des participants humains, incluant toute activités de recherche portant sur des renseignements personnels, et ce, sans égard au niveau de risque des projets.

Le CER a un pouvoir décisionnel.

La recherche, incluant l'accès aux données du lac de données à des fins de recherche, ne peut débuter sans l'approbation du comité d'éthique de la recherche.

En outre, l'accès à des fins de recherche aux renseignements personnels concernant les usagers, en l'absence de consentement, doit être autorisé par le directeur des services professionnels (DSP), sur recommandation du comité d'éthique de la recherche.

4.7.3 Comité d'évaluation et d'approbation des projets d'amélioration de la qualité du CHUSJ

Le comité d'évaluation et d'approbation des projets d'amélioration de la qualité a pour mandat d'évaluer les projets d'amélioration de la qualité soumis par les différentes équipes du CHUSJ. Tout projet d'amélioration de la qualité doit être approuvé par ce comité afin de pouvoir être réalisé au CHUSJ.

Dans le cadre de son évaluation, ce comité peut émettre toute recommandation qu'il juge pertinente.

Ce comité est notamment responsable d'évaluer les accès aux données nécessaires pour la réalisation des projets d'amélioration de la qualité.

Ce comité peut autoriser l'accès aux données et, le cas échéant, assortir cette autorisation de modalités particulières. Au surplus, tout accès aux renseignements personnels concernant les usagers, en l'absence de consentement, doit être autorisé par le directeur des services professionnels (DSP).

5. Données intégrées dans l'UnIC

Les données intégrées dans l'UnIC incluent des données socio-démographiques, cliniques (incluant les données génomiques) et administratives (ressources humaines, finances, etc.) ainsi que des images et des photos médicales (excluant les photos prises à des fins socio-juridiques). Ces données proviennent de plusieurs systèmes sources, incluant mais ne se limitant pas aux services des admissions, départs et transferts (ADT), des ressources humaines, des ressources financières, de la pharmacie, des laboratoires, de l'imagerie médicale et de l'urgence (voir l'annexe A pour la liste complète). Ces données peuvent être sous plusieurs formats, incluant des données en format texte non structuré, des documents numérisés en format PDF, des images en format DICOM, JPEG ou autres. Les données à intégrer peuvent aussi provenir de banques de données de recherche alimentées par les dossiers des usagers. Des systèmes peuvent être ajoutés à l'UnIC en fonction des besoins de la recherche ou d'amélioration de la qualité et de gestion.

Les données brutes provenant de ces systèmes sont intégrées de façon prospective et continue dans leur format d'origine. Les données rétrospectives, qui ont été collectées depuis la mise en fonction des systèmes sources, sont aussi intégrées afin d'obtenir un portrait global de la trajectoire de soins de l'usager depuis la naissance (ou la première date d'admission), jusqu'à la vie adulte. Les données des différents systèmes sources peuvent être appariées en utilisant une clé d'indexation unique à l'exception des données des employés détenues par les ressources humaines qui ne seront jamais appariées aux données cliniques de ceux-ci.

6. Confidentialité et protection des renseignements personnels

L'ensemble des données intégrées à la plateforme de l'UnIC sont des renseignements confidentiels de nature sensible, peu importe leur format et leur provenance. Toutes les données de l'UnIC doivent donc être traitées avec les plus hauts standards en matière de confidentialité et de sécurité de l'information, lesquels sont compatibles avec l'accès aux données à des fins de recherche, de gestion et d'amélioration de la qualité.

Malgré le fait que des identifiants directs (nom, adresse, numéro d'assurance sociale, etc.) sont retirés des jeux de données pour certains projets, l'identification par le biais d'identifiants indirects demeure possible. En ce sens, les données constituent des renseignements personnels soumis aux règles applicables.

En tout temps, il est nécessaire d'appliquer notamment les principes généraux prévus à la Politique de gouvernance des renseignements personnels du CHUSJ lors de l'accès, l'utilisation ou la communication de données hébergées dans l'UnIC :

1. **Nécessité**. Seuls les renseignements personnels nécessaires à l'atteinte des objectifs visés par le projet doivent être collectés, utilisés, conservés ou communiqués. Les identifiants directs sont utilisés uniquement lorsque nécessaire. À défaut, tous les renseignements sont traités de façon dépersonnalisée.

2. **Confidentialité.** Tout renseignement personnel doit être traité avec confidentialité dans le respect des règles prévues par la loi et, lorsqu'applicable, du consentement de la personne concernée (ou de son représentant légal). L'accès à un tel renseignement est permis seulement aux personnes pour lesquelles cet accès est nécessaire pour les fins autorisées.

3. **Sécurité.** Tout renseignement personnel doit être collecté, utilisé, conservé, communiqué et détruit de façon sécuritaire. Des mesures de sécurité rigoureuses et raisonnables selon les circonstances doivent être mises en place afin de protéger la confidentialité des renseignements personnels, et ce, tant au niveau physique qu'informatique.

4. **Destruction dès que possible.** Dès que les fins pour lesquelles une donnée hébergée dans l'UnIC est utilisée sont accomplies, toute copie de cette donnée doit immédiatement être détruite.

Toute personne doit respecter ces principes, qu'il s'agisse de membres de l'équipe de l'UnIC, de la DQEPE, de chercheurs, de cliniciens ou de gestionnaires.

Les principes de protection de la vie privée et de confidentialité constituent l'assise de l'architecture de l'UnIC et des mesures de sécurité s'y rattachant. Ces principes se traduisent par les exigences suivantes : 1) l'application du privilège minimal et de séparation des tâches et 2) la gestion des données en fonction du niveau de risque.

6.1 Mesures organisationnelles

6.1.1 Gestion des permissions

Les membres du personnel de l'UnIC et ceux de la DQEPE, qu'ils aient un profil d'administrateur ou de scientifique de la donnée, doivent utiliser les systèmes et accéder à l'information dans le respect des accès qui leur sont accordés. Ceux-ci ont un identifiant unique et le mécanisme d'authentification permet de vérifier leur identité déclarée. De plus, un registre des responsabilités déléguées est conservé par le directeur de l'UniC et partagé avec le directeur des services professionnels deux fois par année. Les droits d'accès des membres du personnel de l'UnIC et de la DQEPE peuvent être octroyés ou modifiés par l'administrateur de l'UnIC selon les besoins particuliers.

Tout le personnel travaillant avec les données de la plateforme de l'UnIC doit respecter les modalités d'accès au réseau du CHUSJ (incluant la gestion de mots de passe) et prendre toutes les mesures appropriées pour protéger les renseignements confidentiels contre tout vol, perte, interception, utilisation ou divulgation non autorisée, en ayant notamment recours à des mesures de protection, à des méthodes et à des systèmes conformes aux standards des meilleures pratiques.

6.1.2 Formation exigée

Tous les membres du personnel de l'équipe de l'UnIC doivent suivre la formation en éthique de la recherche clinique offerte par le CHUSJ. Cette formation doit être renouvelée tous les trois ans. Cette formation se penche sur les grands principes

régissant la recherche impliquant des humains. Un certificat attestant la complétion de cette formation est exigé avant d'accorder un accès aux ressources de l'équipe de l'UnIC.

Tous les membres du personnel de la DQEPE doivent suivre une formation avancée sur la protection des renseignements personnels et la confidentialité à leur entrée en fonction et à tous les trois ans.

Par ailleurs, tous les membres des deux équipes doivent aussi être sensibilisés régulièrement à l'importance de maintenir la confidentialité des renseignements personnels. Ils doivent se familiariser et se tenir à jour avec certaines politiques et procédures du cadre normatif de sécurité du CHUSJ.

6.1.3 Engagement à la confidentialité

Une enquête sur les antécédents judiciaires réalisée par la Direction des ressources humaines et des communications est requise pour les membres du personnel de l'UnIC et de la DQEPE accédant à l'UnIC. De plus, tous les membres du personnel doivent signer un engagement renforcé à la confidentialité détaillé et spécifique à ces travaux stipulant, entre autres, qu'ils s'engagent à prendre toutes les mesures requises pour protéger la confidentialité des renseignements personnels et à ne les dévoiler à quiconque, que ce soit sous une forme verbale ou écrite, sauf à un autre membre de l'équipe de l'UnIC ou de la DQEPE assujetti à un engagement à la confidentialité ou à un utilisateur secondaire ayant reçu les autorisations nécessaires. Les membres comprennent par ailleurs que le CHUSJ exerce une surveillance continue des accès et de l'utilisation des données et des outils logiciels dans l'environnement de l'UnIC et que tout manquement à leur engagement peut mener à des sanctions. La gestion des engagements à la confidentialité est la responsabilité du directeur de l'UniC.

6.2 Privilège minimal et séparation des tâches

Les membres exploitant l'UnIC sont appelés à effectuer différentes tâches en lien avec la mise en place et le maintien de la plateforme de données. Dans le but de préserver la confidentialité des données, des mesures sont mises en place pour limiter les privilèges d'accès aux stricts besoins. En premier lieu, seuls les membres de l'équipe ayant signé l'engagement à la confidentialité spécifique à l'UnIC et qui œuvrent au développement et au bon fonctionnement de la plateforme de l'UnIC ont un accès aux données dans l'environnement de l'UnIC. Ce personnel doit être qualifié en gestion de données, en programmation et en conception, en développement et en évaluation de plateforme informatique de données massives.

Les individus mandatés ont un des profils suivants : administrateur; ingénieur de la donnée ou scientifique de la donnée pour la recherche, pour la gestion ou les projets d'amélioration de la qualité. En tant qu'utilisateurs, ces individus ont les droits d'accès qui correspondent à leur profil et doivent utiliser les systèmes et accéder à l'information dans le respect des accès qui leur sont accordés. Une journalisation des utilisations et des accès à la plateforme de l'UnIC est effectuée.

Tout le personnel attitré au projet doit respecter les modalités d'accès au réseau du CHUSJ (incluant la gestion de mots de passe) et prendre toutes les mesures appropriées pour protéger les données contre tout vol, perte, interception, utilisation ou divulgation non autorisée, en ayant notamment recours à des mesures de protection, à des méthodes et à des systèmes conformes aux standards des meilleures pratiques.

La plateforme de l'UnIC est compartimentée en trois zones en fonction des niveaux de risque afin de permettre l'application du principe de privilège minimal et de séparation des tâches (annexe B : architecture de la plateforme). Cette architecture de la plateforme de l'UnIC limite les accès aux renseignements personnels à un nombre restreint d'individus.

Les droits d'accès aux zones de la plateforme de l'UnIC sont octroyés uniquement aux personnes pour lesquelles il est nécessaire d'avoir ces droits d'accès. Ces droits d'accès sont autorisés soit par le directeur de l'UnIC, le directeur de la DQEPE, le représentant de la Direction des ressources humaines ou celui de la Direction des ressources financières et de la logistique et ce, selon le type de données. Les personnes ayant des accès aux zones de la plateforme de l'UnIC sont notamment responsables de la gestion des renseignements personnels et des procédures s'y rattachant, incluant le processus de codage et de dépersonnalisation.

L'extraction des données des systèmes sources est effectuée sous la responsabilité de l'équipe de la direction des ressources informationnelles, des stratégies numériques et du génie biomédical (DRISNGBM). La sécurité des données en transit vers le lac est donc sous la responsabilité de la DRISNGBM. Les membres de l'équipe de l'UnIC n'ont pas accès aux bases de données en production des systèmes sources du CHUSJ. Une fois les données extraites, celles-ci sont automatiquement importées de manière cryptée dans un espace sécurisé de l'UnIC (la zone rouge de l'annexe B) accessible qu'à un nombre restreint de membres de l'équipe de l'UnIC et de la DQEPE. C'est dans cet environnement sécurisé que les données sont classées et que des programmes informatiques sont exécutés pour réconcilier les identifiants, créer un identifiant unique

pour chaque patient et exécuter la procédure de dépersonnalisation des données, selon les besoins.

6.3 Gestion des données en fonction des utilisations prévues et du niveau de risque

Le traitement et l'accès aux données de l'UnIC dépendent des utilisations prévues et du niveau de risque. L'UnIC met en place des services et procédures permettant de s'assurer que le partage et l'utilisation des données s'effectuent conformément aux autorisations émises.

Le classement des données est effectué[11,15] en amont de la création des jeux de données pour définir les balises d'accès et de gestion des différents types de renseignements contenus dans le lac de données et sert de guide pour l'évaluation du risque à la réidentification. Les données sont classées selon quatre types :

- renseignement avec identification directe ;
- renseignement avec identification indirecte ;
- renseignements anonymisés ;
- donnée administrative sans référence à une personne.

Un traitement approprié de ces données est appliqué selon les besoins et les autorisations octroyées :

- Lorsque le projet ne nécessite pas un accès à des renseignements avec identification directe, les procédures de dépersonnalisation et de codage sont appliquées dans la zone hautement sécurisée de la plateforme (zone rouge). Les renseignements d'identification directe (annexe C) sont conservés dans la zone sécurisée de la plateforme et exclus des données disponibles pour les scientifiques de la donnée. Un identifiant unique pour chaque personne est créé pour permettre de lier les données des différents systèmes sources. De plus, une fonction de hachage est appliquée aux identifiants pour les rendre illisibles.

- Lorsque le projet nécessite un accès à des renseignements avec identification directe, ces renseignements sont exclus des jeux de données et fournis séparément dans un fichier protégé par un mot de passe. Le fichier comportant des renseignements avec identification direct est généré dans la zone rouge du lac, restreinte aux administrateurs. Dans certains cas, lorsque la séparation des renseignements avec identification directe et des données cliniques ne peut pas

être effectuée (ex. : certains projets de gestion), les scientifiques de la donnée peuvent être appelés à travailler avec des jeux de données comportant des renseignements d'identification directe. Les jeux de données sont alors hébergés dans un environnement dédié, où seuls les scientifiques de la donnée autorisés possèdent un droit d'accès.

Avant de rendre des données disponibles, les autorisations liées à l'utilisation de ces données doivent être validées par le comité de gestion des demandes d'accès. Dans la plupart des cas, les jeux de données sont codés. Pour réduire le risque de réidentification, une transformation des données peut aussi être effectuée; par exemple, la suppression du jour dans les dates. Les décisions concernant le traitement des données pour diminuer le risque de réidentification font appel au jugement du scientifique de la donnée attitré au projet et peuvent se faire en concertation avec le comité d'éthique de la recherche, le comité d'évaluation et d'approbation des projets d'amélioration de la qualité, le comité responsable de l'évaluation des facteurs relatifs à la vie privée, le responsable de la protection des renseignements personnels et le chercheur local.

La transmission de renseignements d'identification directe est possible si l'utilisateur en détient les autorisations. Dans tous les cas, seules les données autorisées sont transférées aux demandeurs.

7. Sécurité de l'information

Plusieurs lois, règlements, directives ou politiques encadrent et régissent l'utilisation et la gestion de l'information, notamment la *Politique générale sur la sécurité de l'information,* qui met en place une gouvernance claire de la sécurité de l'information.

Plus spécifiquement, les objectifs du CHUSJ en matière de sécurité de l'information sont d'assurer :

- le respect de la vie privée des individus, notamment, la confidentialité des renseignements personnels ;
- la disponibilité et l'intégrité de l'information en considérant les utilisations de cette information par le CHUSJ ;
- le respect des mesures de sécurité concernant l'utilisation des actifs informationnels ;
- la conformité aux lois et règlements applicables ainsi qu'aux directives, normes et orientations gouvernementales.

Les mesures physiques mises en place dans le contexte de l'UnIC visent à assurer la confidentialité à tous les niveaux du cycle de vie des données. Celles-ci s'effectuent en respect des politiques et processus du cadre normatif de sécurité de l'information du CHUSJ et des autorités ministérielles. L'élaboration et l'organisation de l'architecture générale du système de sécurité reposent sur le concept de défense en profondeur selon lequel la sécurité ne doit pas reposer sur une seule technologie ou un seul produit de sécurité, mais plutôt sur un ensemble cohérent de stratégies qui doivent être surveillées, protégées et bénéficier d'un plan de réaction et mitigation en cas d'incident.

L'infrastructure de l'UnIC est entreposée sur des serveurs dédiés et protégés au sein des infrastructures du CHUSJ. Le local où sont hébergés les serveurs est verrouillé avec une stricte gestion d'accès.

La gouvernance de la sécurité de l'information est sous la charge du Chef de sécurité de l'information de l'organisation (CISO). Les actifs informationnels de l'UnIC sont soumis aux mêmes standards de sécurité que les données détenues dans les dossiers des usagers du CHUSJ. Seules les personnes responsables de l'organisation et de la maintenance des serveurs dédiés à l'UnIC moyennant une authentification par badge peuvent accéder à l'espace sécurisé des serveurs.

L'architecture technologique contient plusieurs techniques de sécurité afin de réduire l'exposition du système aux différentes menaces, notamment :

- un découpage des zones en fonction des risques, du profil des utilisateurs et des étapes du cycle de vie des données (voir schéma de l'architecture, annexe B) (dans ce cadre, sont rattachées des règles d'accès et de passage de l'une à l'autre des zones) ;
- une journalisation des accès des utilisations de la plateforme ;
- une gestion des accès via un gestionnaire d'accès ;
- l'application de l'authentification forte (double facteurs) lorsqu'un utilisateur veut se connecter à partir d'un point d'accès situé à l'extérieur du RSSS, conforme aux standards du MSSS ;
- le chiffrement des données en transit et au repos ;
- une sauvegarde quotidienne des données ;
- une vérification des sauvegardes semestriellement ;
- une documentation de la gestion de mots de passe système ;
- une mise à jour récurrente des systèmes d'exploitation.

7.1. Évaluation de la vulnérabilité et tests d'intrusion

Les vérifications représentent une composante importante du programme global de sécurité de l'information de l'UnIC. Elles visent à s'assurer du respect des pratiques exemplaires et à mesurer la conformité avec l'ensemble des politiques, procédures et pratiques de sécurité de l'information du CHUSJ. Ces vérifications servent, entre autres, à évaluer la capacité de l'UnIC à protéger l'information et les systèmes contre les menaces et vulnérabilités.

La gestion des vulnérabilités est un exercice mensuel en raison du dynamisme de l'environnement des menaces. Des exercices d'intrusion sont menés sur une base annuelle et au niveau local sur une base plus fréquente. Toutes les recommandations formulées dans le cadre des vérifications font l'objet d'un suivi et les mesures appropriées sont prises le cas échéant.

8. Accès et utilisation des données pour la recherche

8.1 Conditions d'accès

Pour qu'elle soit autorisée, l'utilisation des données hébergées dans la plateforme de l'UnIC pour la recherche doit être conforme au *Cadre réglementaire pour la recherche avec des participants humains* adopté au CHUSJ.

Les projets de recherche pour lesquels toutes les autorisations requises ont été obtenues peuvent faire l'objet d'une demande d'accès aux données de l'UnIC. Ces autorisations comprennent notamment :

- l'approbation du comité d'éthique de la recherche ;
- le consentement des participants/de leur représentant légal ou l'autorisation du DSP (en absence du consentement des participants/de leur représentant légal) ;
- l'approbation du comité de convenance de la Direction de la recherche ;
- l'autorisation de la personne formellement mandatée pour autoriser la recherche au CHUSJ ;
- autres autorisations de détenteurs de données conservées par l'UnIC, si applicables.

L’instigateur de la demande d’accès doit avoir un statut de chercheur au CHUSJ pour pouvoir faire une demande d’accès aux données de l'UnIC. Pour les projets provenant du milieu académique externe au CHUSJ ou pour les projets provenant de l’industrie, une collaboration doit être établie avec un chercheur du CHUSJ préalablement à la demande d’accès aux données.

Aucun document, autre que ceux déposés dans la plateforme Nagano, n’est requis pour l’analyse au Comité de gestion des demandes d’accès.

8.2 Traitement des demandes d’accès

Les demandes d’accès aux données de l'UnIC pour la recherche sont traitées par le comité de gestion des demandes d’accès à la suite de l’obtention de toutes les autorisations requises. L’identification des données requises peut nécessiter l’expertise de d’autres professionnels dont les archivistes médicales et les pilotes de système d’information. Une évaluation de la faisabilité est effectuée dans un délai de cinq jours ouvrables suivant la confirmation des autorisations requises. Plusieurs facteurs peuvent influencer les délais d'accès, notamment la disponibilité de l’instigateur de la demande pour répondre aux questions de l’analyste, la complexité de la demande et l’obtention d’autres autorisations requises. La demande sera toutefois traitée de façon diligente.

Au terme de l’évaluation, l’UnIC rédige l’énoncé des travaux détaillant le plan d’extraction des données, les services offerts et les coûts associés (le cas échéant). Cet énoncé est présenté à l’utilisateur pour approbation. Le bon de travail portant sur les services décrits dans l’énoncé des travaux doit être dûment signé par l’utilisateur.

8.3 Utilisation des données

Tout utilisateur des données de l’UnIC pour la recherche se doit de respecter les règles entourant l’utilisation des données et la publication des résultats de recherche décrits dans ce cadre de gouvernance ainsi que dans toute autre politique du CHUSJ.

Les services de l'équipe de l’UnIC pour les besoins des chercheurs sont sujets à un recouvrement de coûts selon le modèle des plateformes du CHUSJ. L’utilisateur s’engage à payer les coûts pour les services de l’UnIC.

L’utilisateur s’engage à informer l’équipe de l'UnIC advenant la découverte d’erreurs fortuites, telle la présence de renseignements personnels ou de doublons dans les données, afin que celles-ci soient documentées et corrigées.

Si l'utilisateur détecte une incohérence dans les données pouvant avoir un impact sur la prise en charge d'un patient, par exemple, une erreur possible dans le diagnostic, celui-ci devra aviser l'équipe de l'UnIC pour qu'une évaluation du cas soit effectuée. Dans le cas où l'erreur est confirmée, un signalement doit être fait auprès du DSP et à la DQEPE (gestion des risques).

L'utilisateur s'engage à respecter les règles applicables en matière de propriété intellectuelle. Il est à noter que le CHUSJ ne peut revendiquer de droits de propriété intellectuelle du seul fait d'avoir rendu accessible des données de l'UnIC ayant contribué à la réalisation de découvertes, d'inventions ou d'œuvres. En aucun cas, l'utilisateur n'a de droits de propriété intellectuelle sur les données extraites de la base de données ni le droit de commercialiser les données extraites de l'UnIC.

Lors de la publication de résultats de recherche, l'utilisateur s'engage à spécifier que les données utilisées dans l'étude/présentation proviennent de l'UnIC du CHUSJ en documentant les sources de données utilisées. Il est aussi recommandé d'inclure une clause de reconnaissance pour tout autre intervenant ayant permis la collecte ou l'interprétation des données. Ces clauses, fournies par l'équipe de l'UnIC, seront ajustées en fonction des sources de données utilisées. La publication devrait aussi indiquer que toutes les mesures pour préserver la confidentialité des données des personnes concernées ont été mises en œuvre dans le contexte de l'étude.

L'utilisateur s'engage à reconnaitre la contribution d'un membre de l'équipe de l'UnIC lorsque celle-ci respecte les règles en matière de reconnaissance d'auteurs sur les publications[17].

L'équipe de l'UnIC s'engage à publier sur son site web le sommaire des projets utilisant les données de la plateforme. L'équipe de l'UnIC se réserve le droit de contacter l'utilisateur afin de collecter des informations additionnelles visant à mesurer les retombées du projet (publications, présentations à des conférences, etc.).

Lors de la publication, il est possible que certaines revues scientifiques exigent que les données utilisées pour générer les résultats de recherche soient mises à disposition dans un registre public. Dans de telles circonstances, l'utilisateur s'engage à ne pas déposer de jeu de données dans un registre public de données sans l'autorisation formelle du comité d'éthique de la recherche.

Les utilisateurs seront invités à soumettre et à rendre accessible les données d'intérêt qui auraient été générées grâce à l'utilisation des données de l'UnIC. Le contenu et le format des données ainsi que les critères entourant la documentation du code, des

logiciels ou des analyses ayant permis de générer les nouvelles données pourront être soumis et intégrés dans la plateforme de l'UnIC.

L'utilisateur s'engage à aviser le comité de gestion des demandes d'accès de l'UnIC à l'arrivée du terme de la période pour laquelle l'accès a été approuvé et à respecter les exigences relatives à ce qui doit être fait des données concernées. Aucune copie des données ne doit être conservée par l'utilisateur. Au terme du projet, l'utilisateur doit, par conséquent, attester par écrit qu'il n'a pas conservé de copie des données et fournir une attestation de destruction par écrit à l'adresse courriel institutionnelle de l'équipe de l'UnIC. Il est à noter que le code qui a généré les jeux de données et les copies de ces données sont conservés par l'équipe de l'UnIC pour utilisation future.

Les ensembles de données sur lesquels ont travaillé les chercheurs seront conservés dans un répertoire propre au projet pour une durée minimale de 7 ans ou aussi longtemps que prévu par les exigences légales et contractuelles des organismes subventionnaires et partenaires, conformément aux exigences de l'Université de Montréal en matière de conservation de données de recherche[18].

9. Accès et utilisation des données pour les projets d'amélioration de la qualité

9.1 Conditions d'accès

La notion d'amélioration de la qualité (AQ) est une méthodologie qui désigne une approche systémique visant à améliorer les soins et services prodigués aux patients et à leurs proches. Pour mener à bien cet objectif, une structure a été mise sur pied au CHUSJ afin d'accompagner les équipes et de les aider à réaliser des projets d'amélioration de la qualité dans leurs secteurs. Le demandeur de projet doit faire une demande par l'entremise du formulaire de dépôt de projet d'amélioration de la qualité.

Les projets d'amélioration de la qualité pour lesquels toutes les autorisations requises ont été obtenues peuvent faire l'objet d'une demande d'accès aux données de l'UnIC. Ces autorisations comprennent notamment :

- l'approbation du comité d'évaluation et d'approbation des projets d'amélioration de la qualité ;

- le consentement des personnes concernées, de leur représentant légal ou de l'autorisation du DSP (en absence du consentement des participants, de leur représentant légal) ;
- autres autorisations de détenteurs de données conservées par l'UniC, si applicables.

- Si un projet est approuvé, le comité d'évaluation et d'approbation redirigera le demandeur vers l'équipe de l'UnIC ou de la DQEPE, dépendamment de leur capacité respective.

9.2 Traitement des demandes d'accès

Les demandes d'accès aux données de l'UnIC pour les projets d'amélioration de la qualité sont traitées par le comité de gestion des demandes d'accès à la suite de l'obtention de toutes les autorisations requises. Un membre de la DQEPE sera alors invité à se joindre au comité de gestion des demandes d'accès pour évaluer les besoins du projet.

Les demandes d'accès aux données de l'UnIC pour les projets d'amélioration de la qualité sont traitées par le comité de gestion des demandes d'accès à la suite de l'obtention de toutes les autorisations requises. Une évaluation de la faisabilité est effectuée suivant la confirmation des autorisations requises. Plusieurs facteurs peuvent influencer les délais d'accès, notamment la disponibilité de l'instigateur de la demande pour répondre aux questions de l'analyste, la complexité de la demande et l'obtention d'autres autorisations requises. La demande sera toutefois traitée de façon diligente.

9.3 Utilisation des données

Les données communiquées pour un projet d'amélioration de la qualité doivent être utilisés uniquement aux fins de ce projet et conformément aux autorisations émises. Les données doivent être utilisées en respectant les plus hauts standards de confidentialité et de protection des renseignements personnels.

Les résultats des projets d'amélioration de la qualité sont parfois publiés. Le cas échéant, lors de la publication des résultats, l'utilisateur s'engage à spécifier que les données utilisées pour le projet proviennent de l'UnIC du CHUSJ en documentant les sources de données utilisées. Il est aussi recommandé d'inclure une clause de reconnaissance pour tout autre intervenant ayant permis la collecte ou l'interprétation des données. Ces clauses, fournies par l'équipe de l'UnIC ou de la DQEPE seront ajustées en fonction des sources de données utilisées. La publication devrait aussi indiquer que toutes les

mesures pour préserver la confidentialité des données des personnes concernées ont été mises en œuvre dans le contexte du projet.

L'utilisateur s'engage à reconnaitre la contribution d'un membre de l'équipe de l'UnIC ou de la DQEPE lorsque celle-ci respecte les règles en matière de reconnaissance d'auteurs sur les publications[17].

Lorsque le projet est terminé, aucune copie des données ne peut être conservée. Au terme du projet, l'utilisateur doit, par conséquent, attester par écrit qu'il n'a pas conservé de copie des données et fournir une attestation de destruction écrite à l'adresse courriel institutionnelle du comité d'évaluation et d'approbation des projets d'amélioration de la qualité.

10. Accès et utilisation des données pour la gestion

La nature des mandats traités par l'équipe Valorisation des données et analytique (VALDA) de la DQEPE et par les scientifiques de la donnée décentralisés, notamment ceux des ressources humaines, ayant les compétences requises, exige fréquemment des positionnements rapides à l'intérieur de délais restreints. Conséquemment, certaines mesures peuvent être mises en place pour permettre un accès rapide aux sources de données pour soutenir la prise de décision organisationnelle.

10.1 Conditions d'accès

Afin de mener à terme des projets ou des demandes pour la gestion, les gestionnaires, les employés et les médecins de l'hôpital, de concert avec VALDA, peuvent utiliser les données de l'UnIC. Pour être recevable, une demande d'accès relative à la gestion doit préalablement être déposée pour fin d'évaluation de la pertinence, par l'entremise du formulaire de demande de service, valorisation des données et analytique.

Les projets d'utilisation des données à des fins de gestion pour lesquels toutes les autorisations requises ont été obtenues peuvent faire l'objet d'une demande d'accès aux données de l'UnIC. Ces autorisations comprennent notamment :

- l'approbation du gestionnaire du secteur concerné.

La DQEPE est responsable de la gestion générale de ces demandes, incluant l'évaluation du projet et la gestion des ressources à mettre en place pour les réaliser.

10.2 Traitement des demandes d’accès

Les demandes d’accès aux données de l'UnIC pour les projets de gestion seront présentées par la DQEPE dans le contexte du comité de gestion. Le délai de traitement dans le cas de demandes d’information pour la gestion dépendra de la capacité de l’équipe et des priorités organisationnelles.

Les demandes d’accès aux données de l'UnIC pour la gestion sont traitées par le comité de gestion des demandes d’accès à la suite de l’obtention de toutes les autorisations requises. L’accès aux données de l’UnIC dans le cadre d’un mandat de gestion soutenues par l’équipe VALDA ou par les scientifiques de la donnée décentralisés, notamment ceux des ressources humaines, ne fera pas l’objet de facturation.

10.3 Utilisation des données

Les projets de gestion nécessitent un accès rapide à des données non transformées. Des flux de données et un environnement dédié seront utilisés pour permettre de répondre aux besoins de ces projets.

Les données communiquées pour un projet ou une demande de gestion doivent être utilisés uniquement aux fins de ce projet et, le cas échéant, conformément aux autorisations émises. Les données doivent être utilisées en respectant les plus hauts standards de confidentialité et de protection des renseignements personnels.

Lorsque le projet est terminé, aucune copie des données ne peut être conservée.

11. Audits internes et contrôle de la qualité et de la conformité des données

Malgré la mise en place d’un lac de données permettant la mise en commun et l’exploitation des données, il n’en demeure pas moins que la qualité des projets découlant de l’exploitation de l'UnIC est tributaire de la qualité des données collectées par les systèmes sources. Or, l’utilisation de ces données pour des fins de recherche, d’amélioration de la qualité et de gestion comporte certaines contraintes, notamment :

- des contraintes techniques liées au format hétérogène et non structuré des données ;

- des contraintes d'interopérabilité liées à une adhésion variable des systèmes d'information à des terminologies comprenant des codes et des libellés ;
- des contraintes de qualité liées aux erreurs de codage ou autres.

11.1 Mécanismes d'assurance qualité par l'équipe de l'UnIC et de la DQEPE

Dans une perspective d'amélioration continue, l'équipe de l'UnIC mettra en place des procédures et des mécanismes pour assurer une gestion des données qui adhère aux principes FAIR[2]. Ceci inclut, notamment :

- La mise en place d'une procédure permettant d'évaluer l'intégrité des données lors de leur chargement.
- L'utilisation d'opérations visant à réparer, nettoyer, transformer et standardiser les données, notamment en les formatant convenablement, en repérant les erreurs de transposition et les doublons. Le code informatique utilisé pour effectuer ces opérations sera conservé et bien documenté par souci de transparence. Les procédures de transformation ou de nettoyage des données pourront, au besoin, être validées par les pilotes de systèmes.
- La création des dictionnaires de données pour permettre de documenter le contenu des tables de données ainsi que la transformation des données. Le contenu de ces dictionnaires de données pourra, au besoin, être validé par les pilotes de systèmes.
- Un plan de classement de l'espace de stockage pour retrouver facilement les différentes données.
- Une convention de nommage pour identifier les différents types de données.
- Un fichier de métadonnées, basé selon le standard de métadonnées approprié, associé à chaque jeu de données pour les décrire et aider à leur recherche et à leur identification.
- L'ajout d'un identifiant unique et pérenne pour chaque jeu de données.

La traçabilité du cycle de vie d'une donnée sera ainsi assurée de son état initial jusqu'à son état final, en passant par toutes les transformations qui ont eu lieu entre ces étapes.

[2] https://www.go-fair.org

L'équipe de l'UnIC veille à mettre en place un processus de traçabilité permettant de savoir exactement où sont stockées et traitées les données et quels sont les accès qui ont été accordés pour les jeux de données.

Les enjeux de qualité de données sont adressés à la DQEPE, qui en facilitera les corrections par le biais de la structure organisationnelle en gouvernance des données du CHUSJ.

11.2 Mécanismes d'assurance qualité par le responsable de la qualité

L'ensemble de ces mécanismes et procédures feront l'objet d'audits internes de conformité par le responsable de la qualité pour notamment assurer que les lois et le présent Cadre de gouvernance sont respectés, que tous les membres visés ont les formations adéquates, que les processus sont suivis et que les mesures de sécurité sont adéquates.

La qualité et la conformité des services et des processus mis en place par l'UnIC et la DQEPE seront évaluées minimalement à tous les 2 ans par le responsable de la qualité.

12. Appariement avec sources externes

Le couplage des bases de données provenant d'autres organisations que le CHUSJ crée de nouvelles possibilités pour la recherche, mais aussi de nouveaux risques d'atteinte à la vie privée. Lorsqu'approprié et seulement pour l'usage spécifié dans le projet, il est possible que les données de l'UnIC soient appariées ou mises en commun avec d'autres données. Toute liaison ou combinaison des données de l'UnIC avec d'autres sources de données doit être spécifiée dans la documentation du projet et les autorisations requises doivent être obtenues avant l'obtention de l'accès aux données.

Certaines banques de données constituées à des fins de recherche peuvent aussi être appariées aux données clinico-administratives du CHUSJ entreposées dans l'UnIC si le consentement du participant ou de son représentant légal le permet et si toutes les autorisations requises ont été obtenues. Il est à noter que les banques de données constituées à des fins de recherche ont des règles d'accès qui leur sont propres qui doivent aussi être respectées.

13. Adoption, implantation et révision

Le comité stratégique est responsable de l'adoption du cadre défini dans le présent document sous la recommandation du comité exécutif et du comité de gouvernance de l'UnIC. Le directeur de l'équipe de l'UnIC en collaboration avec le directeur de la DQEPE a la responsabilité d'assurer l'implantation et l'application du cadre.

Le document sera revu par le comité de gouvernance tous les deux ans ou selon tout événement qui modifierait les orientations et les objectifs de l'établissement ainsi que le cadre légal ou réglementaire sur lequel il s'appuie.

Historique des révisions

Version	Entrée en vigueur	Résumé des modifications
1	2022-05-26	Version originale
1.1		• Substitution du « détenteur de l'information » par la personne responsable de l'accès aux documents et de la protection des renseignements personnels. • Changement de la description du responsable de la qualité : rôle de veille sur la qualité et la conformité des services et processus plutôt qu'auditeur. • Évaluation des risques par projet : ajout d'information concernant la collaboration avec le CER et responsable de la protection des renseignements personnels. • Prévoir l'ajout du document sur la sécurité de l'UnIC en annexe (dument en cours de révision). • Remplacement de la notion de « contrat d'accès » par le terme énoncé des travaux. • Modification du rôle de l'UnIC qui se limite à assurer la gestion des accès, mais ne fait pas de surveillance concernant les responsabilités des chercheurs en regard de l'utilisation des données. • Substitution du comité d'accès pour le comité de gestion des demandes d'accès. • Mises à jour mineures.
2	Novembre 2024	• Réorganisation du Cadre pour inclure de manière plus détaillé l'accès et l'utilisation des données du lac à des fins de gestion et d'amélioration de la qualité. • Modification de la structure organisationnelle et ajouts de rôles. • Intégration de données supplémentaires dans le lac de données: administratives, ressources humaines, finances, génomiques, images et photographies médicales.

		• Mise à jour du cadre légal. • Mises à jour mineures.

14. Références

1. Portage Network Sensitive Data Expert Group on behalf of the Canadian Association of Research Libraries (CARL). *Sensitive Data Toolkit for Researchers Part 1: Glossary of Terms for Sensitive Data used for Research Purposes*. (2020).
2. *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, chapitre A-2.1.
3. *Charte des droits et libertés de la personne du Québec,* chapitre C-12.
4. *Code civil du Québec*, L.Q. 1991, c.64.
5. *Loi sur les services de santé et les services sociaux*, chapitre *S-4.2*.
6. Innovation, Sciences et Développement économique Canada, du sous-ministre du Canada & Direction générale des communications et du marketing. Déclaration de principes des trois organismes sur la gestion des données numériques. https://science.gc.ca/eic/site/063.nsf/fra/h_83F7624E.html.
7. Direction Qualité, Évaluation, Performance et Éthique. *Politique sur la sécurité de l'information*. (2018).
8. Direction Qualité, Évaluation, Performance et Éthique. *Politique sur la gestion des accès informationnels*. (2017).
9. Direction de la performance et responsable de la sécurité de l'information. *Politique sur les incidents de sécurité informationnelle*. (2019).
10. Direction des services professionnels. *Politique sur la confidentialité et l'accès au dossier de l'usager*. (2019)
11. Direction des services professionnels. *Politique-cadre sur la gestion des renseignements cliniques* (2019)
12. Ministère de la santé et des Services sociaux. *Directive sur la cybersécurité (MSSS-DIR03)*. (2018).
13. Ministère de la santé et des services sociaux. *MSSS-DIR04: Directive sur l'utilisation sécuritaire des outils de collaboration par les médecins*. (2020).
14. Ministère de la santé et des Services sociaux. *Termes et conditions d'utilisation des outils de collaboration*. (2020).
15. Committee on Strategies for Responsible Sharing of Clinical Trial Data, Board on Health Sciences Policy & Institute of Medicine. *Concepts and Methods for De-identifying Clinical Trial Data*. (National Academies Press (US), 2015).
16. Groupe d'experts sur les données sensibles (GEDS) du réseau Portage au nom de l'Association des bibliothèques de recherche du Canada (ABRC). *Boîte à outils pour les données sensibles --- destiné aux chercheurs. Partie 2: Matrice de risque lié aux données de recherche avec des êtres humains*. (2020).
17. International Committee of Medical Journal Editors. *Defining the Role of Authors and Contributors*. (2019).
18. 03000 - Recherche - Gestion de documents et des archives - Université de Montréal. *Archives Université de Montréal* https://archives.umontreal.ca/gestion-de-

documents/regles-de-gestion/03000-recherche/#r03520

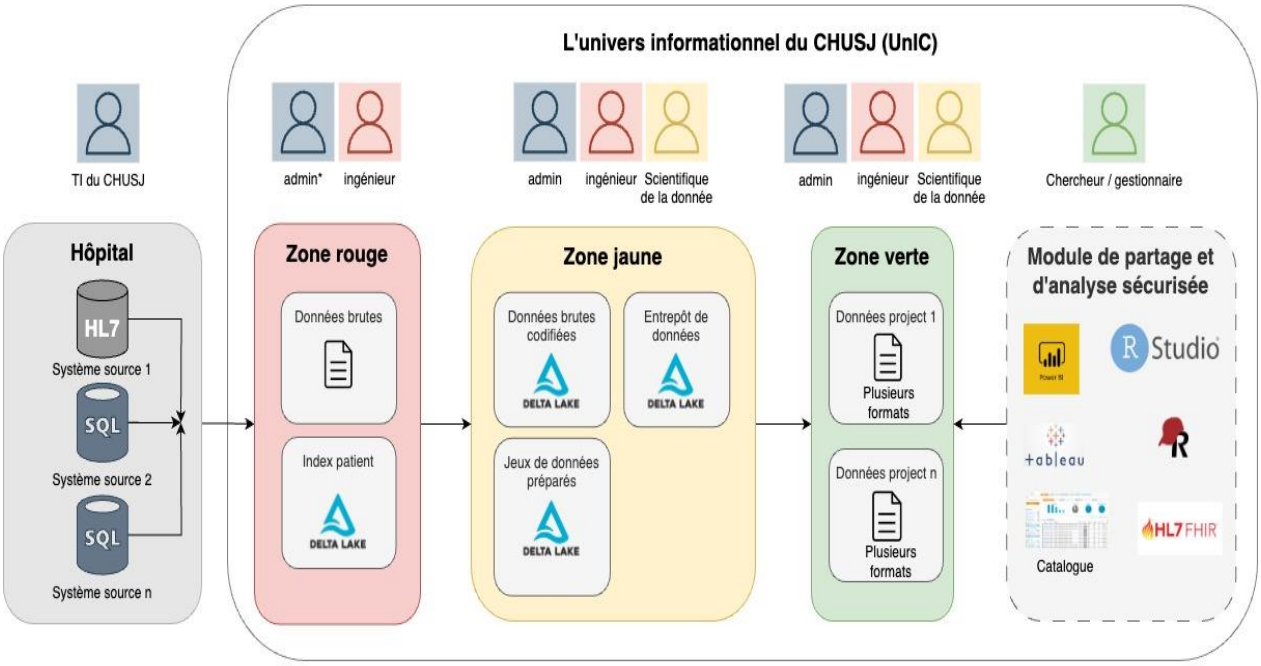
15. Annexes

Annexe A : Liste des systèmes intégrés

Système	Description
clinibaseci	Système source des informations démographiques des patients du CHUSJ (carte bleue de l'hôpital/Index du patient).
eclinibase	Le système de gestion des admissions, départs et transferts regroupant tous les séjours de l'usager allant de la préadmission à l'admission et aux inscriptions en clinique externe ou à l'urgence.
GesPharRx et PANDA	Ce système d'information sert à la gestion des ordonnances et à la gestion de narcotiques ainsi qu'à la gestion de l'administration des médicaments.
opera	Système de gestion du bloc opératoire qui procure les informations pour chaque intervention chirurgicale planifiée, en cours ou réalisée.
medecho	Banque de données qui contient des renseignements personnels clinico-administratifs relatifs aux soins et aux services rendus à une personne, admise ou inscrite en chirurgie d'un jour, au CHUSJ.
radimage	Système de gestion de l'imagerie médicale.
staturgence	Système d'information pour la gestion du département d'urgence, qui permet l'accès rapide aux dossiers des patients et au profil de la clientèle pédiatrique et au profil de la clientèle obstétrique-gynécologie.
softlab	Système d'information pour laboratoires (SIL), qui automatise et gère l'ensemble des traitements des données et des activités de laboratoire.
softmic	Système d'information pour laboratoires (SIL) de microbiologie.
softpath	Système d'information pour laboratoires de pathologie et de génétique.
icca	Dossier numérique des soins intensifs pédiatriques.
philips	Données aux secondes des signes vitaux, respirateurs, pousse-seringues et autres instruments médicaux (pompes à gavage, hémofiltres, etc.).

Chartmaxx-Quanum	Chartmaxx est le dossier informatisé du patient. Cette source comprend les formulaires électroniques provenant de différents services hospitaliers.
centro	Système d'information des cliniques externes du CHUSJ. Cette source comprend tous les formulaires électroniques développés dans les différents services hospitaliers.
etraceline	Système de gestion du laboratoire de la banque de sang.
viewpoint	System de documentation électronique des échographies prénatales du fœtus incluant : les mesures fœtales, les interventions fœtales et les malformations fœtales.
pericalm	Système de surveillance fœtale et d'alertes pour les patientes en obstétrique.
vcardiologie	Rapports en échographie cardiaque incluant les échographies cardiaques fœtales, les chirurgies cardiaques et les autopsies.
unite_des_naissances	Listes des accouchements et naissances au CHUSJ.
cnn	Base de données du Canadian Neonatal Network.
cnfun	Base de données du Canadian Neonatal Follow-up Network et pour le suivi des nouveau-nés après leur séjour en néonatologie.
growthxp	Courbes de croissance.
rop	Base de données de la rétinopathie de prématurité.
NavX	Base de métadonnées concernant les photos médicales.
Nosokos	Système de documentation et gestion des infections nosocomiales

Annexe B : Schéma de l'architecture



* Les administrateurs du Lac incluent les développeurs qui mettent en place les pipelines d'ingestion et dénominalisation et les DevOps qui ont un accès aux serveurs sur lesquels sont hébergées les données

Annexe C : Liste des informations à haut potentiel identificatoire

- Toutes les subdivisions géographiques plus petites qu'un État, y compris l'adresse postale, la ville, le comté, le quartier, le code postal et leurs géocodes équivalents, à l'exception des trois premiers chiffres du code postal
- Tous les éléments de dates (sauf l'année) pour les dates qui sont directement liées à une personne (ex. : date d'admission, date de décès, date de diagnostic, etc.) et toutes les dates (y compris l'année) visant une population de 90 ans et plus
- Numéros de téléphone ou de télécopie
- Identificateurs d'appareil et numéros de série
- Adresses courriel personnelles
- Localisateurs universels de ressources Web (URL)
- Numéros d'assurance sociale (NAS)
- Adresses de protocole Internet (IP)
- Numéros de dossier médical et numéro d’assurance maladie
- Numéro de chambre exact au CHUSJ
- Identifiants biométriques, y compris les empreintes digitales et vocales
- Numéros de bénéficiaires du plan de santé
- Numéro d’employé
- Images ou photographies du visage ou à potentiel identificatoire et toutes images comparables
- Numéros de compte
- Tout autre numéro, caractéristique ou code d'identification unique
- Numéros de certificat et de licence
- Titre d’emploi jumelé à d’autres informations telles que le nombre d’année d’expérience, la direction ou l’unité administrative. Dans certains cas, le titre d’emploi à lui seul permet d’identifier une personne directement.

Annexe D : Documents reliés au Cadre de gouvernance

Titre du document	Description	Status
DOCUMENTS JURIDIQUES		
Engagement à la confidentialité	Engagement renforcé pour les membres du personnel de l'UnIC	V 1.0
Gabarit pour l'énoncé des travaux	Description du plan d'extraction, services offerts et ventilation des coûts	En développement
PROCÉDURES		
Procédure de dépersonnalisation		V 1.0
Procédure d'accès	Accès aux données pour les projets de recherche et les projets d'amélioration de la qualité	V 1.0
Procédure de fin de projet	Procédure administrative de fin de projet	En développement
Procédure pour la découverte d'une erreur fortuite		En développement
Analyse du risque de réidentification	Procédure d'évaluation du potentiel d'identifier un patient dans un jeux de données	En développement
Procédure d'ingestion de données	Procédure décrivant comment les données sont sélectionnées à partir de la base de données d'intégration et déposée dans la zone rouge du Lac de données	En développement
Procédure de cessation d'emploi	Procédure administrative couvrant les étapes suivant l'annonce de cessation d'emploi d'un membre de l'équipe	En développement
Document technique : Architecture du lac de données	Schéma détaillé de l'architecture du lac de données	V 1.0

Mesures de sécurité, confidentialité et protection de la vie privée	Document de spécification des mesures de sécurité, confidentialité et protection de la vie privée	V 1.0