Cadre de gestion du Centre d'intégration et d'analyse des données médicales du CHUM (CITADEL)

Volet recherche

Version préliminaire
En attente d'approbation par le Comité de gouvernance de CITADEL
Février 2019

Le développement du Centre d'intégration et d'analyse des données médicales (CITADEL) du Centre hospitalier universitaire de l'Université de Montréal (CHUM) a été rendu possible grâce à la collaboration étroite de la Direction de la recherche, la Direction de la qualité, de l'évaluation, de la performance et de l'éthique, la Direction des technologies de l'information et des télécommunications et la Direction des affaires médicales et universitaires du CHUM.

Document préparé par :
Camille Craig, Coordonnatrice Carrefour de l'innovation et de l'évaluation en santé
Marie-Josée Bernardi, Directrice Comité d'éthique de la recherche du CHUM
Michaël Chassé, Responsable CITADEL
Carole Jabet, Directrice adjointe de la recherche du CHUM

Cadre de gestion du Centre d'intégration et d'analyse des données médicales du CHUM - volet recherche

Centre d'intégration et d'analyse des données médicales du Centre hospitalier de l'Université de Montréal - volet recherche

Le Centre d'intégration et d'analyse des données médicales (CITADEL) du Centre hospitalier universitaire de l'Université de Montréal (CHUM) s'inscrit dans les initiatives facilitant un CHUM apprenant, enseignant et communiquant. Le principal objectif poursuivi par CITADEL est d'intégrer et analyser les données clinico-administratives du CHUM pour, d'une part, favoriser la prise de décisions fondées sur les données permettant d'améliorer les soins aux patients et d'augmenter la performance du système de soins et, d'autre part, fournir un accès facile, sécurisé, approprié et dans un délai raisonnable à ces mêmes données pour promouvoir et faciliter la recherche, l'évaluation et l'innovation.

Un lac de données qui intègre les données provenant des différents systèmes d'information existants au CHUM a ainsi été développé par CITADEL tel que présenté en Annexe 1. Les données sources, qu'elles soient de nature clinique, administrative, financière, de gestion ou de recherche sont comprises dans les données accessibles via CITADEL. Il est également prévu que la documentation du consentement général du patient, présentement en cours de développement, y soit comprise.

CITADEL est fiduciaire de l'information intégrée dans le lac de données, la propriété de l'information étant détenue par le CHUM. Les données accessibles via CITADEL peuvent être utilisées selon les principes et politiques énoncés dans le présent document.

Le présent document décrit les modalités, exigences et processus pour l'exploitation des données de CITADEL à des fins de recherche. Le processus d'exploitation des données de CITADEL à des fins organisationnelles par les directions du CHUM n'est pas couvert par le présent document.

1. CADRE LÉGAL ET RÉGLEMENTAIRE

Les principes de protection de la vie privée énoncés dans le cadre de gestion de CITADEL sont conformes avec le Code civil du Québec [1] et la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* [2]. Il est à noter qu'un projet de loi modifiant la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* est présentement en cours d'étude [3] ce qui amènera une révision de ce cadre de gestion (voir Section *9. Adoption, Implantation et révision*).

Le cadre de gestion a été développé en cohérence avec les politiques et procédures du CHUM et du Centre de recherche du CHUM notamment :

- *Politique sur la gouvernance de la gestion et de l'exploitation des systèmes d'information* du CHUM [4]
- *Politique cadre sur la gestion de l'information* du CHUM [5]
- *Accès aux données médicales dans un contexte de recherche* (disponible en Annexe 2)
- Politiques et procédures d'approbation éthique du Comité d'éthique de la recherche du CHUM [6]

La *Déclaration de principes des trois organismes*[1] *sur la gestion des données numériques (2016*) [7] a également servi de référence à l'élaboration du présent document.

2. GOUVERNANCE

La gouvernance du Centre d'intégration et d'analyse en données médicales du CHUM fournit un cadre pour que des politiques, procédures, meilleures pratiques et ressources soient mises en place afin d'assurer la protection de la vie privée et de réduire au minimum les risques liés à la sécurité de l'information exploitée par CITADEL. La structure fonctionnelle de CITADEL pour le volet recherche ainsi que les rôles, responsabilités et mandats des comités et équipes impliqués sont détaillés en Annexe 3.

2.1 Rôles et responsabilités[2]

Le *Comité performance et gouvernance des systèmes d'information clinico-administratifs et entrepôts de données,* ci-après *Comité de Gouvernance,* a la responsabilité d'approuver le cadre de gouvernance et de gestion de CITADEL et les politiques et procédures s'y rattachant, ceux-ci étant ensuite déposés pour information au *Comité de direction* du CHUM, ainsi que d'établir les mécanismes de suivis appropriés. Le comité est composé des représentants de différentes directions du CHUM : Direction de la qualité, de l'évaluation, de la performance et de l'éthique (DQEPE), Direction des technologies de l'information et des télécommunications (DTIT), Direction de la recherche (DR), Direction du soutien à la transformation (DSAT), Direction des ressources financières (DRF), Direction du budget et de la performance économique (DBPE), Direction des affaires médicales universitaires (DAMU), Direction des services multidisciplinaires (DSM), Direction des soins infirmiers (DSI), Direction de l'approvisionnement et de la logistique (DAL), Direction des ressources humaines et des affaires juridiques (DRHAJ), Direction générale (DG), Direction des communications et de l'accès à l'information (DCAI), Direction de l'enseignement et de l'Académie CHUM (DEAC). D'autres membres sont invités selon les besoin.

[1] Instituts de recherche en santé du Canada (IRSC), Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG) et Conseil de recherches en sciences humaines (CRSH)
[2] Le genre masculin est utilisé pour décrire les rôles uniquement dans le but d'alléger le texte.

Le *Responsable contrôle qualité* réalise les audits internes de conformité aux procédures et effectue le suivi auprès du Comité de gouvernance. Il s'agit d'un individu employé par le Centre de recherche du CHUM ne faisant pas partie de l'équipe CITADEL.

Le *Comité de pilotage* de CITADEL est responsable de définir les orientations et priorités de développement de CITADEL notamment en termes d'intégration des systèmes d'information, de structuration du lac de données et des entrepôts de données en découlant, ainsi qu'en collaboration avec les utilisateurs, du nettoyage et transformation des données versées dans le lac de données. Le comité comprend le responsable de CITADEL, un représentant de la Direction de la qualité, de l'évaluation, de la performance et de l'éthique, un représentant de la Direction des technologies de l'information et des télécommunications, un représentant de la Direction des affaires médicales et universitaires ainsi que tout autre individu suggéré par le Responsable de CITADEL.

Le *Responsable de CITADEL*, avec le soutien du Responsable des opérations, dirige les équipes opérationnelles (Développement, Intégration & analyse et Bureau d'accès) et doit veiller à ce que son équipe respecte les standards de qualité de de rigueur scientifique. Il a également le mandat de s'assurer que les politiques et procédures et meilleures pratiques mises en place dans l'équipe CITADEL respectent le cadre de gestion établi. Les demandes d'accès aux données de CITADEL sont traitées par le Bureau d'accès et autorisées par le Responsable de CITADEL suite à l'obtention de toutes les approbations requises.

3. DÉFINITIONS

Lac de données : Dépôt de données centralisé exploité par CITADEL dont l'accès est restreint et protégé. Le lac de données ou «data lake» regroupe les données structurées et non structurées des différents systèmes d'information du CHUM. Le lac de données comprend également certaines bases de données constituées à des fins de recherche qui y sont entreposées et qui ont leur propre modèle d'accès.

Entrepôt de données : Ensemble de données extrait à partir du lac de données et ayant subi certaines transformations pour répondre à certains besoins d'exploitation spécifique. L'entrepôt de données est mis à jour aux intervalles de temps autorisés lors d'une requête faite par un utilisateur secondaire. Un ou plusieurs sous-ensembles de données d'analyse peuvent être extraits d'un entrepôt 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.

Copie de sous-ensemble de données d'analyse : Copie identique du sous-ensemble de données d'analyse extrait conservé à des fins d'archivage et de documentation.

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 digitale, un son.

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) [9].

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

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 CITADEL.

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.

4. VIE PRIVÉE ET CONFIDENTIALITÉ

L'exploitation des données de CITADEL à des fins de recherche est rendue possible par la définition de principes transparents de protection de la vie privée et de la confidentialité des individus et par la mise en place des mesures rigoureuses s'y rattachant. La protection de la vie privée et de la confidentialité s'articule autour des principes suivants i) classement des éléments provenant des systèmes sources, ii) séparation des éléments avec identifiants directs des autres éléments, iii) évaluation du risque à la ré-identification des données extraites du lac de données pour chacun des projets approuvés et iv) maintien d'un niveau de risque acceptable. La *Procédure de gestion de la sécurité et de la confidentialité des données* détaille les mesures mises en place tout au long du processus de gestion des données pour assurer la sécurité et la confidentialité des données. Les mesures générales de sécurité de l'information sont détaillées dans la section 5.

4.1 Classement des éléments du lac de données principal

Le lac de données exploité par CITADEL contient des éléments avec identifiants qui sont essentiels pour lier les informations provenant des différents systèmes d'information. Le classement des éléments au préalable est requis pour définir les balises d'accès et de gestion des différents types d'information contenue dans le lac de données et sert de guide pour l'évaluation du risque à la ré-identification. Les éléments sont classés en trois principaux types [10]:

Éléments avec identifiants directs : Un ou plusieurs éléments pouvant être utilisés seuls ou en combinaison avec d'autres sources d'information facilement accessibles pour identifier un individu (ex.: nom, adresse, numéro de téléphone, numéro d'assurance maladie, numéro de dossier CHUM, photo d'un patient). Certains éléments en format texte (ex. : notes du médecin) ou des images (ex. : scan d'un patient) peuvent contenir des identifiants directs.

Éléments avec identifiants indirects ou quasi-identifiants : Éléments pouvant être utilisés seuls ou en combinaison pour identifier un individu avec la connaissance du contexte (ex. : sexe, date de naissance, dates d'événements (admission, diagnostic, procédure, congé), lieux (codes postaux, noms d'établissement, régions)). Certains éléments en format texte (ex. : notes du médecin) ou des images (ex. : scan d'un patient) peuvent contenir des identifiants indirects.

Autres éléments : Éléments ne permettant pas la ré-identification d'un individu.

4.2 Séparation des éléments avec identifiants directs des autres éléments

Le principe de séparation consiste à conserver les données contenant les identifiants dans un espace distinct sur les serveurs des données propres aux patients (ex. : données cliniques) et d'en limiter l'accès. Seuls les utilisateurs principaux détiennent des privilèges d'accès aux systèmes contenant les identifiants ainsi qu'aux autres données détenues par CITADEL pour des fins de développement, d'intégration et d'opérationnalisation, d'exploitation et d'analyse. Par ailleurs, il est possible que certains utilisateurs secondaires ayant constitué leur propre base de données pour un projet de recherche autorisé détiennent les identifiants directs de leurs participants. Ces identifiants directs pourraient éventuellement être transmis aux utilisateurs principaux à des fins de préparation des sous-ensembles de données pour les demandes d'accès aux données de CITADEL ayant été approuvées. Il est à noter qu'aucun identifiant supplémentaire ou autres informations pouvant permettre d'identifier un individu et ne faisant pas partie des autorisations obtenues pour le projet approuvé ne sera transmis au cours de ce processus.

4.3 Évaluation du niveau de risque à la ré-identification

Le processus de dé-identification des données est décrit en détails dans la *Procédure de gestion de la sécurité et de la confidentialité des données*. Celui-ci doit être vu comme un continuum où, dépendamment de la visée et des objectifs du projet, différents niveaux de dé-identification sont requis. Une évaluation du risque de ré-identification par les données est réalisée pour chacun des sous-ensembles de données d'analyse produit afin d'assurer un risque de ré-identification acceptable.

L'évaluation du risque à la ré-identification permet d'attribuer à un entrepôt de données ou à un sous-ensemble de données d'analyse l'un ou l'autre des niveaux de risque suivant :

Risque élevé : L'entrepôt de données ou le sous-ensemble de données d'analyse comprend des éléments avec identifiants directs ou suffisamment d'identifiants indirects pouvant être utilisés pour identifier un individu.

Risque modéré: L'entrepôt de données ou le sous-ensemble de données d'analyse comprend des données potentiellement dé-identifiées (éléments avec identifiants ayant été manipulées afin de les dé-identifier, mais pouvant être partiellement exposés à la ré-identification).

Risque faible : L'entrepôt de données ou le sous-ensemble de données d'analyse contient des données dé-identifiées (ne contient aucun élément avec identifiants directs et les éléments avec identifiants indirects ont été manipulés pour assurer un niveau acceptable de risque à la ré-identification).

L'évaluation du risque de ré-identification est réalisée par l'utilisateur principal de CITADEL attitré à un projet spécifique et celle-ci doit être approuvée par le responsable des opérations. Cette évaluation est réalisée dans le contexte spécifique du projet faisant l'objet d'une demande d'accès, un ensemble de données comportant un risque de ré-identification acceptable dans un projet pouvant ne pas se transposer dans le contexte d'un autre projet. La transmission d'éléments comportant un risque de ré-identification modéré ou élevé est possible dans les situations où l'utilisateur secondaire détient les autorisations requises. Pour toutes les autres situations, les données fournies seront dé-identifiées conformément à la *Procédure de gestion de la sécurité et confidentialité des données*.

4.4 Maintien d'un niveau de risque acceptable

Certaines manipulations sur les éléments d'un sous-ensemble de données d'analyse peuvent être requises pour assurer un risque de ré-identification acceptable et sont réalisées par l'utilisateur principal de CITADEL attitré au projet avant le transfert des données à l'utilisateur secondaire. C'est le cas de certaines données associées à la prestation de soins, pouvant contenir des informations sensibles telles que les noms d'individus ou numéros (ex. : données textuelles contenues dans les dossiers médicaux, images, etc.), qui nécessitent un traitement préalable pour supprimer les identifiants. D'autres manipulations telles que le masquage (ex. : masquage des résultats d'analyse avec un n<5 [11], la généralisation (ex. : création de catégorie 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 « outlier » permettant d'identifier potentiellement un individu), pour n'en nommer que quelques-unes, peuvent également être employées.

5. SÉCURITÉ DE L'INFORMATION

La sécurité de l'information doit être assurée tout au long de son cycle de vie allant de sa création à sa destruction. Les données intégrées dans le lac de données de CITADEL étant une copie des données

des systèmes d'informations existants au CHUM, celles-ci ont un cycle de vie distinct couvrant l'intégration, la structuration, la conservation, la validation, l'utilisation et la destruction des données. 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 ont été mises en place et sont détaillées dans la *Procédure de gestion de la sécurité et de la confidentialité des données*. Ces mesures sont conformes avec les politiques et procédures implantées par la Direction des technologies de l'information et des télécommunications (DTIT) qui veille à l'intégrité et à la sécurité des données notamment en assurant la redondance des structures et systèmes mis en place au CHUM ainsi que la conservation et l'archivage des données des systèmes sources selon le calendrier de conservation de l'établissement.

5.1 Entreposage et organisation des données

Le lac de données ainsi que les entrepôts de données et sous-ensembles en découlant sont entreposés sur des serveurs dédiés à CITADEL et protégées au sein des infrastructures du CHUM. Ils sont soumis aux mêmes standards de sécurité que les données patients du CHUM. Seules les personnes responsables de l'organisation et de la maintenance des serveurs dédiés à CITADEL moyennant une authentification par badge peuvent accéder à l'espace sécurisé des serveurs.

Les serveurs dédiés à CITADEL consistent en une série de serveurs matériels sur lesquels sont installés un réseau de nœuds virtuels utilisés pour extraire, traiter, redistribuer, intégrer, entreposer et analyser les données du CHUM, le tout sur des espaces de stockages contenus au sein des infrastructures du CHUM.

Seuls les utilisateurs principaux de CITADEL détenant le privilège ont accès aux clefs des identifiants qui permettent l'appariement aux données de CITADEL.

5.2 Gestion des accès et traçabilité

Un processus de gestion des accès a été mis en place afin d'assurer la traçabilité et le contrôle des accès aux données de CITADEL. Seuls les utilisateurs principaux détenant le privilège peuvent accéder aux serveurs de CITADEL. Les utilisateurs secondaires accèdent aux sous-ensembles de données d'analyse, entreposés isolément des autres données de CITADEL, via des machines virtuelles dédiées à cette fin.

Un registre des individus s'étant connectés aux serveurs production et/ou de développement pourra être consulté en tout temps par le Responsable de CITADEL ou par le Comité de gouvernance. Le registre des connexions aux serveurs sera également déposé au Comité de gouvernance à tous les trois mois (voir section *6. Conformité*).

5.3 Transfert et analyse des données

Les mesures de sécurité mises en place pour l'hébergement, le transfert et l'analyse des données de même que pour la diffusion des résultats d'analyse sont dépendantes du risque de ré-identification

associé au sous-ensemble de données d'analyse. L'analyse des sous-ensembles de données comportant un risque élevé de ré-identification est réalisée par l'utilisateur principal de CITADEL attitré au projet et approuvé par le responsable des opérations. L'accès à des données à haut risque n'est accordé à un utilisateur secondaire que s'il a obtenu les approbations éthiques et toutes autres autorisations requises. Les mesures sont détaillées dans le Tableau 1.

Tableau 1 : Risque de ré-identification et considérations liées à l'hébergement, au transfert, à l'analyse des données et à la diffusion des résultats

Risque de ré-identification	**Hébergement des données d'analyse et transfert**	**Analyse des données et diffusion des résultats**
Risque élevé	• Sous-ensemble de données d'analyse hébergé sur les serveurs de CITADEL • Aucun transfert du sous-ensemble de données possible	• Analyse réalisée par un utilisateur principal de CITADEL • Partage des résultats à l'utilisateur secondaire sous forme de données agrégées
Risque modéré	• Sous-ensemble de données d'analyse hébergé sur les serveurs du CITADEL • Aucun transfert du sous-ensemble de données possible	• Analyse pouvant être réalisée par un utilisateur secondaire avec les outils d'analyse des systèmes de CITADEL • Partage des résultats à l'utilisateur secondaire après vérification de l'absence de risque de ré-identification par l'utilisateur principal de CITADEL
Risque faible	• Sous-ensemble de données d'analyse pouvant être hébergé hors des serveurs de CITADEL • Transfert du sous-ensemble via le répertoire partagé CHUM de l'utilisateur secondaire ou autre mode de transfert autorisé	• Analyse pouvant être réalisée par un utilisateur secondaire avec les outils de son choix • Aucune restriction quant au partage des résultats

Dans le cas où un transfert d'information serait autorisé auprès d'une ressource externe (de l'interne vers l'externe ou l'inverse), les données seront encryptées et le transfert effectué selon les standards établis [12].

5.4 Archivage et conservation des données

Une copie de chacun des sous-ensembles de données d'analyse préparés pour les projets approuvés (ou le script de reconstruction correspondant) sera conservée sur les serveurs de CITADEL. Un registre des sous-ensembles incluant le nom du projet approuvé, le type de données utilisées de même que la version de l'ensemble de données, identifiée de façon séquentielle, dont il est issu sera maintenu. Le script ayant servi à la production du sous-ensemble, sa version, la date de production et la structure de données au moment de la production seront préservés afin de pouvoir reconstruire de façon identique le sous-ensemble au besoin. Lorsqu'approprié, le sous-ensemble de données pourrait ainsi être détruit pour optimiser l'espace nécessaire sur les disques pour l'archivage et la conservation des copies de sous-ensembles de données d'analyse.

5.5 Formation

Les membres du personnel de CITADEL doivent signer une entente de confidentialité, renouvelable tous les deux ans, spécifiant qu'ils s'engagent à respecter les politiques mises en place au CHUM pour la protection de la vie privée et la sécurité de l'information. Une formation adéquate sur les différentes politiques et procédures est également réalisée avec les utilisateurs principaux ayant à manipuler les données de CITADEL.

6. CONFORMITÉ

Des mesures de suivi régulier sont mises en place par le Comité de gouvernance afin d'assurer la conformité au cadre de gestion de CITADEL et des politiques et procédures s'y rattachant notamment en ce qui concerne l'utilisation des données rendues disponibles via CITADEL. À cet effet, la liste des instigateurs d'une demande d'accès aux données de CITADEL incluant le titre du projet et le statut de la demande et le registre des connexions aux serveurs sont préparés par le Bureau d'accès et déposés au Comité de gouvernance tous les trois mois. De plus, le Comité de gouvernance rapporte annuellement à la direction générale du CHUM la liste des projets ayant obtenu l'autorisation d'utiliser les données de CITADEL.

Une évaluation des facteurs relatifs à la vie privée, largement inspiré des modèles existants [13, 14], est également réalisée au besoin ou lorsqu'une modification au cadre de gestion ou aux politiques et procédures est effectuée. Finalement, des audits internes de conformité et de contrôle qualité des procédures de CITADEL sont réalisés par le Responsable contrôle qualité à tous les ans, ce dernier se rapportant au Comité de gouvernance de CITADEL.

7. ACCÈS AUX DONNÉES

7.1 Conditions d'accès

Les projets de recherche pour lesquels toutes les autorisations requises ont été obtenues (approbation du comité d'éthique de la recherche, approbation du Directeur des services professionnels, autorisation d'effectuer de la recherche par le Directeur de la recherche, autres approbations d'organismes détenteurs de données si applicable) peuvent faire l'objet d'une demande d'accès aux données de CITADEL. L'instigateur de la demande d'accès doit être un utilisateur interne CHUM (i.e. individu ayant un statut de chercheur au CHUM ou un résident). Pour les projets provenant du milieu académique externe au CHUM ou les projets provenant de l'industrie, une collaboration doit être établie avec un chercheur du CHUM préalablement à la demande d'accès aux données. L'accès aux données de CITADEL à des fins d'enseignement (ex. étudiant réalisant un stage nécessitant des données de CITADEL ne s'inscrivant pas dans le cadre d'un projet de recherche) est possible sous certaines conditions et évalué au cas par cas.

Suite à l'obtention de toutes les autorisations requises, l'*Entente d'accès aux données* doit être dûment signé par l'utilisateur secondaire, le Responsable de CITADEL et le Directeur de la recherche du CHUM, pour permettre le transfert et l'utilisation des données de CITADEL. Le modèle général d'accès aux données de CITADEL est présenté en Annexe 4. Les principes généraux d'accès aux données sont décrits ci-dessous.

Le Responsable de CITADEL se réserve le droit de suggérer que l'instigateur de la demande d'accès soit accompagné par l'équipe scientifique de CITADEL pour obtenir du soutien méthodologique lorsque jugé nécessaire.

7.2 Délai 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 de l'instigateur de la demande pour répondre aux questions de l'analyste, la complexité de la demande (ex.: interrogation complexe de la base de données pour évaluer la faisabilité) et l'obtention d'autres autorisations requises.

7.3 Coût des services

Les demandes d'accès aux données et de services à CITADEL sont sujettes à un recouvrement de coût selon le modèle des plateformes du CRCHUM. L'évaluation de la faisabilité détaillée permet de quantifier les coûts qui seront spécifiés dans *l'Entente d'accès aux données*. Les estimés sont sujets à changement advenant que des modifications soient apportées au projet.

7.4 Responsabilités de l'utilisateur secondaire

En tout temps, l'utilisateur secondaire s'engage à respecter les bonnes pratiques en matière de conduite responsable en recherche relativement à la manipulation des données tel que demandé par le FRQ [15].

7.4.1 Confidentialité et protection de l'information personnelle

L'utilisateur secondaire est responsable tenir à jour la liste des individus qui collaborent au projet ou qui ont accès au sous-ensemble de données d'analyse provenant de CITADEL pour le projet approuvé. L'utilisateur secondaire est également responsable de rapporter immédiatement à CITADEL tout bris de confidentialité en lien avec le sous-ensemble de données d'analyse du projet approuvé afin que les mesures préventives ou correctives soient appliquées conformément à la *Procédure de gestion des bris de confidentialité*.

7.4.2 Découverte d'une erreur fortuite

L'utilisateur secondaire est responsable d'informer CITADEL advenant la découverte d'une erreur fortuite dans le sous-ensemble de données d'analyse du projet approuvé afin que les corrections nécessaires soient apportées au sous-ensemble de données produit.

7.4.3 Propriété intellectuelle

Dans le cas où une collaboration de recherche est établie autour du projet utilisant les données de CITADEL, l'utilisateur secondaire s'engage à respecter les règles applicables en matière de propriété intellectuelle selon la collaboration établie.

7.4.4 Reconnaissance des auteurs

L'utilisateur secondaire s'engage à reconnaître la contribution d'un membre de l'équipe CITADEL lorsque celle-ci respecte les règles en matière de reconnaissance d'auteurs sur les publications [16].

7.4.4 Publications

L'utilisateur secondaire est responsable de remettre à CITADEL une copie du manuscrit rapportant les résultats du projet utilisant les données de CITADEL dans un délai de 30 jours ouvrables avant la date prévue de publication. Toute publication ou présentation utilisant les données de CITADEL doit inclure la mention suivante :

«Les Données utilisées dans cette étude/présentation proviennent du Centre d'intégration et d'analyse des données médicales (CITADEL) du Centre hospitalier de l'Université de Montréal (CHUM).»

et inclure une référence au site web de CITADEL.

7.4.5 Résultats

Une fois le projet terminé, les résultats doivent être partagés avec CITADEL sous la forme d'un rapport final à remettre au Bureau d'accès de CITADEL conformément à la *Procédure de fermeture d'un projet*. De plus, CITADEL se réserve le droit de contacter l'utilisateur, après la soumission du

rapport final, afin de collecter des informations additionnelles visant à mesurer les retombées du projet (publications, présentations à des conférences, etc.).

7.4.6 Destruction des données

Une date de début et une date de fin de projet seront établies avec l'utilisateur secondaire et spécifiées dans l'*Entente d'accès aux données*. Le sous-ensemble de données d'analyse du projet approuvé a ainsi un usage limité dans le temps et devra être détruit à la fin du projet ou selon la période de temps définie. Le Bureau d'accès effectuera le suivi avec l'utilisateur lui demandant d'apposer sa signature sur un certificat de destruction de données qui indique la date à laquelle le sous-ensemble de données a été détruit conformément à la *Procédure de fermeture d'un projet*. Il est à noter que les copies de sous-ensembles de données d'analyse entreposés par CITADEL sont conservées à des fins d'archivage (voir section *5.4 Archivage et conservation des données*).

7.5 Transparence

L'information sommaire (titre et résumé) des projets approuvés utilisant les données de CITADEL seront rendus disponibles dans l'intranet du CHUM par le Bureau d'accès.

8. APPARIEMENT ET MISE EN COMMUN DES DONNÉES

Lorsqu'approprié et seulement pour l'usage défini spécifié dans le projet approuvé et pour un temps limité, il est possible que les données de CITADEL soient appariées ou mises en commun avec d'autres données. Toute liaison ou combinaison des données de CITADEL avec d'autres sources de données doit être spécifiée dans la demande d'accès et les autorisations requises doivent être obtenues avant l'obtention de l'accès aux données de CITADEL.

Certaines bases de données constituées à des fins de recherche sont entreposées à CITADEL (ex. : données associées à la biobanque d'un chercheur en particulier). Il est à noter que les bases de données constituées à des fins de recherche ont des règles d'accès qui leurs sont propres. Aucune liaison avec les données clinico-administratives du CHUM et les bases de données constituées à des fins de recherche ne peut être effectuée sans l'obtention de tous les accords préalables (approbation du comité d'éthique de la recherche, approbation du Directeur des services professionnels, autorisation d'effectuer de la recherche par le Directeur de la recherche, autres approbations d'organismes détenteurs de données si applicable).

9. ADOPTION, IMPLANTATION ET RÉVISION

Le *Comité de gouvernance* est responsable de l'adoption du cadre défini dans le présent document et de mettre en place les mécanismes pour assurer la conformité des politiques et procédures s'y rattachant.

Le *Responsable de CITADEL*, avec le soutien du *Responsable des opérations*, 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 le cadre légal ou réglementaire sur quel il s'appuie pour s'assurer de sa cohérence avec la législation actuelle et les meilleures pratiques. Lorsqu'aucune modification n'intervient dans le délai ou pour quelques raisons que ce soit, la dernière version du document demeure néanmoins en vigueur.

Le *Cadre de gestion du Centre d'intégration et d'analyse des données médicales du CHUM* et les principales procédures associées sont disponibles sur demande.

10. DOCUMENTS RELIÉS

Le cadre de gestion est le document principal du plan de documentation de CITADEL auquel plusieurs documents et procédures sont rattachés. Les documents et procédures reliés au cadre de gestion sont disponibles en Annexe 5. Il est à noter que les documents et procédures sont présentement en développement.

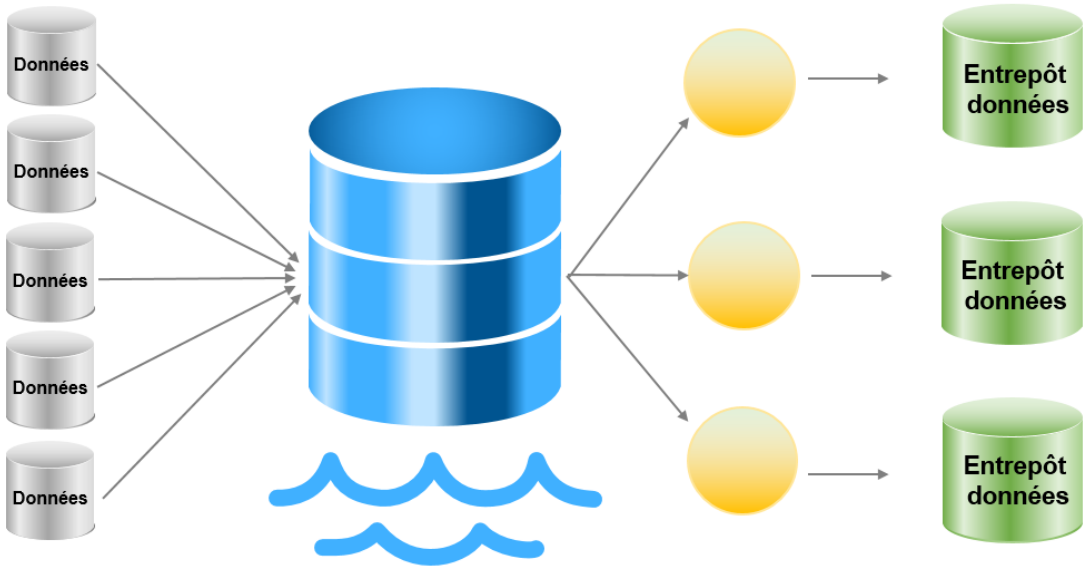
11. REMERCIEMENTS

L'équipe de CITADEL tient à remercier l'équipe du Performance Measurement (Hôpital d'Ottawa – Institut de recherche de l'Hôpital d'Ottawa) pour le partage de la documentation en lien avec l'entrepôt de données de l'Hôpital d'Ottawa qui a grandement servi à l'élaboration du cadre de gestion de CITADEL et des procédures s'y rattachant.

12. RÉFÉRENCES

1. *Code Civil du Québec.* http://legisquebec.gouv.qc.ca/en/showdoc/cs/CCQ-1991.
2. *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. http://www.legisquebec.gouv.qc.ca/fr/ShowDoc/cs/A-2.1
3. Projet No. 179. *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. Mai 2018. http://www.assnat.qc.ca/fr/travaux-parlementaires/assemblee-nationale/41-1/journal-debats/20180517so/projet-loi-presentes.html.
4. *Politique sur la gouvernance de la gestion et de l'exploitation des systèmes d'information* du CHUM. Disponible dans le Manuel de gestion. https://portail.chum.rtss.qc.ca/Document.php?sid=112083.
5. *Politique cadre sur la gestion de l'information* du CHUM. Disponible dans le Manuel de gestion, https://portail.chum.rtss.qc.ca/Document.php?sid=112083.
6. Documentation et formulaires du Comité d'éthique de la recherche du CHUM. Disponible dans Nagano. https://nagano.chumontreal.qc.ca/documentation_sections#C%C3%89R%20CHUM.
7. Trois-Conseils. *Déclaration de principes des trois organismes sur la gestion des données numériques*. 2016. http://www.science.gc.ca/eic/site/063.nsf/fra/h_83F7624E.html?OpenDocument.
8. ISO/EIC 11179-1:2015. *Information technology – Metadata registries (MDR) – Part 1 : Framework*. 2015. https://www.iso.org/standard/61932.html
9. Council of Canadian Academies (2015). *Accessing health-related data in Canada: the expert panel on timely access to health and social data for health research and health system innovation.* http://www.scienceadvice.ca/en/assessments/completed/health-data.aspx
10. Committee on Strategies for Responsible Sharing of Clinical Trial Data, Board on Health Sciences Policy, Institute of Medicine, *Sharing Clinical Trial Data: Maximizing Benefits, Minimizing Risk*. 2010. *https://www.ncbi.nlm.nih.gov/books/NBK285994/#ref_000441*
11. Statistics Canada Research Data Centres (RDCs). *Guide for Researchers under Agreement with Statistics Canada*. 2005. https://cdn.dal.ca/content/dam/dalhousie/pdf/faculty/ardc/researcher-rechercheur-guide-eng.pdf
12. Appendix 1 of Khaled El Emam et al., *Evaluating the Risk of Re-identification of Patients from Hospital Prescription Records*. Canadian Journal of Hospital Pharmacy 62, no. 4 (Jul-Aug 2009): 307–319, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2826964/.
13. The Information Accountability Foundation Collaborative Policy Innovation. *Canadian Assessment Framework. Big Data Assessment for Canadian Private Sector Organizations Project*. 28 février 2017. http://informationaccountability.org/wp-content/uploads/Canadian-Assessment-Framework-final-28-feb.pdf
14. Information and Privacy Commissioner of Ontario. *Planning for Success: Privacy Impact Assessment Guide*. Mai 2015. https://www.ipc.on.ca/wp-content/uploads/2015/05/Planning-for-Success-PIA-Guide.pdf.
15. Fonds Recherche Québec, *Politique sur la conduite responsable en recherche*. 2014. http://www.scientifique-en-chef.gouv.qc.ca/wp-content/uploads/Politique-sur-la-conduite-responsable-en-recherche_FRQ_sept-2014.pdf
16. International Committee of Medical Journal Editors. *Defining the Role of Authors and Contributors*. 2019. http://www.icmje.org/recommendations/browse/roles-and-responsibilities/defining-the-role-of-authors-and-contributors.html

Annexe 1 : Le lac de données du Centre d'intégration et d'analyse des données médicales du CHUM



Données sources

Données clinico-administratives issues des systèmes d'information du CHUM (ex. épisode de soins, laboratoires, pharmacie, imagerie, etc.)

Lac de données

Dépôt de données sources, structurées et non structurées, entreposées centralement

Transformation

Entrepôt de données

Données transformées selon un schéma pour répondre à des besoins spécifiques. Un entrepôt est parfois appelé «cube» ou «data mart».

Pour un aperçu des données disponibles :
https://www.chumontreal.qc.ca/crchum/plateformes-et-services/

Autorisation de réaliser un projet de recherche dans un établissement du Réseau de la Santé et des Services sociaux (RSSS)

Se basant sur les exigences du Plan d'action ministériel[3] du Ministère de la Santé et des Services sociaux, tout projet de recherche impliquant des êtres humains, incluant un projet de recherche sur dossiers, doit être soumis à :

- une évaluation scientifique;
- une évaluation éthique;
- une évaluation de la convenance institutionnelle *(la faisabilité clinico-administrative et les aspects financiers et contractuels)*.

Un résultat positif pour chacune des évaluations est requis pour que la réalisation du projet soit autorisée au CHUM.

Autorisation d'accéder aux informations versées dans le dossier médical d'un usager du CHUM à des fins de recherche

Au Québec, l'article 19 de la *Loi sur les services de santé et les services sociaux (LSSS)* établit le caractère confidentiel du dossier médical de l'usager et en limite l'accès. Dans le contexte de la recherche, l'accès aux dossiers médicaux des usagers en établissement peut être obtenu de deux manières :

A. Avec le consentement du participant ou de son représentant légal *(LSSSS, a.19.1)*

Dans un tel cas, le consentement est donné par écrit.

C'est au comité d'éthique de la recherche (CÉR) que revient la responsabilité de s'assurer, lors de son évaluation, que le formulaire d'information et de consentement (FIC) précise au participant potentiel que les informations contenues dans son dossier médical seront consultées dans le cadre du projet de recherche pour lequel sa participation est sollicitée. Ce point est également expliqué lors de la discussion entourant l'obtention du consentement écrit de celui-ci.

Un usager refusant cet accès, alors que celui-ci est nécessaire pour le déroulement du projet, ne peut être recruté pour l'étude.

Selon le type de projet de recherche, le FIC est versé au dossier médical du participant (Oacis), tel que décrit dans la Procédure CHUM 50212-01 ou conservé avec la documentation essentielle de l'étude par le chercheur principal responsable du projet.

OU

B. Autorisé par le directeur des services professionnels de l'établissement *(LSSSS, a.19.2)*

Note : Au CHUM, c'est la Direction des affaires médicales et universitaires (DAMU) qui fait office de ce rôle.

Le directeur de la DAMU peut consentir en lieu et place d'usagers avec qui il serait difficile ou peu opportun de communiquer pour obtenir cette autorisation. Avant d'accorder les accès demandés, il doit s'assurer que *« l'usage projeté n'est pas frivole et que les fins recherchées ne peuvent être atteintes que si les renseignements sont*

[3] Plan d'action ministériel en éthique de la recherche et en intégrité scientifique (MSSS, 1998)

communiqués sous forme nominative, et, les renseignements personnels seront utilisés d'une manière qui en assure le caractère confidentiel.[4] *»*

Une demande d'accès aux dossiers médicaux doit donc être formulée, par écrit, auprès de la DAMU pour :

a. un projet de recherche sur dossier;

b. valider des critères d'éligibilité de participants potentiels **avant l'obtention de leur consentement**.

Dans de tel cas, le chercheur principal fait une demande à la DAMU en complétant le formulaire de *Demande d'accès aux dossiers médicaux pour des fins de recherche* (RC-MON09-FRMA) qu'il dépose dans Nagano[5] lors de la soumission du projet de recherche pour évaluation. Lorsque le projet a reçu un résultat positif des différentes évaluations requises pour en autoriser sa réalisation au CHUM, la demande d'accès aux dossiers médicaux est transférée à la DAMU. Un résumé du projet et une confirmation que le projet a été évalué positivement d'un point de vue scientifique et éthique sont joints à cette demande.

Suite à une réponse positive autorisant l'accès aux dossiers médicaux, le chercheur principal ainsi que le Service des archives médicales reçoivent une copie électronique du formulaire dûment signé par le Directeur de la DAMU.

Le chercheur principal doit veiller à ce que cette autorisation soit conservée avec la documentation essentielle liée au projet. Il a également la responsabilité de s'assurer que soient identifiés, sur un formulaire de délégation de tâches, les membres de son équipe de recherche qui, dans le cadre de leurs fonctions, peuvent consulter les dossiers médicaux des usagers du CHUM et de maintenir à jour ce formulaire.

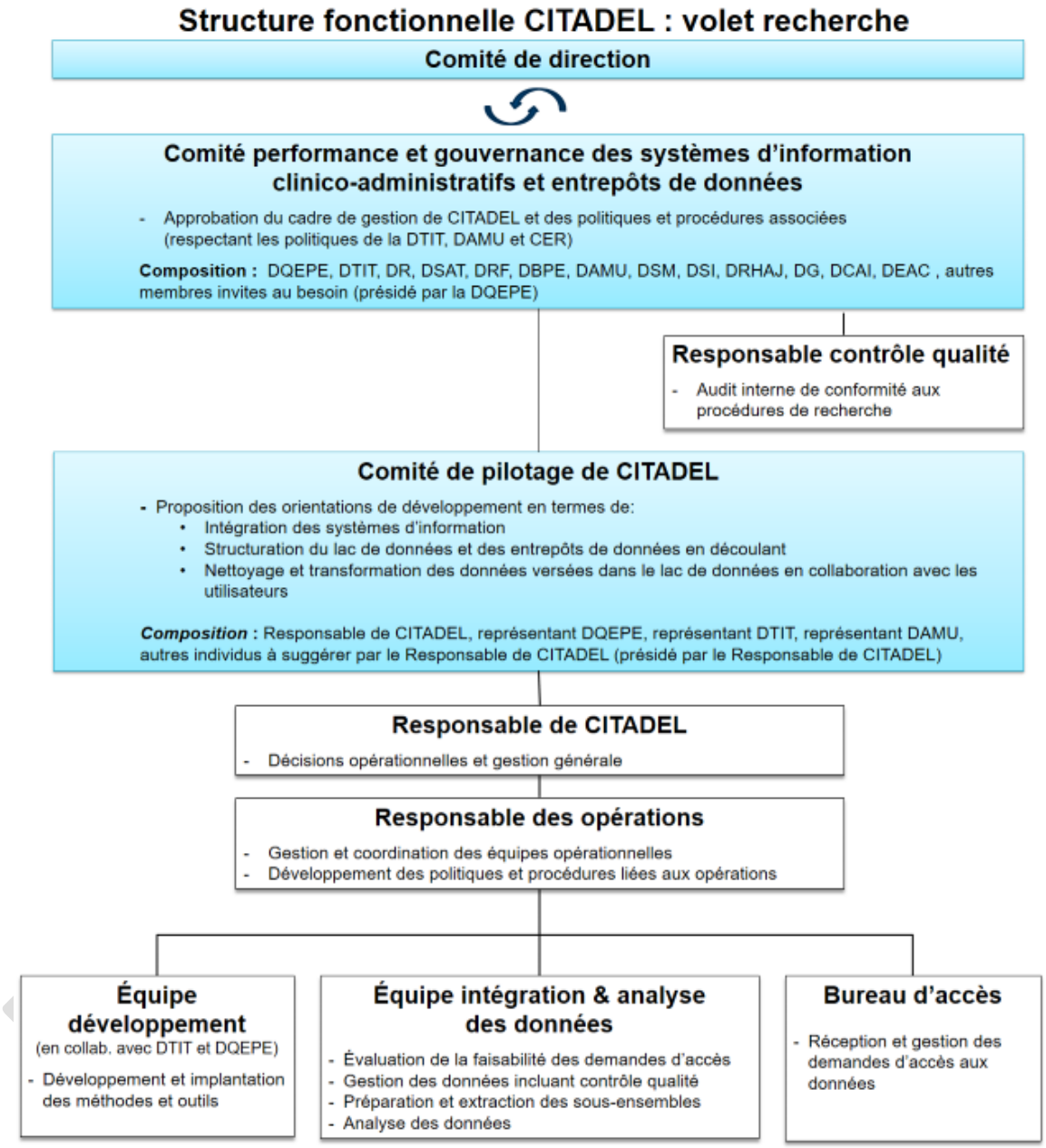
Pour des fins de contrôle quant aux accès aux dossiers médicaux du CHUM dans le cadre d'un projet spécifique, le Service des archives médicales peut en tout temps faire une demande de consultation du formulaire de délégation de tâches auprès du chercheur responsable de l'étude concernée.

Dans les deux cas, le consentement du participant et l'autorisation du directeur de la DAMU sont valables pour une activité précise. Ils sont consentis pour une durée limitée et peuvent être assujettis à de conditions spécifiques

[4] Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1., a.125)

[5] Plateforme informatique pour le dépôt et la gestion des projets de recherche soumis pour l'évaluation éthique, scientifique et de convenance institutionnelle.

Annexe 3 : Structure fonctionnelle du Centre d'intégration et d'analyse des données médicales du CHUM : volet recherche



COMITÉ DE PILOTAGE DU CENTRE D'INTÉGRATION ET D'ANALYSE DES DONNÉES MÉDICALES DU CHUM

MANDAT

RAISON D'ÊTRE

Le Comité de pilotage du Centre d'intégration et d'analyse en données médicales du CHUM (CITADEL) est responsable de proposer les orientations et priorités de développement de CITADEL. Ce comité est présidé par le Responsable de CITADEL.

MANDAT

- Proposer les orientations et priorités dans le plan de développement en termes :
  - d'intégration des systèmes d'information du CHUM dans le lac de données;
  - de structuration du lac de données et des entrepôts de données en découlant;
  - de nettoyage et transformation des données versées dans le lac de données.
- Réaliser le suivi du plan de déploiement des développements priorisés.
- Déposer la liste des projets approuvés et registre des connexions aux serveurs au Comité de performance des systèmes d'information clinico-administratifs et entrepôts de données.

LIEN D'AUTORITÉ

Le Comité de pilotage de CITADEL est un comité qui se rapporte au Comité de performance des systèmes d'information clinico-administratifs et entrepôts de données.

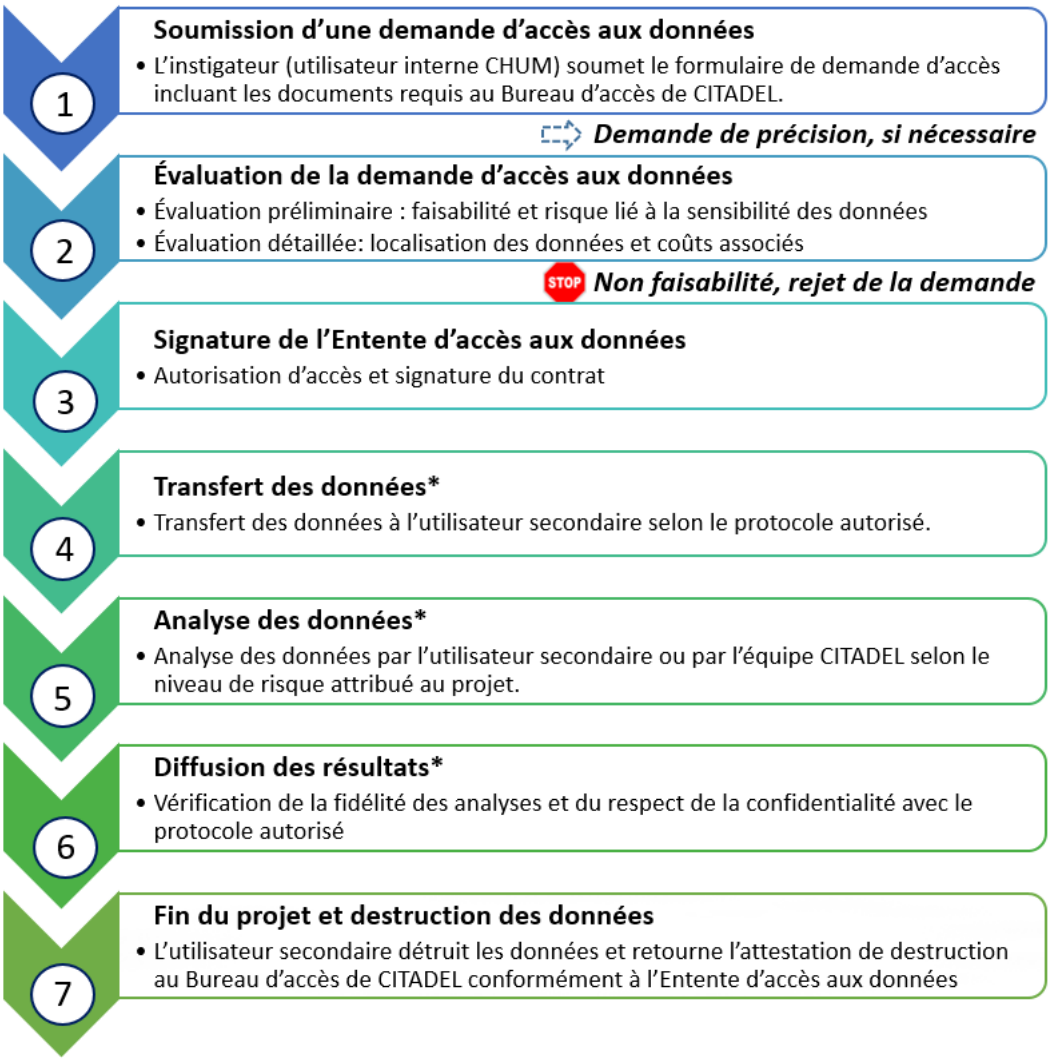
COMPOSITION

Équipe ou direction	Représentant ou délégué	
Responsable de CITADEL		
Direction de la qualité, de l'évaluation, de la performance et de l'éthique		
Direction des technologies de l'information et des télécommunications		
Direction des affaires médicales et universitaires		
Autres individus à déterminer par le responsable de CITADEL		

RÉUNIONS ET ORGANISATION

Les réunions se tiennent deux fois par année.

Annexe 4 : Modèle général d'accès



** Dépendamment du niveau de risque attribué au projet, il est possible que les analyses soient conduites par l'équipe CITADEL et que les résultats agrégés soient transmis à l'utilisateur secondaire.*

Annexe 5 : Documents reliés au cadre de gestion de CITADEL

Les documents suivants font partie du plan de documentation et se rattachent au cadre de gestion de CITADEL.

Il est à noter que les documents et procédures sont présentement en développement.

Nom du document	Description
Entente d'accès aux données	Contrat entre le Centre Hospitalier de l'Université de Montréal (CHUM) et l'utilisateur secondaire qui décrit les conditions générales et spécifiques de l'accès aux données comprises dans le lac de données exploités par CITADEL.
Procédure de gestion de la sécurité et de la confidentialité des données	Procédure décrivant la gestion des données de CITADEL en termes de sécurité et confidentialité, notamment, et sans y être limité, à l'entreposage des données, la gestion des accès aux serveurs, les journaux d'accès, le processus de dé-identification des données et le transfert des données à l'utilisateur secondaire.
Procédure de gestion d'un bris de confidentialité – données exploitées par CITADEL	Procédure décrivant les différents processus entourant la gestion, l'évaluation, la documentation et le suivi d'un bris de confidentialité en lien avec l'exploitation des données de CITADEL. La procédure précise également les obligations et délais à respecter pour la déclaration de ce bris de confidentialité auprès des différentes instances responsables.
Procédure de requête de services CITADEL – *en développement*	Procédure décrivant le processus de requête de services CITADEL.
Procédure de fermeture d'un projet – *en développement*	Procédure décrivant le processus de fermeture d'un projet approuvé ayant eu accès à des données de CITADEL et arrivant à échéance. La procédure comprend les deux documents suivants : - Attestation de destruction des données - Contenu du rapport final