CADRE DE GOUVERNANCE DES DONNÉES

du Centre intégré universitaire de santé et de services sociaux de l'Estrie – Centre hospitalier universitaire de Sherbrooke

PAR LE CENTRE INTÉGRÉ UNIVERSITAIRE DE SANTÉ ET DE SERVICES SOCIAUX DE L'ESTRIE – CENTRE HOSPITALIER UNIVERSITAIRE DE SHERBROOKE

PRÉSIDENCE DIRECTION GÉNÉRALE ADJOINTE

VERSION 2023-02-26

Production
Centre intégré universitaire de santé et de services sociaux de l'Estrie – Centre hospitalier universitaire de Sherbrooke
375 rue Argyll, Sherbrooke QC J1J 3H5

Rédaction
Présidence-Direction générale adjointe

Révision
Comité de révision, Exécutif du Comité de pilotage du Programme de gestion des données de santé

AVANT-PROPOS

Bienvenue dans cette première édition du Cadre de gouvernance des données du CIUSSS de l'Estrie – CHUS. Sa rédaction résulte d'une réflexion qui a débuté en 2019, alors que le CIUSSS de l'Estrie – CHUS démarrait un projet de conception et de mise en œuvre d'un plan de remplacement de son entrepôt de données CIRESSS. Installé au début des années 2000, CIRESSS se faisait vieux et sa technologie l'empêchait d'évoluer pour répondre aux nouveaux besoins d'analyses avancées de données massives. Les travaux de conception du plan ont amené l'équipe de projet à se questionner sur la valeur réelle de travailler sur un projet technologique sans examiner les processus entourant l'utilisation de la technologie. L'équipe de projet a donc élargi ses horizons et s'est penchée sur la stratégie à adopter pour mettre en valeur les données de l'établissement. Le projet technologique s'est vite transformé en un projet de valorisation des données qui comprend deux volets : un volet technologique et un volet organisationnel. Le volet technologique consiste à moderniser l'écosystème d'analyse des données de l'établissement. Le volet organisationnel consiste à transformer la culture organisationnelle actuelle en une culture axée sur les données dans laquelle le processus décisionnel est basé sur l'analyse des données. Le présent document est l'un des résultats du volet organisationnel du projet.

Le cadre de gouvernance présenté ici fait suite à la publication de la *Stratégie de gestion des données du CIUSSS de l'Estrie – CHUS*. Son rôle est de soutenir cette stratégie en proposant une structure de gouvernance des données, ainsi que les rôles et responsabilités de chaque composante de cette structure. Gouverner les données pour en tirer la plus grande valeur requiert un engagement à long terme à gouverner différemment les opérations de l'établissement.

Ce document est toutefois bien plus qu'un traité sur la gouvernance des données. Il énonce des principes directeurs, présente des modèles et des mécanismes de gestion, propose des programmes à mettre en place, ainsi que des processus à transformer. Il guide les acteurs du numérique de la santé dans l'instauration des processus nécessaires à la saine gestion des données, non seulement dans le respect des règles, politiques et lois établies, mais surtout, dans le respect de la vie privée des usagers et des intervenants du CIUSSS de l'Estrie – CHUS. Le lecteur, qu'il soit expérimenté ou non, peut en tirer les informations pertinentes dont il a besoin pour réaliser ses objectifs de gestion des données.

Le souhait des auteurs de ce document est que ce dernier passe l'épreuve du temps et se modernise au gré des changements qui surviendront dans l'établissement. Qu'on le veuille ou non, le domaine du numérique de la santé est là pour rester. Il deviendra de plus en plus exigeant en termes d'accès aux données, mais il apportera des bénéfices tangibles aux usagers en termes de qualité et de pertinence des soins ainsi que de prise en charge de la santé des populations.

L'ÉQUIPE DE RÉDACTION

SOMMAIRE EXÉCUTIF

Le présent document constitue la première étape de mise en œuvre de la *Stratégie de gestion des données* du CIUSSS de l'Estrie – CHUS. Il présente les principaux mécanismes de gouvernance à mettre en place pour assurer la gestion des données dans le respect des principes qui sont chers à l'établissement, tels que l'utilisation sécuritaire, confidentielle, éthique et transparente des données, la protection des renseignements personnels et le respect de la vie privée. Il aborde aussi d'autres aspects de la gestion des données par l'énoncé de principes directeurs, la présentation de modèles et de mécanismes de gestion et la suggestion de programmes à mettre en place et de processus à transformer.

Le document est divisé en quatre grandes sections :

Section 1 : Considérations générales

Cette section définit plusieurs termes importants, fréquemment utilisés dans le document. Elle présente les grands principes à respecter en matière de gestion des données ainsi que le cadre légal et réglementaire en vigueur qui balise les mécanismes de gestion proposés.

Section 2 : Établir la stratégie globale

Cette section résume la stratégie de gestion des données de l'établissement et montre comment le présent document soutient cette stratégie. Elle discute de l'importance à accorder à la communauté du CIUSSS de l'Estrie – CHUS dans la mise en œuvre d'une culture axée sur les données, ainsi que dans l'actualisation des mécanismes de gestion des données, le tout soutenu par une structure de gouvernance forte et connectée sur les opérations.

Section 3 : Assurer la vie privée des personnes

Cette section se concentre sur l'objectif principal de la gestion des données : protéger la vie privée des usagers et des membres du personnel du CIUSSS de l'Estrie – CHUS. Elle présente les principales règles à respecter et actions à réaliser afin d'assurer la confidentialité et la protection des données confidentielles stockées dans les banques et bases de données accessibles à des fins secondaires.

Section 4 : Optimiser l'utilisation des données

Cette section aborde l'aspect de la qualité des données. Elle propose un modèle de gestion de la qualité et montre l'importance d'exploiter des données normalisées pour en tirer les meilleurs bénéfices. Elle évoque l'importance de considérer les normes dans la gestion de la qualité des données.

Le document se conclut par un résumé des principaux messages véhiculés, et propose un regard futuriste sur la gestion des données.

LISTE DES ACRONYMES

BAJ	Bureau des affaires juridiques
BAPR	Bureau d'approbation des projets de recherche
BDI	Banque de données informationnelles
CA	Conseil d'administration
CAI	Commission d'accès à l'information
CdRV	Centre de recherche sur le vieillissement
CER	Comité d'éthique de la recherche
CGSI	Conseiller en gestion de la sécurité de l'information
CPSS	Coût par parcours de soins et services
CRCHUS	Centre de recherche du CHUS
CSIO	Chef de la sécurité de l'information organisationnelle
CTI	Centre de traitement informatique
DAMA	Data Management Association
DCMU	Direction de la coordination de la mission universitaire
DPI	Dirigeant principal de l'information
DORISE	Centre de données organisées du réseau informatique de la santé de l'Estrie
DQEPP	Direction de la qualité, éthique, performance et partenariat
DRF	Direction des ressources financières
DRHCAJ	Direction des ressources humaines, des communications et des affaires juridiques
DRI	Dirigeant réseau de l'information
DRIT	Direction des ressources informationnelles et technologiques
DSP	Direction des services professionnels
DSPu	Direction de santé publique
EFVP	Évaluation des facteurs relatifs à la vie privée
ICIS	Institut canadien de l'information de la santé
ISQ	Institut de la statistique du Québec
ITQ	Infrastructure technologique Québec
IUPLSSS	Institut universitaire de première ligne en santé et services sociaux
MCN	Ministère de la cybersécurité et du numérique
MSSS	Ministère de la Santé et de Services sociaux
OSI	Officier de la sécurité de l'information
PDG	Présidence-direction générale

PDGA	Présidence-direction générale adjointe
PDRH	Plan de développement des ressources humaines
PIJ	Système clinico-administratif Projet intégration jeunesse
PRP	Protection des renseignements personnels
RSI	Responsable de la sécurité de l'information
RSSS	Réseau de la santé et des services sociaux
SCT	Secrétariat du Conseil du trésor
SI	Systèmes d'information
SIT	Systèmes d'information transactionnels

TABLE DES MATIÈRES

LISTE DES FIGURES

INTRODUCTION

MISE EN CONTEXTE

Depuis 2018, le ministère de la Santé et des Services sociaux (MSSS) accélère le passage au numérique de son réseau de la Santé et des Services sociaux (RSSS). L'objectif du MSSS est de fournir à la population du Québec des services gouvernementaux numériques, incluant les services de santé, et aux usagers de son RSSS, des informations sur la gestion des établissements de santé, ainsi que des accès numériques aux professionnels soignants. Plusieurs travaux ont été réalisés, dont les plus percutants sont l'adoption de deux projets de lois, la création d'un nouveau ministère de la cybersécurité et du numérique et la diffusion d'un tableau de bord sur la gestion des établissements de santé. De plus, le MSSS soutient les établissements de son RSSS dans la transformation numérique, plus particulièrement dans l'accès aux données de santé pour des fins de recherche et d'amélioration continue de la performance organisationnelle.

En 2019, le CIUSSS de l'Estrie – CHUS emboîte le pas du numérique en initiant un grand projet de valorisation de ses données de santé dans l'objectif de se transformer en organisation apprenante axée sur les données. Une telle initiative lui permet de mieux soutenir l'ensemble de ses activités cliniques et administratives, ainsi que ses activités universitaires, dont la recherche et l'innovation dans des disciplines comme le numérique de la santé, la médecine de précision, le domaine des mégadonnées et l'intelligence artificielle, tout en assurant la sécurité de ses données.

Les travaux s'étalent sur plusieurs années et comprennent un volet organisationnel et un volet technologique. Sur le plan organisationnel, le CIUSSS :

- A adopté une Stratégie de gestion de ses données;
- A mis en place une structure de gouvernance de ses données;
- A transformé son Info-Centre pour créer le Centre DORISE, un centre d'expertise en valorisation des données;
- A rédigé et publié un Cadre de gouvernance des données (le présent document);
- Soutient son personnel dans la révision de ses politiques, directives et cadres de gestion (sécurité, risques, etc.), ainsi que dans la rédaction et la mise à jour de plusieurs cadres de gestion visant différents aspects de la gestion des données (transformation, qualité, métadonnées, normes, etc.);
- Soutient son personnel dans la mise en place d'une culture axée sur les données.

Sur le plan technologique, le CIUSSS de l'Estrie – CHUS a entrepris de grands travaux de transformation de son écosystème de gestion et d'exploitation de ses données. Ces travaux visent l'accès simplifié aux données, l'analyse des données dans un environnement sécurisé accessible à tous, la visualisation des résultats d'analyses dans un format compréhensible et l'interprétation des résultats visualisés pour une prise de décision éclairée, pour l'avancement de la recherche et de l'innovation, et pour le soutien à l'enseignement et à l'évaluation.

Aujourd'hui, les demandes d'accès aux données du CIUSSS proviennent aussi d'autres établissements de santé, d'autres universités, d'entreprises privées et d'autres organismes de recherche et développement qui innovent dans ces secteurs d'activités névralgiques. Cette situation amène les dirigeants du CIUSSS de l'Estrie – CHUS à :

- Développer l'expertise spécialisée nécessaire pour répondre aux nouveaux besoins qui font surface aujourd'hui;

- Installer la technologie nécessaire à soutenir les exigences de manipulation, de transformation, d'analyse et de visualisation de grandes quantités de données diversifiées dictées par les partenaires;
- Mettre en place les mécanismes de gestion et de gouvernance de ses données requis pour permettre l'accès à ses données tout en les protégeant de manière à assurer le respect de la confidentialité, la protection des renseignements personnels et des renseignements de santé ou de services sociaux, et le respect de la vie privée de ses usagers et des membres de son personnel.

Toutefois, le CIUSSS de l'Estrie – CHUS ne part pas de zéro. Il possède une bonne expérience en matière de gestion de l'information clinique sensible, qu'il met en œuvre dans la gestion des données stockées dans ses banques et bases de données.

En somme, le CIUSSS de l'Estrie - CHUS entend bien utiliser le plein potentiel de ses données pour atteindre ses propres objectifs cliniques, administratifs et universitaires, et pour contribuer à l'atteinte des objectifs de ses partenaires. Pour l'établissement, les données sont un atout considérable et constituent l'un de ses actifs stratégiques les plus importants.

STRATÉGIE GLOBALE DE GESTION ET D'UTILISATION DES DONNÉES

Pour pouvoir déployer des modes de gestion des données qui permettent d'atteindre ses objectifs organisationnels, le CIUSSS de l'Estrie – CHUS s'appuie sur une stratégie globale qui établit une vision et sur les personnes qui réalisent cette vision. Ces personnes sous-tendent toute la démarche et constituent la clé pour la mise en œuvre de pratiques qui intègrent la gestion des données au quotidien dans l'organisation.

Stratégie de gestion des données

Le CIUSSS de l'Estrie – CHUS a élaboré sa stratégie globale de gestion des données sur laquelle repose les fonctions de gestion des données de l'organisation ainsi que toutes les activités qui y sont rattachées. Dans un document, intitulé *Stratégie de gestion des données*, le CIUSSS présente deux catégories de fonctions de gestion des données : celles qui sont en symbiose avec la gestion des processus et celles qui sont en résonance à la gestion de la performance. Les activités qui sont rattachées à ces fonctions sont de deux natures : organisationnelle et technologique. La stratégie intègre ces fonctions et ces activités en un système unique de gestion des données qui contribue à la réalisation de la vision de l'organisation.

Développement des personnes

En matière de personnes, le CIUSSS mise sur l'augmentation de la littératie en matière de données de manière à créer un engouement pour l'émergence d'une culture orientée sur les données. Pour y arriver, le CIUSSS devra soutenir le développement des compétences pour habiliter les personnes à :

- Découvrir les données et y accéder;
- Manipuler les données;
- Évaluer la qualité des données;
- Effectuer des analyses à l'aide de données;
- Interpréter les résultats des analyses;
- Comprendre l'éthique de l'utilisation des données.

Au-delà de l'habilitation des personnes, l'organisation tout entière devra opérer un changement de culture qui soutient l'actualisation d'une organisation apprenante axée sur les données.

Gouvernance des données

Pour soutenir la stratégie et les personnes qui y adhèrent, le CIUSSS a mis en place une structure de gouvernance forte et cohérente qui implique un **dynamisme de système**[1] bien intégré au fonctionnement de l'établissement. Le Président-directeur général (PDG) du CIUSSS de l'Estrie – CHUS, qui est responsable des données générées et conservées dans les différentes bases de données de l'établissement, a délégué la responsabilité de la gestion des actifs informationnels de l'établissement et de leur contenu au Président-directeur général adjoint (PDGA). Ce dernier dirige une structure de gouvernance qui est composée de plusieurs comités et qui agit sur les trois niveaux de gestion : stratégique, tactique et opérationnel. Il s'assure que chaque partie prenante assume pleinement son rôle et que tous les niveaux de gestion soutiennent les activités proposées dans la stratégie. Ceci implique, entre autres, de développer des compétences en gestion de données axées sur les meilleures pratiques.

Stratégie d'utilisation des données

Les données collectées sont nombreuses, diversifiées et proviennent d'une grande quantité de systèmes d'information (SI) différents répartis dans l'ensemble des installations du CIUSSS de l'Estrie – CHUS. Elles comprennent les données de santé ou de services sociaux des usagers, les renseignements personnels des usagers et des membres du personnel, les données administratives, financières et de ressources humaines de l'établissement, et les données techniques des équipements et systèmes que l'établissement possède. Les formats de ces données diffèrent d'un système à l'autre, ce qui rend difficile leur exploitation pour atteindre un objectif donné.

Pour optimiser l'utilisation de ses données, le CIUSSS mise sur la normalisation des données à exploiter et sur la gestion de leur qualité. Les normes sont les clés de voûte qui permettent à un utilisateur d'accéder à des données de qualité, fiables, cohérentes et sécuritaires, et de les exploiter de manière optimale. Le CIUSSS utilise des normes dans plusieurs de ses systèmes d'information transactionnels. Il doit s'assurer que ces normes sont propices à l'exploitation des données. Dans le cas contraire, il devra choisir des normes plus appropriées. Le choix de normes doit être basé sur des critères élaborés par des experts et la normalisation doit reposer sur de bonnes pratiques à adopter aux différentes étapes du cycle de vie des données.

La qualité des données ne repose pas seulement sur leur normalisation. Elle se base sur l'adoption d'un modèle qualité qui propose différentes dimensions couvrant les perspectives technologique, humaine et organisationnelle de la gestion des données d'une part, et d'autre part, sur l'application d'un programme de gestion de la qualité pris en charge par un comité d'experts. Le CIUSSS de l'Estrie – CHUS doit choisir son modèle et élaborer son programme. La qualité des données est un incontournable à la prise de décision éclairée pour deux raisons principales. La première est que la qualité des informations menant à la prise de décision est intimement liée à la qualité des données exploitées. La seconde est que des solutions automatisées d'analyse de données sont de plus en plus utilisées comme outils d'aide à la prise de décision. La performance de ces outils dépend de la qualité des données analysées.

[1] La dynamique de systèmes (DS) est une approche permettant de comprendre le comportement non linéaire de systèmes complexes au fil du temps.

ASSURER LA VIE PRIVÉE DES PERSONNES

Le droit au respect de la vie privée est l'une des pierres angulaires de notre démocratie. Ce droit repose sur la *Charte québécoise des droits et libertés de la personne* et sur le *Code civil du Québec*. Il assure aux personnes une protection contre les intrusions injustifiées dans leur vie privée et contre la diffusion de renseignements personnels. Il leur confère le pouvoir d'obtenir réparation lorsqu'il y a eu atteinte.

Le 22 septembre 2021, entrait en vigueur la Loi 25 – ***Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*** (PRP). Cette loi renforce le droit au respect de la vie privée en introduisant des modifications importantes à la législation en matière de PRP dans le secteur privé et le secteur public. Le 3 décembre 2022, le projet de loi 3 – ***Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives***, est déposé à l'Assemblée nationale pour étude. Ce projet de loi vise à favoriser une circulation plus fluide des renseignements de santé ou de services sociaux tout en les protégeant. Il définit ce type de renseignement et il le qualifie de renseignement confidentiel.

Le CIUSSS de l'Estrie – CHUS collecte et gère à la fois les renseignements personnels de ses usagers et membres de son personnel et les renseignements de santé ou de services sociaux de ses usagers. Ces renseignements sont des données confidentielles[2] qui doivent être protégées. Pour y arriver, le CIUSSS a mis en place une *Politique de sécurité de l'information* qui sert d'assise à l'orchestration de plusieurs actions visant la confidentialité et la protection des informations confidentielles qu'il détient.

Les mécanismes de gestion de la confidentialité et de la protection des informations se trouvent dans deux documents produits et publiés par la Direction adjointe des mesures d'urgence, de la sécurité civile et des enjeux organisationnels du CIUSSS de l'Estrie – CHUS. Ces documents sont le *Cadre de gestion en sécurité de l'information* et le *Cadre normatif en sécurité de l'information*. Ils sont révisés pour tenir compte des données stockées dans les banques et bases de données de l'établissement.

Le concept de confidentialité, qui s'applique à toutes les données qui peuvent identifier une personne directement ou indirectement, se définit comme le fait d'assurer que ces données ne sont accessibles ou divulguées qu'aux personnes désignées et autorisées. L'obligation de confidentialité, applicable à tous sauf pour certaines exceptions prévues par la Loi 25, implique de mettre en place des mécanismes de gestion des accès aux données contenues dans les banques, et des mécanismes de gestion de l'authentification des personnes désignées et autorisées à accéder aux données des banques, en plus des mécanismes de protection décrits dans les deux cadres mentionnés plus haut.

Au CIUSSS de l'Estrie – CHUS, l'ensemble des données collectées sont stockées dans des banques et bases de données et deviennent alors disponibles à une utilisation secondaire[3]. Une utilisation inappropriée des données confidentielles, même involontaire, peut causer des préjudices sérieux sur le bien-être des personnes concernées, d'où l'importance de bien les protéger. Les mécanismes de sécurité de l'information déjà en place au CIUSSS comprennent un processus d'analyse du préjudice et des actions visant à éviter la récurrence. Ces mécanismes, moyennant quelques ajustements, sont applicables aux données contenues dans les banques et bases de données utilisées à des fins secondaires.

---

[2] Dans le présent document, les renseignements confidentiels sont appelés « Données confidentielles ».

[3] L'utilisation secondaire des données (ou l'utilisation à des fins secondaires) est l'utilisation des données à des fins autres que celles pour lesquelles les données ont été collectées. Ces fins peuvent être les opérations cliniques et administratives, la gestion, la recherche et développement, l'innovation, l'enseignement et l'évaluation.

PORTÉE DU DOCUMENT

Le présent document fait suite au document *Stratégie de gestion des données*. Il porte sur la gouvernance des données stockées dans les systèmes d'information, banques et bases de données du CIUSSS de l'Estrie – CHUS et qui sont utilisées à des fins secondaires. Il présente les obligations de l'établissement, les principales règles et les principes à respecter, les modèles à adopter et les mécanismes à considérer dans la gestion de ces données. Il présente également les responsabilités des différents niveaux de gouvernance à l'égard de la gestion des données stockées dans les banques et bases de données de l'établissement.

Le document fait abstraction des documents d'information, en format papier ou électronique, que possède l'établissement. La gestion de ces documents est déjà prise en charge par des politiques, des directives et des mécanismes de gestion conformes aux lois et règlements en vigueur.

Le document couvre les grandes étapes du cycle de vie des données, soit la collecte ou le chargement, le stockage, la transformation et l'organisation, l'analyse et la visualisation, l'entreposage et l'élimination. Il couvre également l'ensemble des utilisateurs de données tant à l'interne qu'à l'externe du CIUSSS de l'Estrie – CHUS, qu'ils soient cliniciens, gestionnaires, chercheurs ou tout autres partenaires publics ou privés désirant exploiter les données de l'établissement.

SECTION 1 – CONSIDÉRATIONS GÉNÉRALES

Publié par : La Presse canadienne avril 2019

CHAPITRE 1 – PRINCIPES GÉNÉRAUX D'UTILISATION DES DONNÉES

DÉFINITIONS

Il existe une littérature foisonnante sur la valorisation des données. Les auteurs utilisent généralement les termes renseignement, information et donnée pour exprimer des concepts précis. Parfois, les auteurs utilisent toutefois un même terme pour exprimer des concepts différents. Cette façon de procéder peut faire naître une certaine confusion chez les lecteurs non-initiés sur ce sujet. C'est pourquoi les termes fréquemment utilisés dans ce document sont définis dans la présente section. L'annexe A propose des définitions plus précises de plusieurs termes.

DONNÉE – INFORMATION - RENSEIGNEMENT

Une **donnée** est un résultat d'une observation ou d'une expérience faite délibérément[4]. Elle prend la forme de chiffre, d'énoncé et de caractère. Elle est brute, elle n'a pas de sens et elle est inconséquente en soi, car elle n'apporte rien. Elle est le plus bas niveau du processus de transformation vers la connaissance.

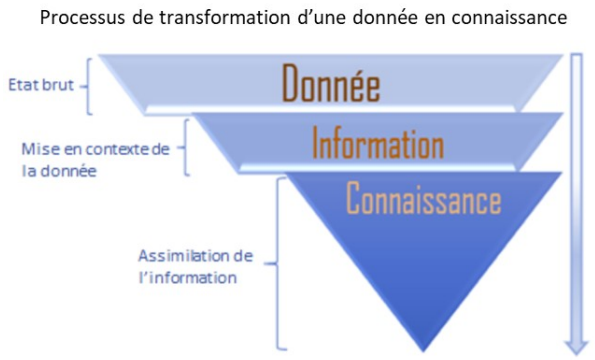


Figure 1 – Processus de transformation d'une donnée en connaissance. Tiré de Datatame.fr

Lorsque les données sont regroupées, traitées, organisées, structurées ou mises en contexte, elles portent collectivement une signification logique et génèrent de l'**information**. L'information est fiable lorsque les données qui la composent sont basées sur des faits véritables. Lorsque l'information est assimilée et comprise par une personne, elle génère la **connaissance**.

Lorsque l'information est jugée importante pour sa valeur et sa pertinence dans le contexte pour lequel elle a été recueillie, elle devient un **renseignement**. Le renseignement se définit aussi par la connaissance qu'il génère pour guider des prises de décisions et des actions.

L'exemple suivant permet de comprendre ces concepts. *5000* et *pieds* sont chacune une donnée. Leur mise en commun, « *5000 pieds* », génère une information pouvant correspondre à une longueur, une distance ou une hauteur. Cette information jumelée à l'information « *au-dessus du niveau de la mer* » crée une nouvelle information de plus grande valeur « *5000 pieds au-dessus du niveau de la mer* ». Cette nouvelle information correspond à une hauteur. Mise dans le contexte d'écrasement d'un avion, cette nouvelle information devient un renseignement utile pour circonscrire les recherches.

La législation utilise le terme **renseignement** pour définir l'information faisant l'objet de certains articles de lois, par exemple : les renseignements de santé pour désigner l'information sur la santé d'une personne, ou les renseignements personnels pour désigner les informations identifiant une personne. Elle utilise aussi le terme **information** pour désigner le contenu de certaines ressources informationnelles, comme les systèmes d'information opérationnels. Le contexte est indicatif du sens du terme utilisé.

[4] Tiré du dictionnaire Larousse.

Dans la perspective du présent document, les bases de données, les répertoires et les systèmes d'information opérationnels collectent et stockent des données. Les logiciels utilisés par les utilisateurs (cliniciens, gestionnaires ou autres) pour afficher les données, affichent plutôt des informations. En effet, à la suite d'une requête, ces logiciels accèdent aux données, les regroupent, les traitent et affichent le résultat de ce traitement, soit des informations. Dans un contexte donné, ces informations deviennent des renseignements.

DONNÉES À CARACTÈRE PERSONNEL ET DONNÉES PERSONNELLES SENSIBLES

Les données à caractère personnel, aussi appelées données personnelles, sont les données qui permettent l'identification d'une personne physique tels les nom, prénom, adresse, date de naissance, numéro de téléphone, etc.

Bien que les données personnelles soient des données sensibles, certains auteurs préconisent que certaines données personnelles sont plus sensibles que d'autres, comme les données liées à la santé, la sphère intime, l'origine ethnique ou culturelle, les mesures d'aide sociale, les opinions ou activités religieuses, philosophiques, politiques ou syndicales, etc.

Plus les données personnelles sont considérées comme sensibles, plus la législation exige une protection renforcée.

TYPES DE DONNÉES COLLECTÉES ET EXPLOITÉES

Au CIUSSS de l'Estrie – CHUS, les données sont collectées dans les systèmes d'information opérationnels. Elles sont ensuite utilisées principalement pour soutenir les activités journalières de l'établissement. On y retrouve les données de santé ou de services sociaux, les données personnelles et non personnelles. Ces mêmes données sont aussi exploitées à des fins autres que celles pour lesquelles elles ont été collectées : gestion, recherche, enseignement, évaluation, autres. Si elles n'ont subi aucune transformation, on les appelle **données brutes**. Si elles sont transformées, elles prennent un nom différent selon le type de transformation qu'elles subissent. Elles deviennent **anonymisées**, lorsque les informations les liant aux personnes concernées sont irrévocablement retirées, ou **dépersonnalisées**, lorsque ces mêmes informations sont remplacées par des codes, ou encore **dérivées**, lorsqu'elles résultent d'un calcul, algorithme ou autre transformation.

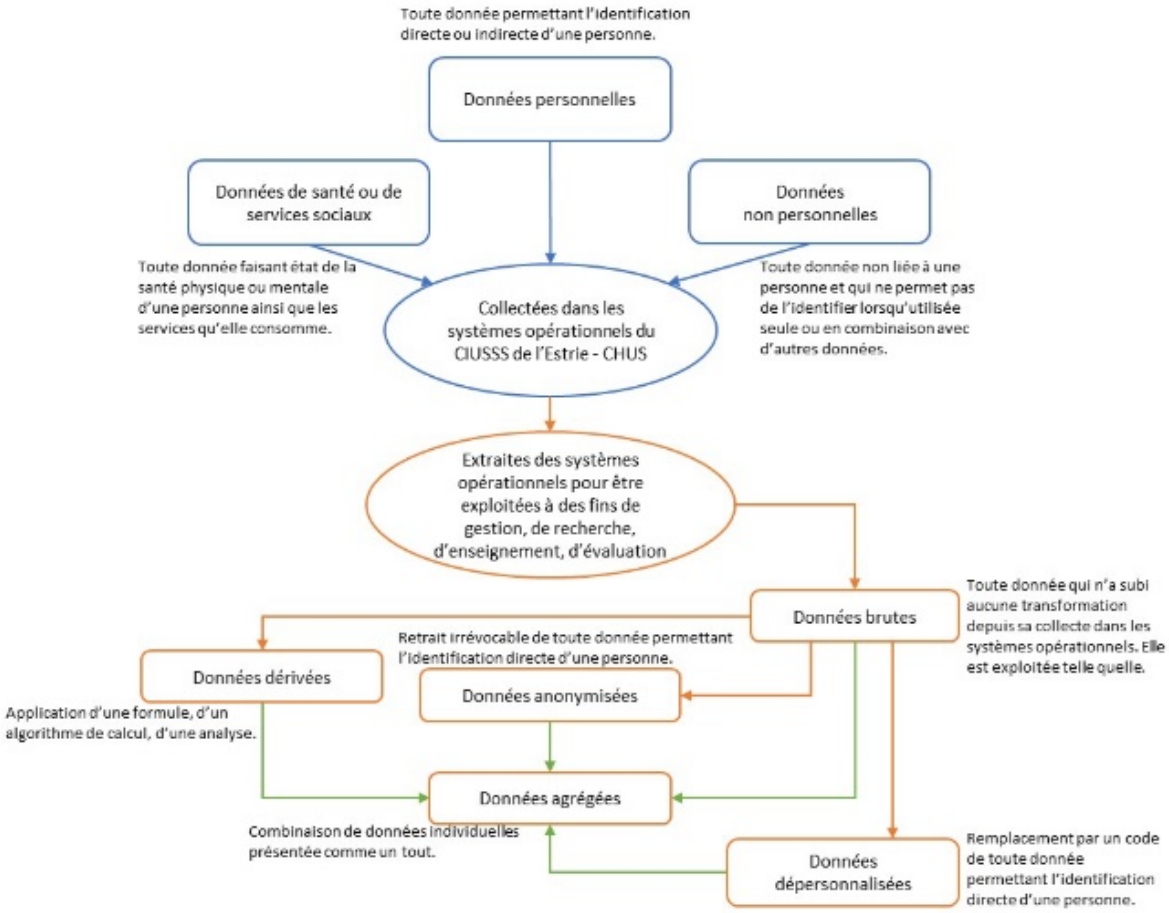


Figure 2 – Types de données collectées et exploitées.

TYPES D'UTILISATION DES DONNÉES

Deux types d'utilisation des données prédominent dans une organisation comme le CIUSSS de l'Estrie – CHUS. Ils sont :

- *L'utilisation primaire* des données : fait référence à des données qui sont collectées pour la première fois et qui sont utilisées uniquement à des fins pour lesquelles elles sont collectées. Par exemple : les données de santé et de services sociaux collectées à des fins de prestation de soins et de services directs sont utilisées à ces mêmes fins. Aussi, les données collectées dans le cadre d'un protocole de recherche ou dans le cadre d'une étude statistique sont utilisées pour ces mêmes fins. Les données administratives collectées à des fins de gestion sont utilisées à ces mêmes fins.
- *L'utilisation secondaire* des données : fait référence à des données qui existent déjà, qui ont été collectées à des fins autres que celles pour lesquelles elles sont utilisées. Ces données sont stockées dans des systèmes d'information transactionnels ou dans des bases de données opérationnelles, ou déjà publiées dans des journaux, articles, WEB, autres. Elles sont chargées dans une banque de données physique ou virtuelle à des fins d'exploitation. Par exemple : les données de santé et services sociaux collectées à des fins de prestation de soins et de services sont utilisées à des fins de gestion, de recherche, de développement, d'enseignement, d'évaluation, de statistique et d'autres objectifs connexes non liés à la

prestation des soins et services. Les données administratives collectées à des fins de gestion sont utilisées à des fins de dispensation de soins et services, de recherche, de développement, d'enseignement, d'évaluation de statistique et d'autres objectifs connexes non liés à l'administration.

UTILISATEURS DE DONNÉES

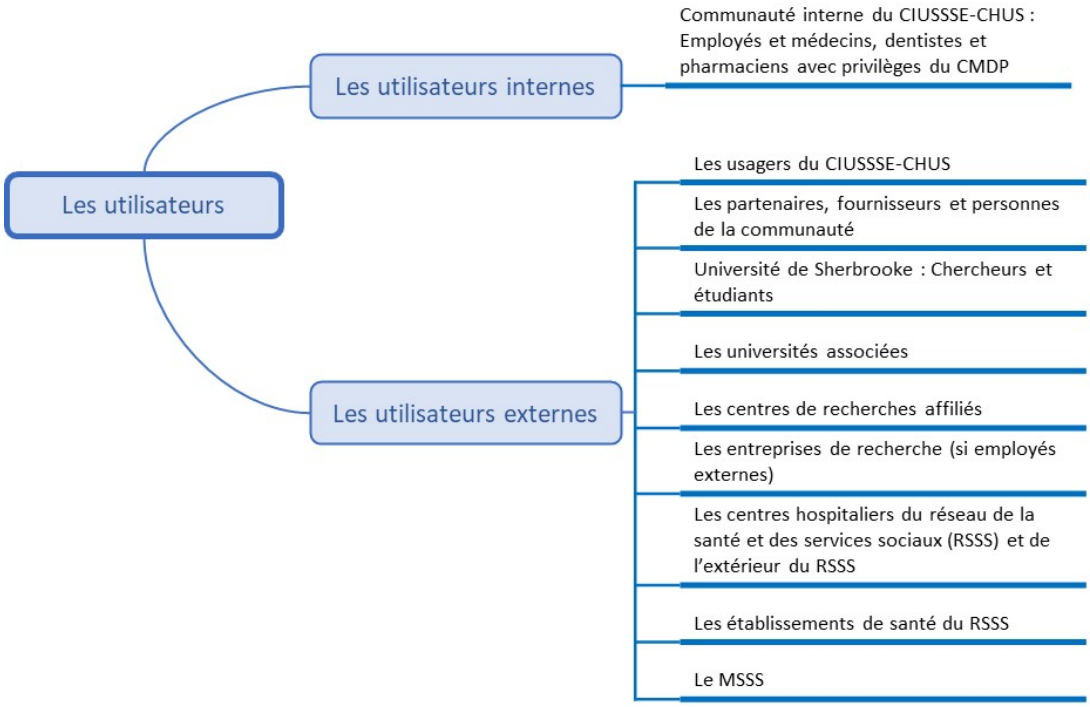


Figure 3 – Schéma des utilisateurs de données.

Utilisateurs internes

Sont considérés comme des utilisateurs internes au CIUSSS de l'Estrie – CHUS, l'ensemble des personnes qui ont un lien d'emploi avec l'établissement et qui y exercent leurs fonctions en lien avec ses missions cliniques ou administratives. Les médecins, dentistes et pharmaciens qui ont des privilèges accordés par le CMDP du CIUSSS de l'Estrie – CHUS font aussi partie de ce groupe d'utilisateurs.

Utilisateurs externes

Sont considérés comme des utilisateurs externes au CIUSSS de l'Estrie – CHUS, toutes les autres catégories de personnes œuvrant au sein du CIUSSS de l'Estrie-CHUS, les partenaires et les fournisseurs privés.

Conformément à l'article 110 de la *Loi sur les services de santé et services sociaux* (LSSSS), les centres de recherche affiliés au CIUSSS de l'Estrie – CHUS, soit le Centre de recherche du CHUS (CRCHUS) et le Centre de recherche sur le vieillissement (CdRV), ainsi que l'Institut universitaire de première ligne en santé et services sociaux (IUPLSSS) sont des partenaires incontournables de la mission universitaire du CIUSSS de l'Estrie – CHUS. Les travailleurs de ces centres sont en grande

majorité des employés de l'Université de Sherbrooke. À ce titre, ils sont donc considérés comme des utilisateurs externes des données du CIUSSS de l'Estrie – CHUS. Malgré le fait que plusieurs acteurs dans ces centres soient également des employés du CIUSSS de l'Estrie – CHUS, ils sont considérés comme des utilisateurs externes lorsqu'ils exercent leurs activités universitaires. En revanche, ils sont considérés comme des utilisateurs internes lorsqu'ils exercent leurs activités cliniques ou administratives au CIUSSS de l'Estrie – CHUS.

Les étudiants et chercheurs de l'Université de Sherbrooke sont considérés comme des utilisateurs externes des données du CIUSSS. Il en est de même pour les étudiants, les contractuels et les chercheurs invités œuvrant au sein de l'Université de Sherbrooke.

D'autres utilisateurs des données du CIUSSS de l'Estrie – CHUS sont considérés aussi comme des utilisateurs externes :

- Les universités autres que l'Université de Sherbrooke qui désirent s'associer au CIUSSS de l'Estrie – CHUS pour réaliser des projets;
- Les centres hospitaliers du réseau de la santé et des services sociaux (RSSS) et de l'extérieur du RSSS;
- Les entreprises en recherche, développement et innovation qui désirent s'associer au CIUSSS de l'Estrie – CHUS pour initier ou poursuivre des projets de recherche et développement;
- Les usagers qui reçoivent des soins et services du CIUSSS de l'Estrie – CHUS qui ont accès aux données de leur dossier de santé;
- Finalement, le ministère de la Santé et des Services sociaux (MSSS) qui est un acteur d'influence par ses politiques de santé qu'il met en place dans le RSSS, dont la stratégie de valorisation des données.

Catégories de chercheurs

Pour accéder aux systèmes, équipements et services du CIUSSS de l'Estrie – CHUS, ainsi qu'à ses données et informations, les chercheurs doivent tous avoir des privilèges de recherche au sein des centres de recherche de l'établissement. Certains chercheurs ne sont pas membres d'une infrastructure de recherche (ex. chercheur externe) mais leurs privilèges doivent quand même être reconnus. L'établissement reconnaît six catégories de chercheurs dans sa politique des privilèges et des statuts de chercheur : chercheur clinicien, chercheur universitaire, chercheur d'établissement, chercheur externe, chercheur invité et chercheur de collège.

Quant aux entreprises privées de recherche, développement et innovation, elles sont vues comme des organisations externes qui doivent signer une entente avec l'établissement avant qu'une permission d'accéder aux données leur soit octroyée.

IMPORTANCE DE GOUVERNER LES DONNÉES

Les lois et règlements traitent d'information et de renseignements, car ils sont significatifs pour l'individu qui les possède et leur utilisation malveillante cause un préjudice d'importance variable selon la nature de l'information ou du renseignement. Quant aux données, parce qu'elles n'ont pas cette caractéristique de signification, elles ne peuvent causer de préjudice. Ainsi, le gouvernement répond aux demandes de la communauté de recherche, qui désire accéder plus facilement aux données de santé. Puisque le traitement des données de santé par les logiciels experts des

chercheurs génère des informations et renseignements qui peuvent potentiellement être préjudiciables pour le citoyen, le gouvernement prévoit des lois et règlements protégeant davantage les informations et renseignements Au-delà de cet encadrement, le gestionnaire des données qui génère ces informations et renseignements a aussi un rôle à jouer.

Le propriétaire des bases de données, des répertoires et des systèmes d'information qui stockent les données doit s'assurer que les données utilisées ne génèrent pas d'information ou de renseignements préjudiciables. C'est le cas pour un établissement de santé envers les données de ses usagers et des membres de son personnel. Dans une banque de données, chaque donnée est étiquetée. On retrouve sur cette étiquette une foule d'informations caractérisant la donnée, par exemple la date et l'heure de sa collecte ou le numéro de dossier auquel elle est rattachée. On appelle ces informations **les** métadonnées.

Les utilisateurs de données ont aussi accès aux métadonnées. Il est donc important, avant de permettre l'accès aux données à un utilisateur, de s'assurer de retirer, sur l'étiquette, toute information reliant la donnée à une personne, de manière à préserver sa confidentialité et protéger sa vie privée. C'est la **dépersonnalisation** des données. Un utilisateur qui regroupe, traite et analyse des données dépersonnalisées obtient des résultats agrégés et anonymes.

D'autres techniques de protection des données existent, comme la gestion de la sécurité et la gestion des accès. Le présent document traite des principales techniques dans les chapitres qui suivent.

CADRE LÉGAL ET RÉGLEMENTAIRE GÉNÉRAL

La Figure 4 Figure 4montre la complexité du cadre juridique et réglementaire qui touche la gestion de l'information dans le secteur de la santé et des services sociaux.[5] Il est constitué d'un nombre important de lois, de politiques et de règlements regroupés dans quatre secteurs: le gouvernement du Québec, le Secrétariat du Conseil du trésor, le Réseau de la santé et des services sociaux (RSSS) et le CIUSSS de l'Estrie – CHUS.

La gouvernance des données n'échappe pas à cette complexité, car elle s'appuie sur le même cadre juridique et réglementaire, tout en accentuant les principes de confidentialité des données et de protection des renseignements personnels qui, lorsqu'ajoutés à la sécurité des données, constituent l'assise du respect de la vie privée des personnes.

Quelques précisions

Le présent cadre de gouvernance des données s'appuie également sur les exigences *du Cadre de gestion gouvernemental de la sécurité informationnelle.* Ce dernier est une composante complémentaire au *Cadre de gestion de la sécurité de l'information* du CIUSSS de l'Estrie – CHUS et à ses règlements, politiques et procédures internes.

Il n'existe aucun article de loi spécifique aux banques de données; le présent cadre de gouvernance applique aux banques de données les règles qui régissent les documents. En effet, « est assimilé au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite » (*Loi concernant le cadre juridique des technologies de l'information, art. 3),* ce qui s'applique aux banques de

[5] Le présent document ne tient pas compte des modifications législatives qu'apporte le projet de loi 3 - Loi sur les renseignements de santé et services sociaux et modifiant diverses dispositions législatives – puisque ce dernier est en commission parlementaire et n'a pas encore été sanctionné.

données du CIUSSS de l'Estrie – CHUS. Les règles applicables comprennent donc le cadre légal et réglementaire prévu dans la *Loi sur les services de santé et les services sociaux* (LSSSS) quant au dossier des usagers, la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (*ci-après nommée *Loi 25)*, la *Loi sur les archives* et les lois touchant la sécurité de l'information.

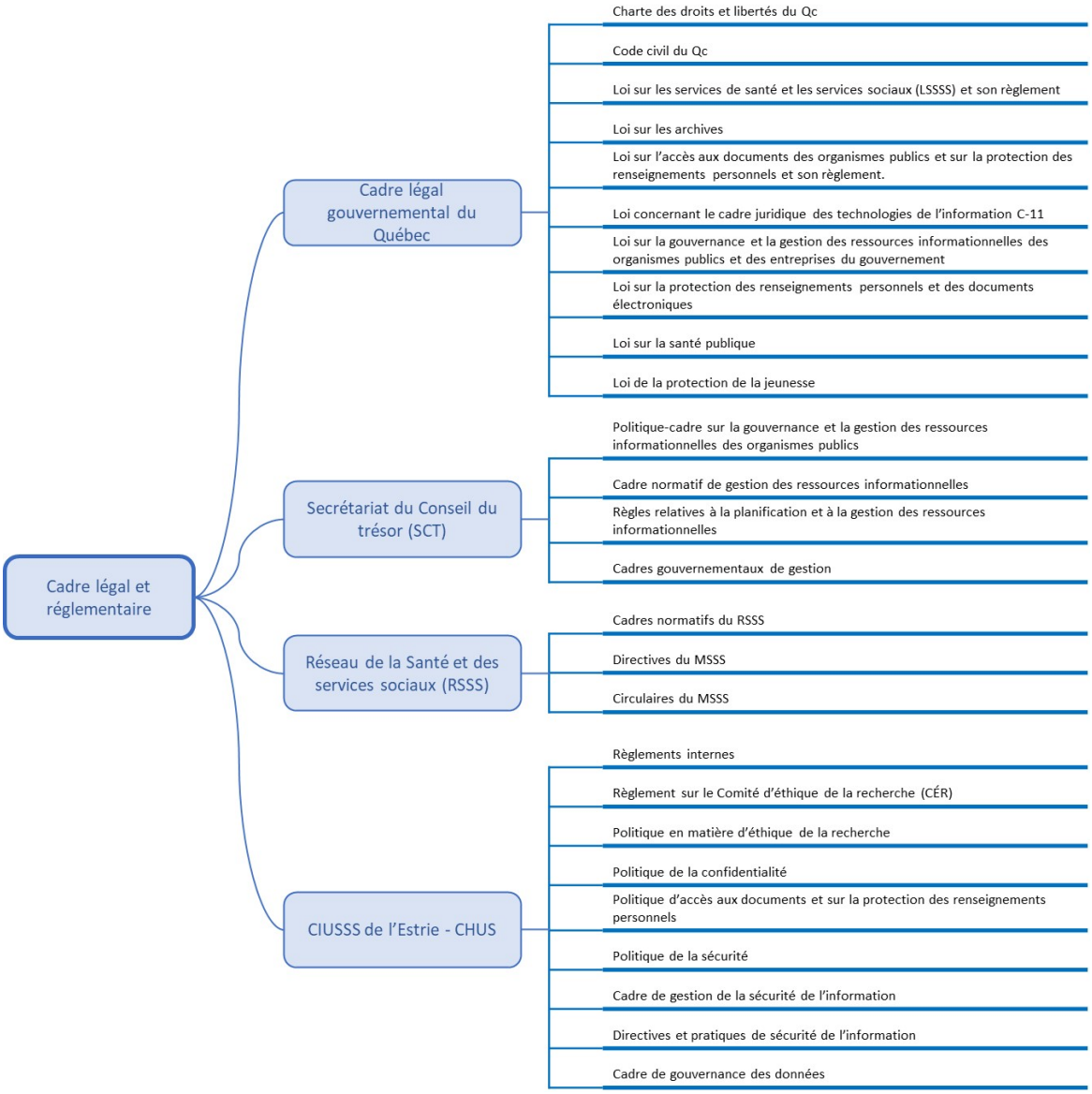


Figure 4 – Cadre légal et réglementaire de la gestion de l'information.
Ce cadre regroupe quatre secteurs législatifs : le Gouvernement du Québec, le Secrétariat du conseil du trésor, le Réseau de la Santé et des services sociaux et le CIUSSS de l'Estrie – CHUS.

La *Loi 25* adoptée en 2021 permet l'utilisation des données pour des fins de recherche.

Il est à noter que la *Loi 25* a été adoptée le 8 octobre 2021. Son entrée en vigueur est progressive sur une période de 3 ans. Désormais, la *Loi 25* non seulement permet la cueillette, l'utilisation *(*art.64*)* et la transmission (art.67) des renseignements personnels dans la mesure où cela est nécessaire à l'exercice des attributions du CIUSSS de l'Estrie - CHUS ou la gestion d'un programme dont il a la responsabilité, mais aussi permet l'utilisation des données à des fins d'étude,

d'enseignement, de recherche ou de statistique selon certains critères déterminés par la Loi à la suite d'une évaluation par le CÉR de l'établissement, s'il y a lieu, et par la CAI si les conditions s'appliquent (art. 161 (67.2.1 à 67.2.3)).

REGROUPEMENT DES LOIS

Dans le but de faciliter la compréhension du contexte légal et règlementaire présenté à la Figure 4, la Figure 5 regroupe les principales lois selon les thèmes abordés dans les chapitres du présent document. Le lecteur est invité à se référer à cette figure lors de la lecture des différents chapitres de ce document.

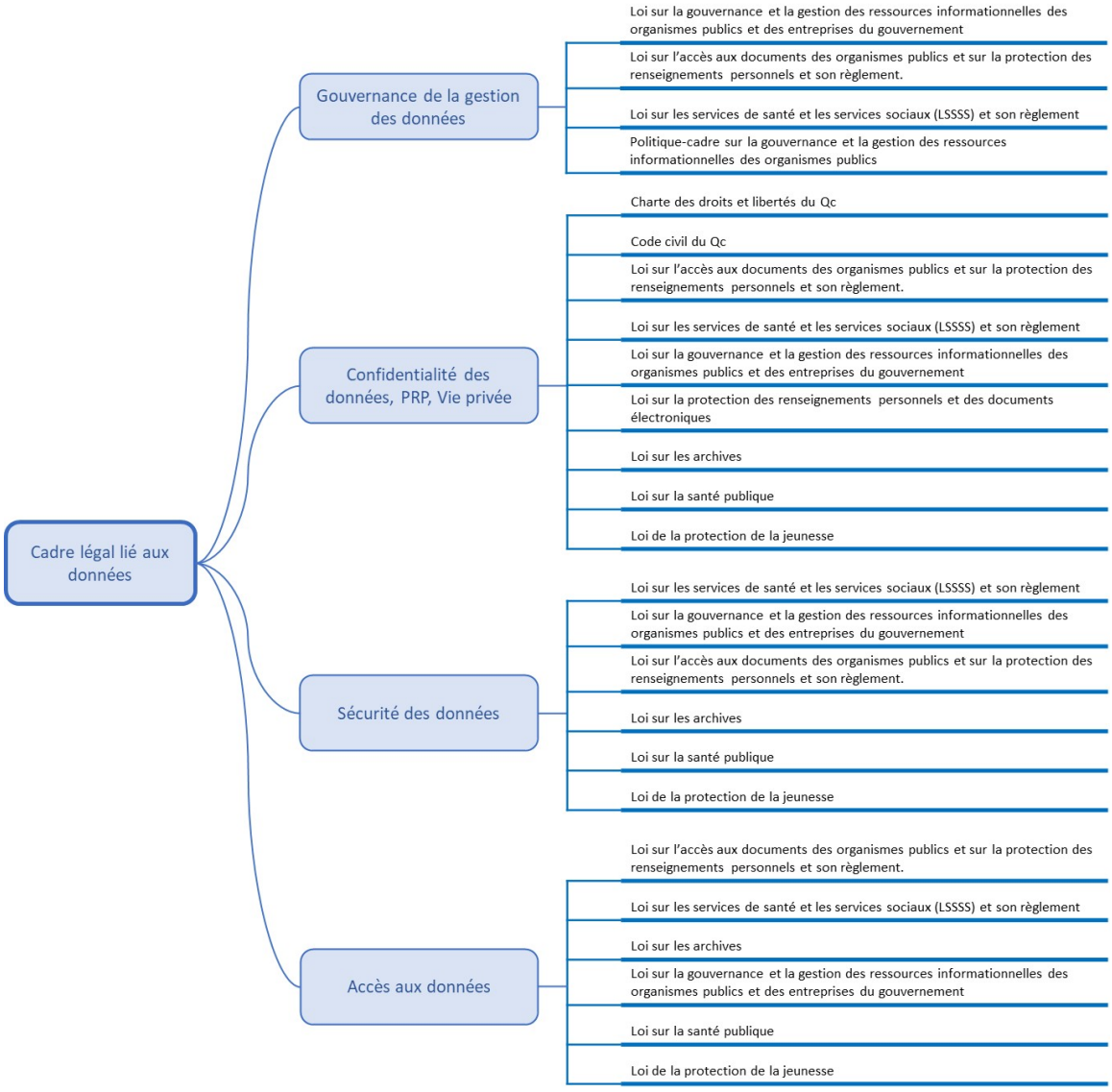


Figure 5 – Cadre légal lié aux données.
Ce cadre regroupe les principales lois traitant des sujets discutés dans les chapitres du présent document. Les politiques et règlements n'ont pas été inclus dans ce regroupement puisque les inclure rendrait le regroupement plus difficile à réaliser, sans en améliorer la compréhension.

PRINCIPES GÉNÉRAUX DU CADRE DE GOUVERNANCE

Le présent cadre de gouvernance est une composante importante d'une stratégie de gestion des données qui appuie les valeurs d'humanisme, d'engagement et d'adaptabilité qui accompagnent la vision du CIUSSS de l'Estrie – CHUS *:*

EN ESTRIE, ENSEMBLE, INNOVONS POUR LA VIE.

En respect de cette vision et des principes évoqués dans la *Stratégie de gestion des données,* le présent document repose sur les principes fondamentaux qui engagent le CIUSSS de l'Estrie-CHUS :

- À positionner l'usager au centre de la gestion de l'information de santé;
- À respecter la vie privée de ses usagers et de son personnel en assurant la sécurité et la confidentialité des renseignements personnels qu'il collige et partage au sein de ses missions et désignations;
- À encourager et soutenir les gestionnaires du CIUSSS de l'Estrie – CHUS à l'utilisation des données au bénéfice de l'amélioration continue de leurs services;
- À encourager et soutenir le personnel du CIUSSS de l'Estrie – CHUS à l'utilisation des données aux bénéfices de la qualité des soins, du continuum de services, de la performance organisationnelle et clinique, de l'amélioration de la santé de la population, de la recherche, de l'enseignement et de l'évaluation;
- À appuyer une gouvernance forte en gestion des données, comprise et adoptée par toute la communauté du CIUSSS, qui vise une utilisation judicieuse et éthique des données;
- À soutenir l'amélioration continue de la qualité des données à la source;
- À appuyer le partage des données avec d'autres organisations garantes du respect des lois et règlements ainsi que de ses valeurs et principes fondamentaux.

LE CIUSSS DE L'ESTRIE – CHUS FACE À LA GESTION DES DONNÉES

PRINCIPE DE TRANSPARENCE

Droits des usagers

L'encadrement légal au Québec met en relief des principes de transparence au regard de la gestion des données qu'un organisme public, comme le CIUSSS de l'Estrie – CHUS, collecte, stocke, utilise, partage, archive ou détruit. Les lois et chartes édictent en ce sens des droits fondamentaux à la personne et aux usagers du réseau de la santé et des services sociaux (RSSS), à savoir :

- le droit d'être informés des activités reliées à l'utilisation et au partage des données qui les concernent et
- le respect des droits suivants :
    - À la vie privée et au secret professionnel;

- À être informés, lors de prestation de soins, de l'utilisation secondaire possible de leurs données et des mécanismes de contrôle que l'établissement met en place pour protéger leurs renseignements personnels;
- À consulter la liste des personnes qui ont pu consulter les données qui les concernent;
- D'accéder et de rectifier s'il y a lieu des données les concernant qui sont stockées dans les actifs informationnels de l'établissement;
- D'être informés des processus de plaintes s'ils désirent s'en prévaloir;
- D'être informés du soutien qu'ils peuvent obtenir pour faire valoir leurs droits.

Actions de l'établissement

Pour respecter le principe de transparence auquel il tient, le CIUSSS de l'Estrie – CHUS :

- Diffuse sur son site internet :
  - Les politiques de gestion des renseignements personnels collectés et utilisés dans ses activités, dans des termes clairs et simples;
  - Les droits des personnes[6] concernant les activités reliées à l'utilisation et au partage de leurs données de santé et leurs renseignements personnels;
  - Les mécanismes de communication permettant aux personnes de formuler une plainte si elles croient que leurs droits à la confidentialité et à la vie privée n'ont pas été respectés;
- Met en place les mécanismes permettant à ses usagers et son personnel :
  - D'obtenir sur demande un rapport faisant état des activités de consultation de leurs renseignements personnels;
  - D'être informés rapidement de toute utilisation ou communication inappropriée de leurs renseignements personnels;
- Met en place des mécanismes de traçabilité (journalisation) des accès et communications des données et renseignements personnels des usagers à des fins de surveillance et d'investigation;
- Forme et sensibilise son personnel sur l'importance de la confidentialité des données et la protection des renseignements personnels ainsi que sur la gravité du non-respect.

UTILISATION DES DONNÉES

Le CIUSSS de l'Estrie – CHUS collige les données nécessaires à l'exercice de ses fonctions et à la mise en œuvre de ses programmes dans le but de :

- Soutenir la prestation des soins et services dans l'ensemble de l'établissement;
- Améliorer en continu la performance organisationnelle;
- Soutenir les activités universitaires de recherche, enseignement et évaluation;

[6] Le terme « personnes » inclut les usagers et le personnel de l'établissement.

- Soutenir, suivre et évaluer le continuum de soins et services et les trajectoires qui y sont associées;
- Effectuer de multiples analyses (exemple : exploratoires, prédictives, prescriptives, descriptives, diagnostiques, transversales, complexes, etc.).

Ces différents objectifs se regroupent dans les deux types d'utilisation des données du CIUSSS, soit l'utilisation primaire et l'utilisation secondaire.

PROTECTION DES SYSTÈMES OPÉRATIONNELS

Le principe guidant l'utilisation des banques de données pour des fins d'exploitation est :

Détacher les systèmes opérationnels des activités autres que celles pour lesquelles ils ont été conçus, soit collecter des informations de santé et les utiliser pour dispenser des soins et des services.

Les données collectées et utilisées dans le contexte de dispensation de soins et services sont de nature sensible, car elles sont reliées à la santé des usagers. Ces mêmes données sont d'intérêt pour les gestionnaires et chercheurs, car elles permettent d'améliorer les services et générer des innovations transférables en clinique. La nature sensible des données de santé impose une prudence quant à l'utilisation des systèmes opérationnels dans des activités analytiques complexes. Ainsi, pour préserver la vie privée de ses usagers et protéger ses données de santé, et afin que celles-ci soient traitées et exploitées adéquatement, le CIUSSS de l'Estrie – CHUS a choisi de copier ses données dans des banques de données indépendantes des systèmes opérationnels.

De plus, en vertu de la *Loi sur les archives*, de la *Loi 25* et du *Cadre de gestion de la sécurité de l'information* :

L'établissement doit tenir à jour l'inventaire de ses banques de données et des fichiers de renseignements personnels qu'il détient.

Cet inventaire doit spécifier les catégories de personnes qui ont accès aux banques et fichiers, le lieu et le délai de leur conservation ainsi que la catégorisation et le niveau de sensibilité des données qui y sont stockées. La mise à jour de cet inventaire doit se faire minimalement annuellement ou dès qu'un changement survient.

SECTION 2 – ÉTABLIR LA STRATÉGIE GLOBALE

CHAPITRE 2.1 – STRATÉGIE DE GESTION DES DONNÉES

VISION DE LA STRATÉGIE

La stratégie des données du CIUSSS de l'Estrie – CHUS établit la vision de l'organisation en matière de gestion des données :

Baser nos activités sur des données de qualité, pertinentes et accessibles en toute sécurité et confidentialité à la bonne personne, au bon moment et dans le bon format afin de soutenir la gestion intégrée de la performance et d'offrir de meilleurs services à la population, dans le respect de la vie privée.

Cette vision sous-tend les fonctions de gestion des données de l'organisation ainsi que toutes les activités qui y sont rattachées.

Les fonctions de gestion des données sont de deux ordres :

- La gestion des données en symbiose avec la gestion des processus qui permet de garantir que, dans une organisation, les différentes équipes prennent les mesures qui s'imposent pour disposer en permanence des données de la plus haute qualité et les plus récentes pour soutenir les processus internes de l'organisation. Ceci n'est possible que si les ressources humaines se donnent les moyens de suivre les changements et tendances des activités de l'organisation en temps réel;
- La gestion des données en résonance à la gestion de la performance qui permet de guider les personnes, les organisations et les systèmes connectés à optimiser l'utilisation des données pour soutenir la fluidité des processus. Cette optimisation doit se faire dans les limites des politiques et des réglementations afin de prendre des décisions et des mesures qui maximisent les avantages pour l'organisation. Pour y arriver, il est nécessaire de définir, d'approuver et de communiquer les stratégies, politiques, normes, architectures et procédures entourant la gestion des données et assurer le suivi du respect de ces dernières par une équipe de professionnels aguerris.

Les activités qui sont rattachées à ces fonctions de gestion sont classées dans deux grandes catégories :

- Les activités organisationnelles qui sont davantage liées à la gouvernance, la qualité et la sécurité des données, la protection des renseignements personnels et de la vie privée, ainsi que la gestion des accès et les mécanismes d'exploitation des données;
- Les activités technologiques qui sont liées aux systèmes d'information et applications qui gèrent le cycle de vie des données et qui assurent une orchestration des données cohérente avec les besoins de l'organisation en matière d'exploitation des données.

L'intégration des fonctions de gestion et des activités qui y sont rattachées en un système unique de gestion des données fait de ce dernier un incontournable du fonctionnement d'une organisation.

PRINCIPALES COMPOSANTES DE LA STRATÉGIE

La stratégie de gestion des données est bien alignée sur la vision et les priorités du CIUSSS de l'Estrie – CHUS, en plus de considérer la stratégie de transformation numérique gouvernementale. Elle dessert une clientèle diverse composée des décideurs, des gestionnaires et du personnel prodiguant des services de santé et des services sociaux, des chercheurs et des usagers eux-mêmes. Elle repose sur quatre piliers et sur trois moteurs opérationnels.

a. Les piliers sont des domaines d'affaires incontournables qui regroupent et organisent les activités à gérer et à réaliser pour répondre aux objectifs généraux et spécifiques de la stratégie et atteindre les résultats attendus. Ils sont :

   1. *Encadrement et Pratiques*;

      Qui consiste à mettre en œuvre une stratégie de données qui s'aligne sur la stratégie de l'organisation et la réaliser en mettant en place une gouvernance de données et une intendance de données basées sur les meilleures pratiques.

   2. *Actifs et Normes*;

      Qui consiste à gérer les données comme un actif stratégique et à les orchestrer de manière à les repérer facilement et à les exploiter pour créer de la valeur pour l'organisation.

   3. *Outils et Environnement*;

      Qui consiste à fournir aux utilisateurs des outils et un environnement technologique avancés et habilitants leur permettant d'exploiter les données sans nécessairement avoir recours à une équipe d'experts.

   4. *Personnes et Culture*;

      Qui consiste à créer une main-d'œuvre renseignée et compétente en matière de données et à développer une culture organisationnelle axée sur les données.

b. Les moteurs opérationnels sont les grands principes à respecter dès la mise en œuvre de la stratégie et tout au long de son cycle de vie. Ils sont :

   1. *Confidentialité des données, Protection des renseignements personnels et Respect de la vie privée*;

      Qui consiste à rendre les données disponibles aux personnes qui en ont besoin dans un environnement de confiance. Les données sont identifiées et sécurisées en fonction de leur sensibilité, confidentialité et niveau de diffusion. Elles sont utilisées de façon éthique et transparente face aux usagers;

   2. *Qualité des données de leur collecte jusqu'à leur exploitation*;

      Qui consiste à nettoyer et à organiser les données afin qu'elles apportent de la valeur pour l'organisation. Les données sont fiables, c'est-à-dire qu'elles ne sont pas faussées d'aucune façon et elles sont aptes à l'emploi;

   3. *Sécurité des environnements, des outils et des réseaux*;

      Qui consiste à sécuriser les environnements qui collectent et hébergent les données, les outils qui traitent et exploitent les données et les réseaux sur lesquels transitent les données. L'environnement d'exploitation des données est donc un environnement de confiance qui protège les données. Il est robuste, fiable et à l'abri des intrusions malveillantes.

Par une transition des approches traditionnelles vers des approches numériques et à terme, par un changement de la culture organisationnelle, le CIUSSS de l'Estrie – CHUS compte utiliser sa stratégie de gestion des données pour devenir une organisation apprenante axée sur les données. Le tableau synoptique de la stratégie se trouve à l'annexe B.

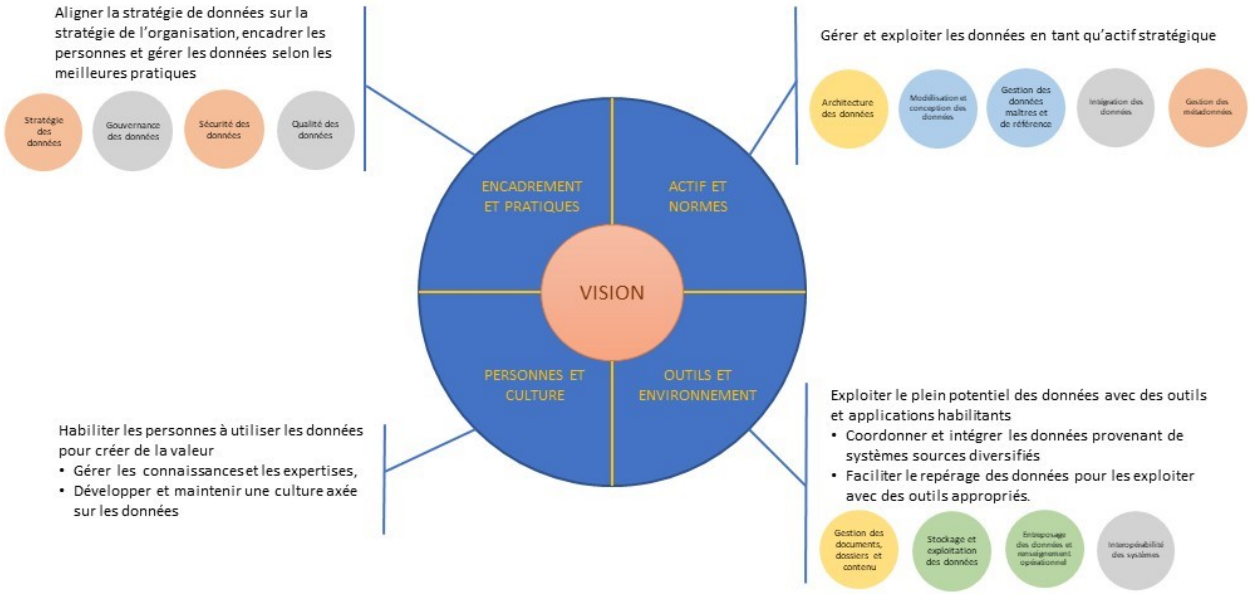


Figure 6 – Les quatre piliers de la Stratégie de gestion des données.
Chaque pilier regroupe un certain nombre de domaines de connaissance dans lesquels des activités doivent être réalisées pour soutenir la vision de l'organisation en matière de gestion des données. Les 11 domaines de connaissance du modèle DAMA s'y retrouvent en plus de la Stratégie elle-même et le domaine « Interopérabilité des systèmes ».

MISE EN ŒUVRE DE LA STRATÉGIE

La mise en œuvre de la stratégie de gestion des données repose sur l'application sur le terrain d'un modèle de gestion des données. Le modèle adopté par le CIUSSS de l'Estrie – CHUS est le modèle de « Data Management Association International » (DAMA International). Il est l'un des modèles les plus développés et il est adopté par de nombreuses grandes organisations qui traitent des mégadonnées. Le modèle comprend 11 domaines de connaissance répartis dans 3 des 4 piliers de la stratégie. À ces 11 domaines s'ajoute la Stratégie elle-même ainsi que le domaine « Interopérabilité des systèmes » (voir Figure 6). La description de chaque domaine de connaissance et les éléments à considérer qui lui sont attribués se retrouvent dans le document *Stratégie de gestion des données du CIUSSS de l'Estrie – CHUS*.

Le présent document, *Cadre de gouvernance des données*, regroupe les pratiques de gestion des données qui englobent les activités organisationnelles et les activités technologiques. Certaines de ces activités de gestion des données pourraient être automatisées à l'aide de technologies intelligentes pour soutenir et faciliter leur réalisation.

La mise en œuvre d'une stratégie de gestion des données permet au CIUSSS de l'Estrie – CHUS de :

- D'instaurer un modèle d'encadrement et de pratiques axés sur les données favorisant la réalisation de ses objectifs stratégiques et ses priorités organisationnelles;

- Miser sur des approches numériques axées sur les données, vues comme un actif stratégique pour la prise de décisions et leur opérationnalisation, afin de réaliser ses missions cliniques et universitaire. Ces approches numériques doivent s'harmoniser avec les directives et politiques du gouvernement du Québec, comme le *Plan stratégique MSSS 2019-2023* et la *Stratégie de transformation numérique gouvernementale 2019-2023*;
- Se doter d'un environnement de confiance qui favorise l'utilisation des données en mode « libre-service » sur une base quotidienne;
- Développer une culture organisationnelle axée sur les données lui permettant de devenir une organisation apprenante.

La réalisation de la *Stratégie de gestion des données* est la responsabilité de la Présidence-direction générale de l'organisation ou du gestionnaire qu'il délègue. Elle repose sur une gouvernance et une intendance des données bien orchestrées et performantes, permettant d'assigner les responsabilités appropriées à chaque personne liée de près ou de loin à la gestion des données de l'organisation d'une part, et d'autre part, de s'assurer que les données sont exactes, contrôlées, et faciles à découvrir et à traiter par les utilisateurs.

Publié par : La Presse canadienne avril 2019

CHAPITRE 2.2 – PERSONNES ET CULTURE

STRATÉGIE

La réalisation de la stratégie de gestion des données s'appuie de manière considérable sur les personnes et la culture. La stratégie adoptée en matière de personnes et de culture est la suivante :

Augmenter la littératie en matière de données et soutenir l'émergence d'une culture orientée sur les données afin d'assurer une utilisation éthique des données en mode libre-service.

Au-delà de l'habilitation des personnes, c'est toute l'organisation qui doit opérer un changement de culture en s'appropriant la vision qui guide la gestion du changement et en respectant les principes qui gouvernent la mise en œuvre et le maintien de la culture.

VISION

Habiliter les utilisateurs de données afin que ceux-ci puissent accéder aux données et les utiliser pour créer de la valeur pour l'organisation, et développer une culture de données pour devenir une organisation apprenante.

PRINCIPES DIRECTEURS

Les principes directeurs en matière de personnes et de culture sont les suivants :

1) L'établissement met en place les changements de pratique pour devenir une organisation apprenante axée sur les données, qui encourage son personnel et ses équipes à baser ses planifications et décisions sur l'analyse des données de l'organisation et de son environnement externe.
2) Le plan de développement des ressources humaines de l'établissement (PDRH) intègre la mise à niveau des compétences et l'augmentation de la littératie en matière de données afin que les utilisateurs accèdent aux données et les utilisent sans l'aide d'experts, en respect du contexte légal et réglementaire.
3) Les utilisateurs de données dans la communauté sont proactifs dans le développement de leur expertise et de leurs compétences. Ils adoptent un comportement éthique dans l'utilisation des données.

LES PERSONNES

Les personnes dans une organisation constituent le socle sur lequel s'appuie le développement de l'organisation apprenante. À titre de rappel, la clientèle visée par le présent cadre est constituée des groupes suivants :

- Les décideurs;
- La communauté interne du CIUSSS de l'Estrie – CHUS;

- Les chercheurs;
- Les usagers.

L'HABILITATION DE LA COMMUNAUTÉ INTERNE

La communauté interne du CIUSSS de l'Estrie – CHUS doit posséder les connaissances nécessaires pour comprendre les données et les utiliser adéquatement. Cette habilitation du personnel passe par :

- L'évaluation du degré actuel de littératie du personnel en matière de données;
- La mise en place d'un programme de développement des compétences et de formation continue en matière de données pour le personnel autorisé à utiliser les données dans le cadre de leurs fonctions;
- Des stratégies RH favorisant le recrutement et la rétention de personnel qualifié en gestion, analyse et science des données;
- En matière de recrutement et d'accueil des nouveaux employés :
  - À l'embauche, la considération du critère du niveau de littératie en matière de gestion des données.
  - Lors de l'accueil des employés, l'inclusion de connaissances de base sur la gestion des données dans les activités d'intégration.

L'ACCESSIBILITÉ POUR LES USAGERS

Afin que les usagers ou leur représentant légal puissent accéder à leurs données de santé :

- L'établissement développe des modalités qui permettent aux usagers d'accéder à leurs données de manière sécuritaire et confidentielle, conformément aux lois et règlements actuels.

LE DÉVELOPPEMENT DE L'EXPERTISE

Afin de permettre les échanges sur l'utilisation des données et de favoriser le développement du potentiel de création de valeur par les données au sein de l'établissement :

- L'établissement favorise la mise en place d'une communauté de pratique regroupant des experts de la donnée;
- Le PDRH considère les besoins de développement d'expertise en gestion des données;
- L'établissement favorise la participation des experts de la donnée à des groupes d'experts et des communautés en gestion des données provinciaux, nationaux et internationaux.

LA CULTURE

Effectuer un changement de culture vers une organisation apprenante qui valorise les données constitue un projet organisationnel d'envergure qui doit être soutenu par la haute direction puisqu'il vise l'établissement dans son ensemble. La Présidence-direction générale exerce un leadership qui permet d'appuyer et de promouvoir la confiance dans la culture des données, ainsi que dans la valeur de celles-ci. La haute direction fait également la promotion de l'utilisation des données dans les processus décisionnels.

Le changement souhaité dans l'organisation doit s'opérer à deux niveaux :

1. De façon plus large, on vise à développer un intérêt envers les données et à sensibiliser l'ensemble des utilisateurs potentiels en développant la connaissance générale sur le sujet.
2. Chez les utilisateurs de données, on souhaite augmenter la littératie pour développer une expertise de pointe, une connaissance de l'environnement de données et des potentialités liées à leur utilisation.

Le centre DORISE est à l'avant-plan de ce changement de culture et en est la tête de proue en matière d'expertise.

LE DÉVELOPPEMENT D'UNE CULTURE GÉNÉRALE AXÉE SUR LES DONNÉES

Pour soutenir le développement d'une culture partagée en matière de données :

- Le CIUSSS de l'Estrie – CHUS met de l'avant une culture axée sur l'utilisation éthique des données et promeut la transparence quant aux aspects touchant l'utilisation des données.
- Le principe de qualité des données à la source doit être bien compris et adopté largement pour atteindre les objectifs en matière d'accessibilité des données. Les personnes amenées à utiliser les systèmes qui comprennent des données doivent être sensibilisées à l'aspect névralgique de la qualité des données.
- Des protocoles d'échanges de données sont établis au sein et à l'extérieur de l'établissement afin de favoriser le partage des données, tout en assurant la protection des renseignements personnels et le respect de la vie privée.
- Un plan de gestion du changement et un plan de communication doivent être développés en amont de l'implantation, puis mis en œuvre pour accompagner celle-ci, afin de soutenir pleinement le changement de culture.

LE DÉVELOPPEMENT DU POTENTIEL DES UTILISATEURS

Pour soutenir le développement des compétences en matière de données chez les utilisateurs:

- Les outils d'exploitation des données développés ou acquis sont conviviaux et performants; ils soutiennent l'habilitation des utilisateurs afin que ceux-ci puissent éventuellement accéder aux données en mode libre-service.

- Le centre DORISE conseille et soutient les utilisateurs dans le développement d'une culture des données, promeut l'utilisation sécuritaire des données et assure l'utilisation des données dans un environnement de confiance.
- Le centre DORISE exerce un rôle de vigie quant aux nouveaux produits de données qui soutiennent le développement des utilisateurs.

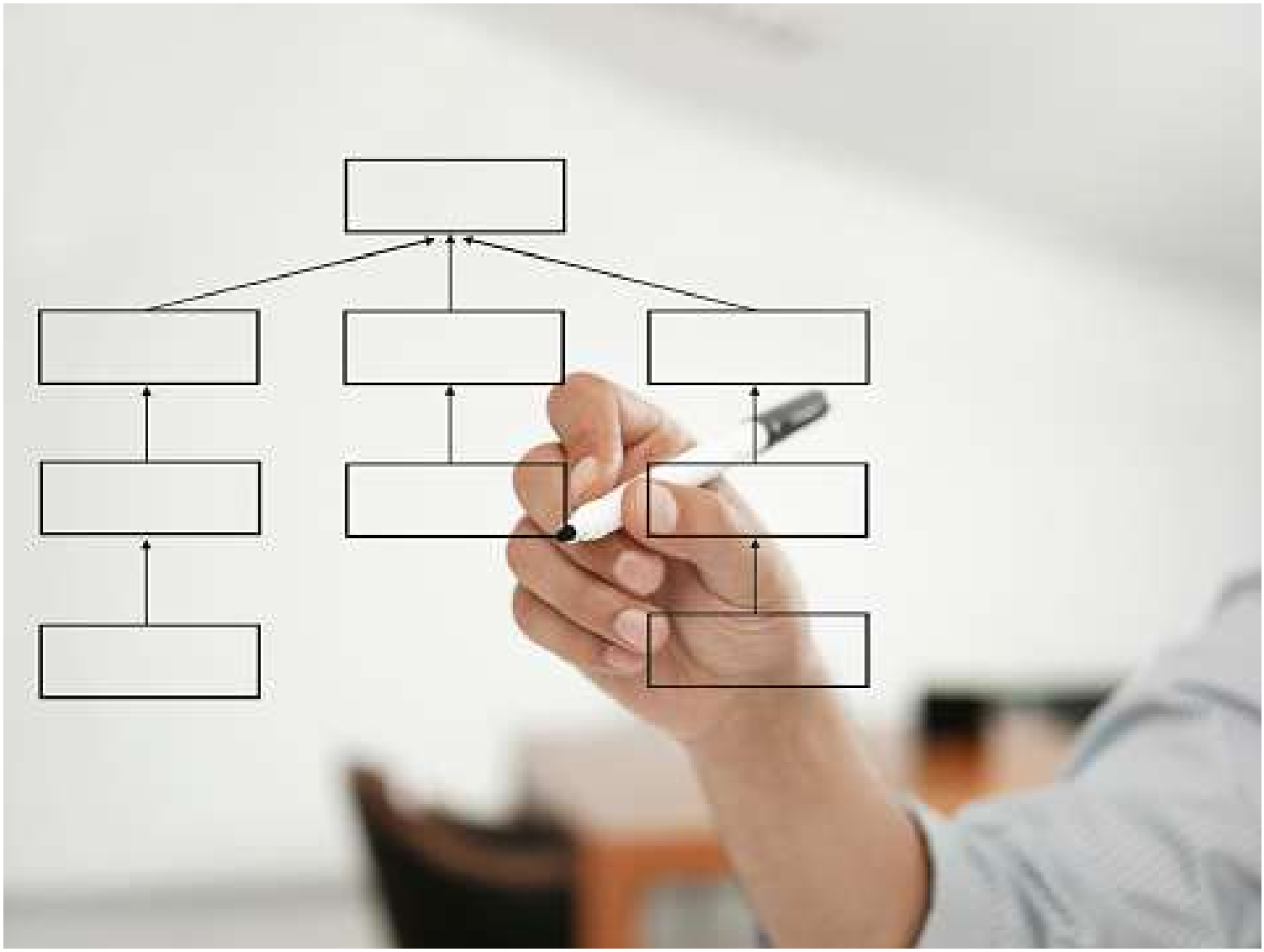
GOUVERNANCE

En matière de culture, la Présidence-direction générale soutient la transition vers une culture des données et vers le modèle de l'organisation apprenante. En ce sens, elle exerce un leadership mobilisateur en matière de données et imprime une direction forte.

L'ensemble des directions contribue à l'actualisation du changement de culture en matière de données.

La DRHCAJ est un acteur-clé en matière de changement chez les personnes et de changement de culture, puisqu'elle voit au développement des compétences du personnel et au recrutement d'une main d'œuvre adaptée aux défis de l'avenir en matière de données.

Le centre DORISE exerce un rôle central d'expertise et de référence en matière de données.



CHAPITRE 2.3 – Structure de gouvernance

PRINCIPES DIRECTEURS

La mise en place de la Stratégie de gestion des données et son suivi requièrent une structure de gouvernance qui respecte les principes directeurs suivants :

1. La structure de gouvernance des données s'intègre à la vision, à la mission et au plan d'organisation de l'établissement;
2. La gouvernance des données de l'établissement repose sur un **processus décisionnel centralisé** et une **intendance distribuée** à travers l'organisation dans les différentes directions détentrices de l'information;
3. La coordination des activités est mobilisée selon un **regroupement logique** des domaines d'affaires de la gestion des données;
4. Les détenteurs de l'information sont responsables de la production d'une donnée de qualité, de sa protection et de son utilisation sécuritaire et éthique.

Ces principes positionnent les données en tant qu'actif informationnel stratégique, capable de soutenir toute transformation qu'un établissement doit effectuer. Ils favorisent l'accès et l'utilisation sécuritaire des données par la communauté du CIUSSS de l'Estrie – CHUS et aident l'établissement à offrir des services optimaux à sa population.

STRUCTURE DE GOUVERNANCE

L'organigramme présenté à la Figure 7 Figure 7montre le positionnement des comités œuvrant dans les trois niveaux de gestion : stratégique, tactique et opérationnel.

- Au niveau stratégique, on retrouve la PDGA et le ***Comité stratégique de la mission universitaire*** qui assume les fonctions de ***Comité directeur de la gestion des données.***
- Au niveau tactique, on retrouve deux instances : le ***Comité de coordination de la sécurité, de l'accès et la protection des renseignements personnels*** et le ***Comité de coordination de la gestion des données, de la qualité et de l'éthique.***
- Au niveau opérationnel, on retrouve le ***Comité de gestion et d'assurance qualité des données*** et le ***Comité d'éthique de la recherche.***

Les directions DSP (responsable de la PRP), DRHCAJ (responsable de l'accès), PDGA (responsable de la sécurité) et DQEPP (par son centre DORISE) collaborent à soutenir la gouvernance.

Les détenteurs de données sont des instances opérationnelles importantes et se voient confier des responsabilités face à l'application des différents cadres liés à la gestion des données.

Les responsables suivants assument aussi un rôle important au sein de la gouvernance des données :

- Le responsable de la protection des renseignements personnels;
- Le responsable de l'accès aux documents;
- Le responsable de la sécurité de l'information (RSI);
- Le conseiller en gestion de la sécurité de l'information (CGSI);

- L'officier de sécurité de l'information (OSI);
- Le responsable de la gestion intégrée des risques.

Un lien fonctionnel entre les comités de coordination assure l'harmonie dans la mise en œuvre et le suivi des activités de gestion des données. Un lien hiérarchique entre le comité directeur et les comités de coordination assure la transmission d'une vision transversale de gestion des données à tous les niveaux de la gouvernance. Ce lien est assuré par la présence des présidents des comités de coordination au sein du comité directeur. Un lien hiérarchique similaire assuré par la présence des responsables des comités opérationnels au sein des comités de coordination permet la réalisation des activités opérationnelles en concordance avec la vision du comité directeur.

ORGANIGRAMME DE GESTION DE L'INFORMATION DU CIUSSS DE L'ESTRIE – CHUS

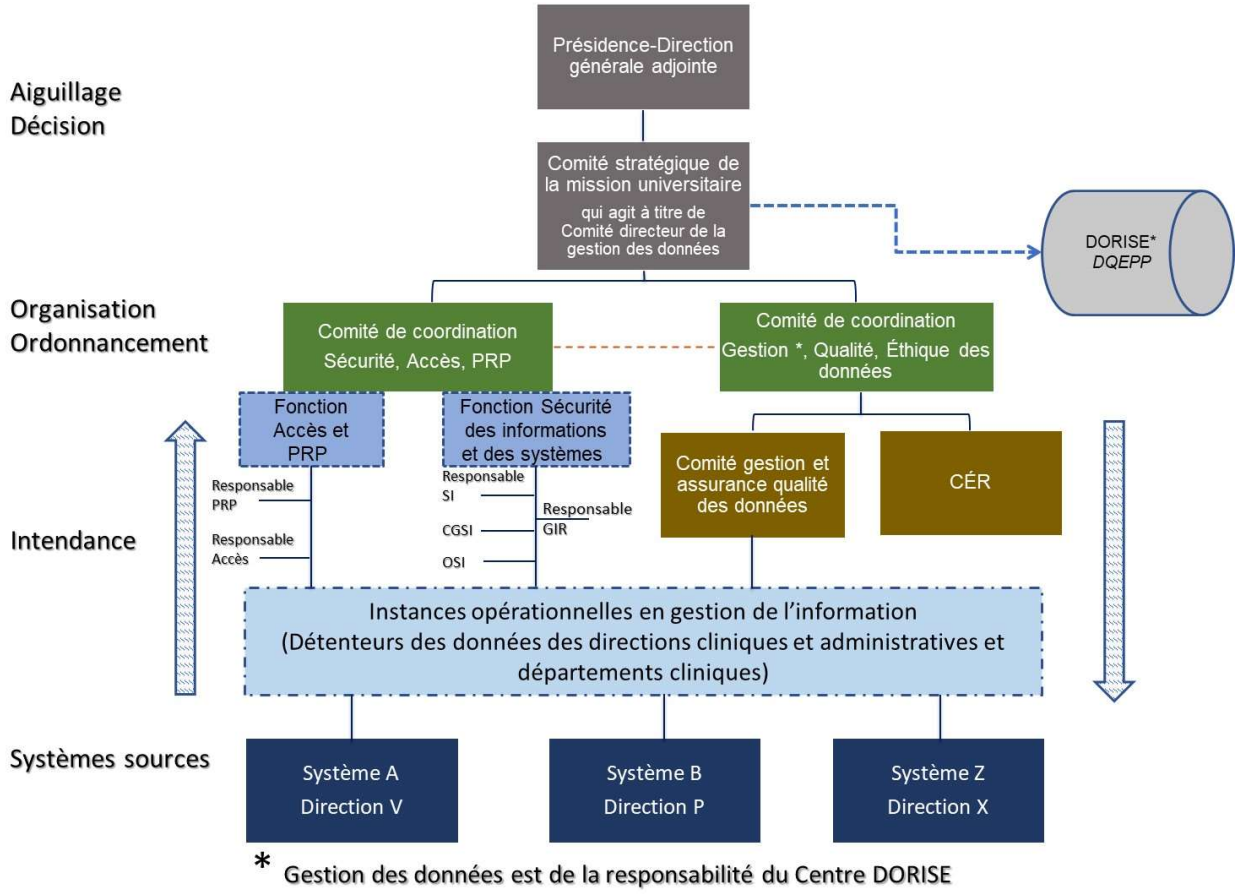


Figure 7 – Organigramme de gouvernance de la gestion des données du CIUSSS de l'Estrie – CHUS.
Ce diagramme montre le positionnement des comités œuvrant dans les trois niveaux de gestion : stratégique, tactique et opérationnel. La Présidence-direction générale adjointe est la direction-maître déléguée par le PDG pour assurer les responsabilités en matière de gestion des données dans l'ensemble de l'établissement.

COMITÉS PRÉVUS PAR LA LOI

En vertu de diverses lois au Québec, dont le Code civil du Québec, la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LGGRI) et la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (PRP)*, modernisée par la *Loi 25*, l'établissement doit mettre en place trois comités spécifiques : le *Comité d'éthique de la recherche*, le *Comité sur la sécurité de l'information* et le *Comité sur l'accès à l'information et sur la protection des renseignements personnels (PRP)*. L'organigramme de gouvernance de la Figure 7 montre que les fonctions des deux derniers comités sont intégrées au ***Comité de coordination de la sécurité, de l'accès et de la PRP.***

COMITÉS DE LA GOUVERNANCE

Comité directeur de la gestion des données

La responsabilité de la gestion des données de l'établissement est confiée à la Présidence-Direction générale adjointe. Sous l'autorité du PDGA, **le *Comité stratégique de la mission universitaire (CSMU)* assume le mandat du *Comité directeur de la gestion des données.***

Le comité se concentre sur les différents aspects stratégiques de la gouvernance des données, dont la supervision des travaux de mise en œuvre de la feuille de route de la Stratégie de gestion des données du CIUSSS de l'Estrie – CHUS et le pilotage des activités qui en découlent.

Les activités du comité touchent non seulement la gestion globale des données et de l'information de l'établissement, mais aussi l'ensemble des systèmes d'information qui y sont rattachés. Il s'assure que toutes les parties prenantes de la communauté du CIUSSS de l'Estrie – CHUS comprennent bien leurs rôles et responsabilités en matière de gestion des données et des systèmes.

Comité de coordination de la gestion, de la qualité et de l'éthique des données

Le ***Comité de coordination de la gestion, de la qualité et de l'éthique*** *des données* convient de la mise en œuvre et du suivi des orientations ou décisions du ***Comité directeur de la gestion des données*** dans les domaines relevant de sa responsabilité et en fait rapport à ce dernier.

Il s'assure de l'application des différents cadres de gestion des données en lien avec ses responsabilités, notamment le cadre de gestion des métadonnées, celui de la gestion de la qualité des données ainsi que les politiques et procédures d'application qui les concernent. Il s'associe au CÉR pour toute demande d'exploitation des données pour des fins de recherche.

Il est l'instance qui s'assure de la gestion et du suivi des priorités de développement du Centre DORISE qui relève de la Direction de la qualité, de l'éthique, de la performance et du partenariat (DQEPP).

Comité de coordination de la sécurité, de l'accès et de la protection des renseignements personnels

Le ***Comité de coordination de la sécurité, de l'accès et de la protection des renseignements personnels*** (PRP) coordonne la mise en œuvre et le suivi des orientations du ***Comité directeur de la gestion des données*** concernant ses responsabilités. Il est responsable de l'application opérationnelle et du respect de l'ensemble des règles et exigences définies au Cadre de gouvernance des données ainsi qu'aux différents cadres de gestion traitant de la sécurité de l'information, des règles d'accès aux données et aux documents, ainsi que de la PRP.

Le comité assume les responsabilités légales du ***Comité sur la sécurité de l'information***. Il agit à titre de conseiller-expert et assume l'évaluation des facteurs relatifs à la vie privée dans tous les projets de l'établissement qui concernent un système d'information ou une prestation électronique de services qui recueille, utilise, conserve, communique et élimine des renseignements personnels.

Le comité assume également les responsabilités légales du ***Comité sur l'accès et la protection des renseignements personnels***. Il est responsable d'établir la Politique de confidentialité et de rédiger le Cadre de gestion sur l'accès et la PRP ainsi que d'en assurer le respect au quotidien. Il joue également un rôle-conseil auprès des directions en ces matières.

Comité de gestion et de l'assurance qualité des données

Le ***Comité de gestion et de l'assurance qualité des données*** assume le mandat opérationnel d'amélioration continue de la qualité des données. Il établit les critères de qualité et les mécanismes de gestion de la qualité, élabore le plan d'action annuel et met en place un tableau de bord de suivi de la qualité des données.

Il collabore avec les pilotes de systèmes à la validation des mécanismes de gestion des données des systèmes sources (compilation, traitement, exploitation) conformément aux règles internes de l'établissement. Il collabore aussi à la validation des différents cadres et directives ministériels. Il en évalue les impacts sur la gestion des données à tous les niveaux de l'organisation et recommande les correctifs nécessaires aux processus de saisie, de traitement et d'analyse des données.

Détenteurs de l'information

Les détenteurs de l'information sont les directions du CIUSSS de l'Estrie – CHUS qui utilisent des systèmes d'information sources, soit pour collecter des informations ou pour les manipuler afin de soutenir les activités de l'établissement. Les détenteurs de l'information jouent un rôle primordial dans la gestion de l'information qu'ils colligent et qu'ils détiennent. Ils s'assurent que les données qu'ils détiennent dans leurs systèmes d'information sont sécuritaires, disponibles, intègres, de qualité et confidentielles. Ils sont responsables de l'application des différents cadres de gestion ou cadres normatifs par l'ensemble de leur personnel et doivent faire rapport aux deux comités de coordination, selon les responsabilités de chacun, des problématiques rencontrées. Ils travaillent en collaboration avec le Centre DORISE dans l'évolution des cadres de gestion et des cadres normatifs.

CONTRIBUTEURS À LA GOUVERNANCE

Centre DORISE de la DQEPP

Le Centre de données organisées du réseau informatique de la santé de l'Estrie (DORISE) est situé dans la DQEPP. Au sein de la gouvernance des données de l'établissement, ce centre est désigné comme l'intendant principal des données. À ce titre, il applique les règles et politiques à suivre durant tout le cycle de vie des données afin de fournir des données de qualité, en toute sécurité et confidentialité et en respect de la vie privée. Le Centre DORISE ne travaille pas seul. Ses principaux collaborateurs sont les pilotes des systèmes des directions productrices de données. On les appelle les détenteurs de données.

Le Centre DORISE et les détenteurs de données sont des portes d'accès aux données de l'établissement (voir chapitre « Accès aux données » pour plus de détails). Le Centre DORISE est l'unique porte d'accès aux données pour les secteurs de la recherche et de l'innovation. Il gère les demandes d'accès aux données (évaluation de l'admissibilité et de la faisabilité des demandes) en collaboration avec le comité d'éthique à la recherche et les directions directement impliquées dans l'évaluation des projets de recherche et des projets d'innovation.

La mission du Centre DORISE est

> *Promouvoir et soutenir l'utilisation des données de santé, créer et diffuser la connaissance et contribuer au développement d'innovations en valorisation des données dans l'établissement*

Il assume ainsi l'application sur le terrain du *Cadre de gouvernance des données*, en plus d'appliquer les différents cadres de gestion, notamment le *Cadre normatif de l'anonymisation des données,* le *Cadre de gestion de la qualité des données*, le *Cadre de gestion intégré des risques*, le *Cadre de gestion des accès*, le *Cadre de gestion des métadonnées* et le *Cadre sur les pratiques organisationnelles sur l'analyse avancée des données*. Il convient des moyens pour actualiser les orientations prises concernant la sécurité, la qualité et l'accès aux données. Il réalise les audits internes de conformité, émet les avis et met en place les changements requis.

Directions contributrices

Plusieurs instances et directions du CIUSSS de l'Estrie – CHUS assument déjà des responsabilités en gestion de l'information et des systèmes. Une telle contribution permet d'assurer une gestion transversale des données et informations. Elle permet aussi d'augmenter les forces vives directement impliquées dans la gouvernance des données. Chacune d'entre elles collabore à sa manière en accomplissant diverses tâches détaillées à l'annexe C. Les principaux contributeurs sont :

- Conseil d'administration (CA);
- Présidence-Direction générale adjointe (PDGA);
- Direction de la qualité, éthique, performance et partenariat (DQEPP);
- Direction de la coordination de la mission universitaire (DCMU);
- Direction des services professionnels (DSP);
- Direction des ressources humaines, des communications et des affaires juridiques (DRHCAJ);
- Direction des ressources financières (DRF);

- Direction des ressources informationnelles et technologiques (DRIT);
- Directions détentrices de données.

SECTION 3 – ASSURER LA VIE PRIVÉE DES PERSONNES

CHAPITRE 3.1 – CONFIDENTIALITÉ ET PROTECTION DES DONNÉES ASSURANT LA VIE PRIVÉE

LIEN AVEC LA STRATÉGIE DE GESTION DES DONNÉES

Le présent chapitre traite de confidentialité et des mécanismes de protection des données confidentielles (PDC) dans le contexte d'utilisation secondaire. L'appellation « **donnée confidentielle** » comprend le renseignement personnel, tel que défini dans la *Loi 25*, et le renseignement de santé ou de services sociaux, tel que défini dans le projet de loi 3. Les concepts de confidentialité et de protection des données confidentielles présentés ici sont l'essence même du premier moteur opérationnel de la *Stratégie de gestion des données du CIUSSS de l'Estrie – CHUS* :

Assurer le respect de la vie privée, la confidentialité des données et la protection des renseignements personnels des usagers.

Ce moteur opérationnel comporte certains principes à respecter :

1. Le respect de la vie privée des usagers guide l'utilisation des données;
2. Les données sont disponibles seulement aux personnes autorisées qui en ont besoin;
3. Les données sont disponibles et utilisées dans un environnement de confiance;
4. Les données sont identifiées et sécurisées en fonction de leur sensibilité et leur confidentialité;
5. Les données sont utilisées de façon éthique et transparente pour les usagers;

DÉFINITIONS

RESPECT DE LA VIE PRIVÉE

Le droit au respect de la vie privée consiste à garder secrète l'intimité de la vie d'une personne physique. Selon le Code civil du Québec : « Toute personne a droit au respect de sa réputation et de sa vie privée. Nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci y consente ou sans que la loi l'autorise ».[7] Ce droit s'applique aussi dans les activités d'exploitation des données d'un établissement de santé comme le CIUSSS de l'Estrie – CHUS.

RENSEIGNEMENTS PERSONNELS

Les **renseignements personnels** sont les données qui concernent une personne physique et qui permettent de l'identifier, par exemple : nom, prénom, numéro d'assurance maladie, date de naissance, numéro de téléphone, le lieu de résidence, les caractéristiques physiques distinctives, etc.

[7] Art. 35 C.c.Q.

RENSEIGNEMENTS DE SANTE OU DE SERVICES SOCIAUX

Les **renseignements de santé ou de services sociaux** sont les données détenues par un organisme du secteur de la santé et des services sociaux qui concernent une personne physique et qui permettent ou non de l'identifier, par exemple : l'état de santé, les habitudes de vie, tout matériel prélevé dans le cadre d'une évaluation ou d'un traitement, etc.

Les renseignements personnels sont considérés comme des renseignements de santé ou de services sociaux[8] lorsque :

- Ils sont accolés à un autre renseignement de santé ou de services sociaux ;
- Ils sont collectés lors de l'enregistrement, de l'inscription ou de l'admission de la personne concernée dans un établissement de santé ou de services sociaux ou de sa prise en charge par un autre organisme du secteur de la santé et des services sociaux.

CONFIDENTIALITÉ DES DONNÉES

Le concept de confidentialité s'applique aux **renseignements personnels** et aux **renseignements de santé ou de services sociaux.** Ces deux types de renseignements sont traités en toute **confidentialité**[9] – ils ne sont accessibles ou divulgués qu'aux personnes ou entités désignées et autorisées. Les renseignements traités de cette manière sont appelés dans ce chapitre « données confidentielles ».

À l'inverse, le **bris de confidentialité** est toute divulgation illégale de données confidentielles ou leur accès par une personne non autorisée ou qui n'a pas obtenu le consentement de la personne concernée, peu importe le support sur lequel les données se trouvent.

L'obligation de confidentialité est applicable à tous en matière de données confidentielles, sauf pour certaines exceptions prévues spécifiquement par la loi, dont le consentement de la personne concernée.

PROTECTION DES DONNÉES CONFIDENTIELLES

Les données qui doivent être protégées pour assurer leur caractère confidentiel sont les **données confidentielles.** La protection des données confidentielles constitue la mise en œuvre d'un ensemble de mesures légales et administratives prises par un établissement de santé et de services sociaux pour protéger les données portant sur les personnes physiques contre toute utilisation inappropriée[10]. Ceci s'applique aux données recueillies, détenues, conservées, utilisées et éliminées par le CIUSSS de l'Estrie – CHUS.[11]

[8] Tiré des définitions du Projet de loi 3.

[9] Confidentiel : Qui se dit, se fait en confidence, qui contient des informations qui doivent rester secrètes.

[10] Thésaurus de l'activité gouvernementale http://www.thesaurus.gouv.qc.ca/tag/terme.do?id=10264

[11] Le lecteur peut se référer à la politique B001-POL-03 « Politique de la sécurité de l'information » du CIUSSS de l'Estrie – CHUS pour obtenir plus de détails.

OBLIGATIONS DE L'ÉTABLISSEMENT ET DE SON PERSONNEL

Les notions de respect de la vie privée, de confidentialité et de protection des renseignements personnels sont édictées par plusieurs lois. Dans ce chapitre, nous spécifions certaines obligations spécifiques à ces notions. Ces obligations sont étendues aux données confidentielles gérées par l'établissement.

OBLIGATIONS LIÉES À LA VIE PRIVÉE

Le respect de la vie privée d'une personne passe non seulement par la mise en place et le respect de mesures visant la confidentialité et la protection des données confidentielles, mais aussi **par une obligation d'évaluer les facteurs liés à la vie privée**. La ***Loi 25*** exige la réalisation d'une telle évaluation dans plusieurs circonstances impliquant les renseignements personnels. Dans ce chapitre, ces circonstances s'étendent aux données confidentielles que l'établissement collecte, exploite et conserve ou détruit. Ces circonstances sont :

1. Lors d'un projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui implique des données confidentielles (article 63.5);
2. Lorsqu'un organisme public veut communiquer des données confidentielles sans le consentement des personnes concernées à une personne ou à un organisme qui souhaite utiliser ces données à des fins d'étude, de recherche ou de production de statistiques (article 67.2.1);
3. Lorsqu'un organisme public veut communiquer, à l'extérieur du Québec, des données confidentielles ou qu'il souhaite confier à une personne ou à un organisme à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte de telles données (article 70.1).

Selon la Commission d'accès à l'information (CAI), l'évaluation des facteurs relatifs à la vie privée est une démarche préventive qui consiste à considérer tous les facteurs qui entraîneraient des conséquences positives ou négatives sur le respect de la vie privée des personnes concernées. La CAI rend disponible sur son site web un guide d'accompagnement intitulé : *Réaliser une évaluation des facteurs relatifs à la vie privée*.

OBLIGATIONS LIÉES À LA CONFIDENTIALITÉ ET LA PROTECTION DES DONNÉES CONFIDENTIELLES

Le CIUSSS de l'Estrie – CHUS se donne des obligations à respecter au regard de la confidentialité et de la protection des données confidentielles qu'il collecte, utilise et dont il dispose dans le cadre de ses activités quotidiennes. Elles sont calquées sur les règles édictées dans la *Loi 25* et le *Projet de loi 3* et sont résumées à la Figure 8. Elles seront détaillées dans le futur Cadre de gestion des accès et de la protection des données confidentielles dont l'établissement se dotera.

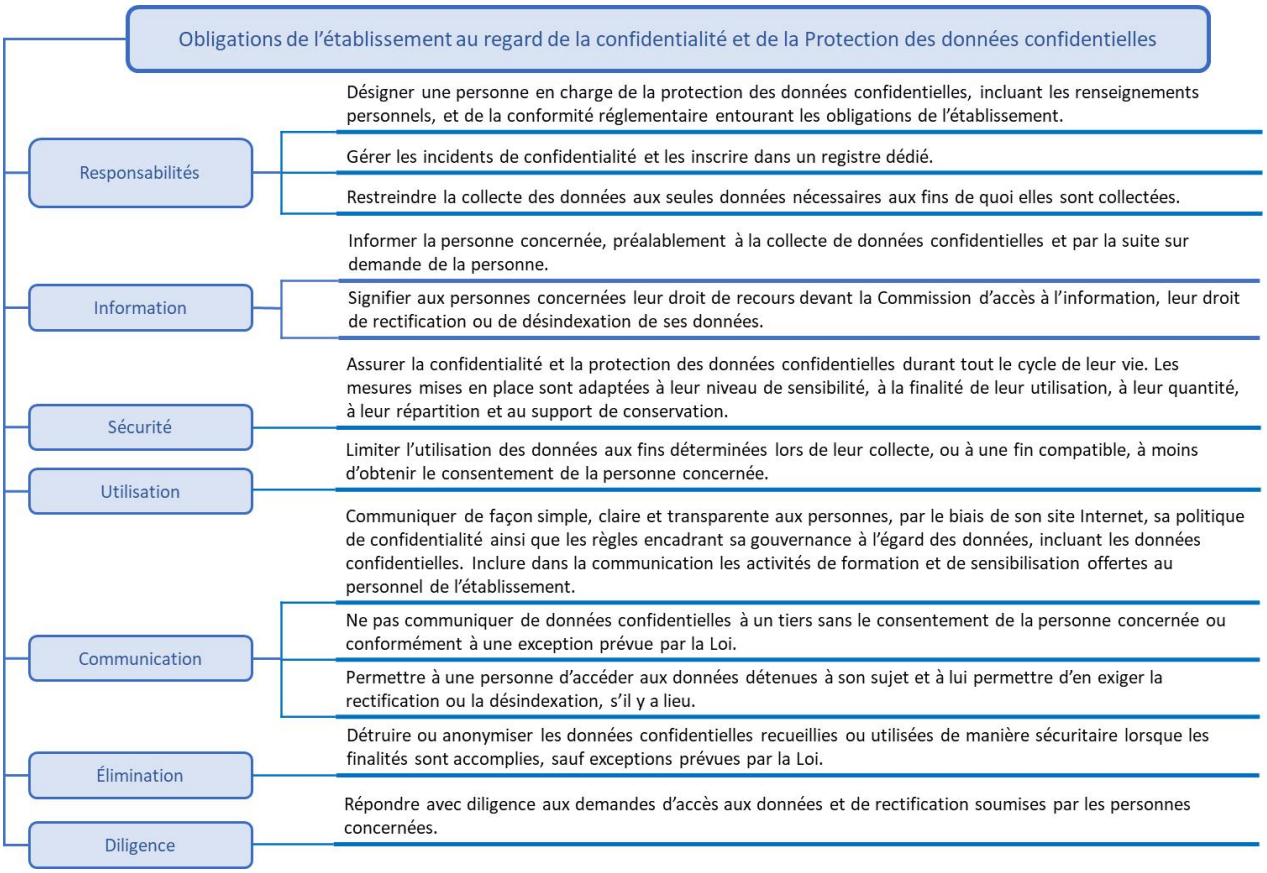


Figure 8 – Obligations de l'établissement au regard de la confidentialité et la protection des données confidentielles.
Obligations de l'établissement au regard des données confidentielles qu'il collecte, exploite et conserve ou détruit. Ces données incluent les renseignements personnels, selon la définition spécifiée dans la Loi 25, et les renseignements de santé ou de services sociaux, selon la définition spécifiée dans le Projet de loi 3.

Étant un organisme public, le CIUSSS de l'Estrie – CHUS s'acquitte de ses obligations en mettant en place les structures et les ressources nécessaires. L'une des structures importantes à mettre en place est un modèle de gestion de la protection des données confidentielles adapté à sa situation. Le modèle publié par le gouvernement du Québec en 2009 : *Modèle de pratique de la protection des renseignements personnels* version 1.1 (voir Figure 9) comprend tous les principaux éléments de gestion des renseignements personnels. **Étendu à l'ensemble des données confidentielles que détient l'établissement, ce modèle constitue une base de travail intéressante à l'élaboration du modèle de l'établissement.** L'annexe D détaille davantage le modèle gouvernemental.

Le modèle présente 17 pratiques de gestion et 24 pratiques spécifiques du processus opérationnel à atteindre pour assurer une saine gestion de la PRP. L'établissement choisit et adapte jusqu'à la totalité des pratiques en élaborant des exigences et en mettant en place une série d'activités pour les employés, professionnels, gestionnaires et utilisateurs de banque de données. Ils sont des acteurs de premier plan dans la gestion adéquate des données qui circulent au sein de l'établissement. Les exigences élaborées se retrouveront dans le futur Cadre de gestion des accès et de la protection des données confidentielles. Ce cadre deviendra alors l'outil de gestion privilégié.

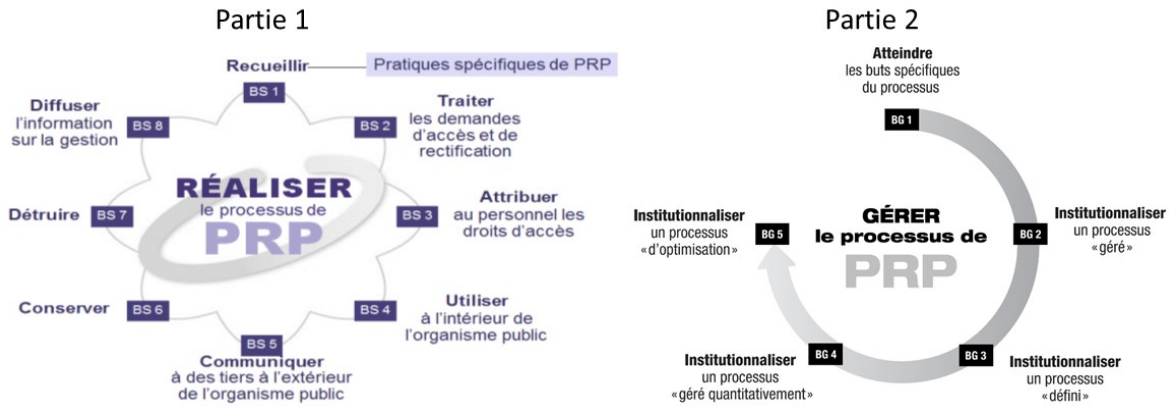


Figure 9 – Modèle de pratique de la protection des renseignements personnels, version 1.1.
Modèle suggéré comme référence à la conception du modèle de pratique de la protection des données confidentielles adapté à la situation de l'établissement. La partie 1 du modèle comprend un processus de gestion qui vise l'atteinte de 5 buts de gestion (BG-1 à BG-5) en observant 17 pratiques de gestion (PG-1.1 à PG-5.2). La partie 2 du modèle comprend un processus de PRP qui vise l'atteinte de 8 buts spécifiques (BS-1 à BS-8) en observant 24 pratiques spécifiques (PS-1.1 à PS-8.2).

MÉCANISMES DE PROTECTION DES DONNÉES CONFIDENTIELLES

Les mécanismes de protection des données confidentielles sont un ensemble de mesures appliquées aux données de l'établissement visant à assurer leur confidentialité et protection. Les mécanismes jugés importants sont discutés brièvement dans cette section. La Figure 10 montre une synthèse de ces mécanismes.

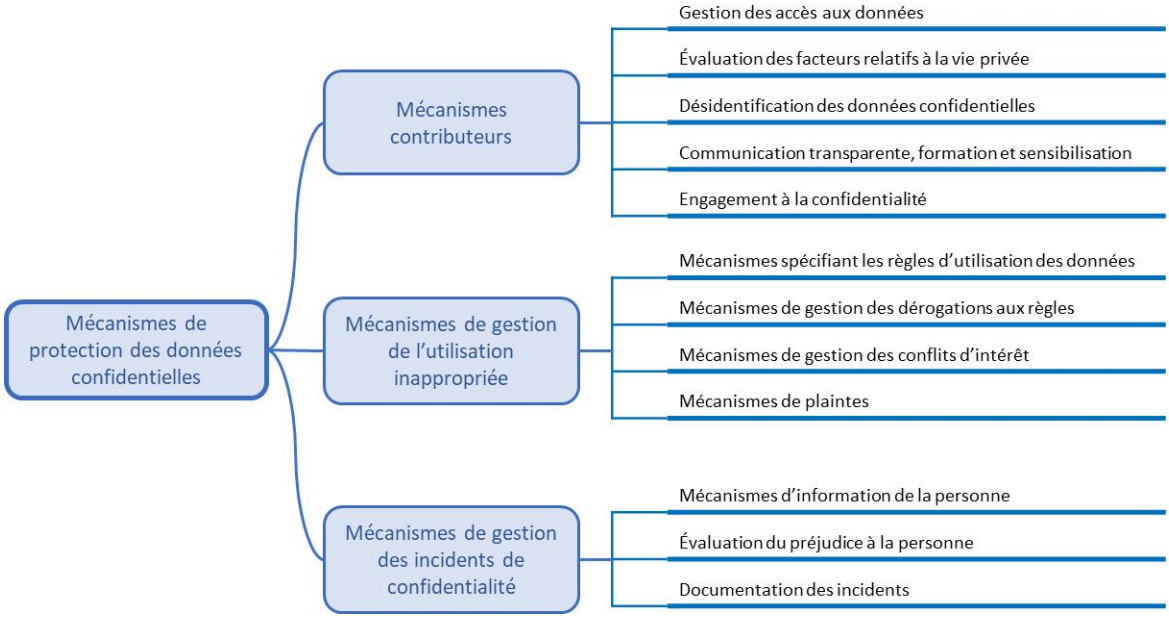


Figure 10 – Synthèse des mécanismes de protection des données.
Ils constituent l'ensemble des mesures appliquées aux données afin d'assurer leur confidentialité et protection. Trois types de mécanismes sont considérés : les mécanismes contribuant directement à la protection des données, les mécanismes de gestion de l'utilisation inappropriée des données et les mécanismes de gestion des incidents de confidentialité.

MÉCANISMES CONTRIBUTEURS À LA PROTECTION DES DONNÉES CONFIDENTIELLES

Les mécanismes contributeurs, discutés plus en détail à l'annexe E, ont un impact direct sur la confidentialité des données. Ils concernent les données confidentielles elles-mêmes, les droits des personnes concernées et les obligations des utilisateurs de données. Les principaux mécanismes sont :

1. La gestion des accès – deux mécanismes sont préconisés, selon les capacités des systèmes d'information et des banques de données :
    - Autorisation d'accès basée sur le rôle de l'utilisateur (*role-based authorization*);
    - Autorisation d'accès plus raffinée impliquant des conditions particulières (*fine-grained authorization*);
2. L'évaluation des facteurs relatifs à la vie privée (voir section précédente);
3. La désidentification des données confidentielles – deux méthodes éprouvées sont préconisées :
    - La dépersonnalisation, un mécanisme **réversible** de désidentification;
    - L'anonymisation, un mécanisme **irréversible** de désidentification;
4. La communication transparente, la formation et la sensibilisation;
    - L'établissement communique de façon transparente, par le biais de son site Internet, les règles qu'il met en place pour gérer ses données, en vertu de la ***Loi 25*** (art. 63.3 et 63.4);
    - Le plan de développement des ressources humaines (PDRH) de l'établissement inclut une description des activités de formation et de sensibilisation que l'établissement offre à son personnel;
5. L'engagement à la confidentialité.
    - Tout utilisateur de données confidentielles signe le formulaire d'engagement à la confidentialité de l'établissement, en vertu de la ***Loi 25*** (art. 67.2.3);

Lors de l'acquisition de son code d'accès aux données, l'utilisateur de données confidentielles reçoit un rappel spécifiant qu'il s'engage à respecter les politiques et procédures de l'établissement concernant la sécurité de l'information, la confidentialité et la protection des données confidentielles contribuant au respect de la vie privée. Ce rappel mentionne la notion d'imputabilité de tous les utilisateurs et inclut également les représailles possibles suivant le non-respect des politiques tel que spécifié dans la ***Loi 25***.

MÉCANISMES DE GESTION DE L'UTILISATION INAPPROPRIÉE DES DONNÉES CONFIDENTIELLES

Règles fondamentales d'utilisation des données

Deux règles fondamentales doivent être respectées :

- N'utiliser les données qu'aux seules fins prévues à l'autorisation d'accès;

  - L'autorisation d'accès pour des fins d'études et de recherche suit un processus bien défini qui respecte plusieurs règles assurant la protection des données confidentielles.

- N'utiliser les données qu'aux seules fins prévues dans le formulaire de consentement de l'usager;
  - D'autres fins d'utilisation des données, sans le consentement de l'usager, sont prévues par la ***Loi 25***;
  - D'autres fins d'utilisation des données sont possibles si une procédure pour recontacter la personne concernée est explicitement prévue pour obtenir un nouveau consentement.

Dérogation aux règles de protection des données confidentielles

Les mécanismes administratifs internes existants concernant toute personne de la communauté interne du CIUSSS de l'Estrie – CHUS qui contrevient ou déroge aux directives de confidentialité et de protection des renseignements personnels, sont aussi utilisés dans le contexte d'utilisation secondaire des données confidentielles.

Toute personne qui contrevient ou déroge à ces directives peut s'exposer, selon le cas, à des mesures disciplinaires, administratives ou légales en fonction de la gravité de son geste.

Un membre de la communauté du CIUSSS de l'Estrie - CHUS qui est au fait d'un acte répréhensible doit le divulguer selon la procédure en vigueur (B000–PROCD-01).

Gestion des conflits d'intérêts

Les mécanismes administratifs internes existants concernant toute personne de la communauté interne du CIUSSS de l'Estrie – CHUS qui se place dans une situation de conflit d'intérêt, sont aussi utilisés dans le contexte d'utilisation secondaire des données. En effet, tout utilisateur d'une banque de données ne peut se placer en situation de conflit d'intérêts pour tirer profit personnellement des accès qui lui sont dévolus et de l'information qu'il obtient dans le cadre de ses fonctions ou par entente particulière. Nul ne peut distribuer, publier ou vendre des données de l'établissement ou des rapports quelconques issus des données de l'établissement sans autorisation. De plus, la politique sur la propriété intellectuelle s'applique dans le cas de données produites à la suite d'une analyse (données dérivées telles que définies au premier chapitre de ce document).

Mécanisme de plaintes

Le mécanisme administratif interne existant est utilisé pour un usager ou toute personne désirant formuler une plainte concernant l'utilisation secondaire inappropriée des données.

Un usager ou un membre du personnel de l'établissement peut déposer une plainte au Commissaire aux plaintes de l'établissement s'il est au fait d'un non-respect des règles de confidentialité, de protection des données confidentielles et de respect de la vie privée, conformément aux règles de l'établissement, incluant l'application des règles inscrites au présent chapitre. La procédure existante qui en détaille le mécanisme est aussi utilisée dans le contexte d'utilisation secondaire des données et le Bureau du commissaire aux plaintes analyse la plainte et émet les recommandations jugées nécessaires.

MÉCANISMES DE GESTION DES INCIDENTS DE CONFIDENTIALITÉ

Selon la *Loi sur la protection des renseignements personnels dans le secteur privé* (art. 9.1), « une personne qui exploite une entreprise et qui recueille des renseignements personnels en offrant un produit ou un service technologique doit s'assurer que, par défaut, les paramètres de ce produit ou service assurent le plus haut niveau de confidentialité, sans aucune intervention de la personne concernée ».

Le présent chapitre applique cette règle aux données confidentielles recueillies, conservées ou auxquelles on accède par le biais d'un produit ou d'un service technologique que possède un établissement de santé. Ce produit ou service est identifié dans le ***Projet de loi 3*** comme étant : une banque de données, un système d'information, un réseau de télécommunication, une infrastructure technologique, un logiciel ou une composante informatique d'un équipement médical.

Malgré les meilleures intentions du monde, des incidents de confidentialité peuvent survenir. Dans ce cas, trois étapes fondamentales doivent être réalisées :

1. Déclarer l'incident;
2. Évaluer le préjudice que cet incident cause à la personne concernée;
3. Documenter l'incident dans un registre spécialement conçu à cet effet.

Déclaration d'un incident

L'établissement qui a des motifs de croire que s'est produit un incident de confidentialité impliquant des données confidentielles qu'il détient et que cet incident présente un risque qu'un préjudice sérieux soit causé, doit, avec diligence, aviser :

1. La Commission d'accès à l'information (CAI);
2. La ou les personnes concernées par l'incident;

Si la ou les personnes concernées n'ont pas été avisées, la CAI peut ordonner à l'établissement de le faire, sauf lorsque cela est susceptible d'entraver une enquête effectuée en vertu de la Loi.

3. Toute personne ou tout organisme susceptible de diminuer ce risque;

Dans ce dernier cas, l'établissement n'est tenu de lui communiquer que les données confidentielles nécessaires à cette fin sans le consentement de la ou des personnes concernées. Le responsable de la protection des renseignements personnels de l'établissement enregistre la communication dans le registre des incidents.

Évaluation du préjudice à la personne

Lorsque l'établissement évalue le risque qu'un préjudice soit causé à une personne dont des données confidentielles sont concernées par un incident de confidentialité, il doit considérer minimalement les éléments suivants pour déterminer la marche à suivre :

- Le niveau de sensibilité des données concernées (p. ex. : données de santé ou d'identité);
- Les conséquences appréhendées de l'utilisation de ces données (p. ex. : vol d'identité ou atteinte à la vie privée);
- La probabilité que les données soient utilisées à des fins préjudiciables.

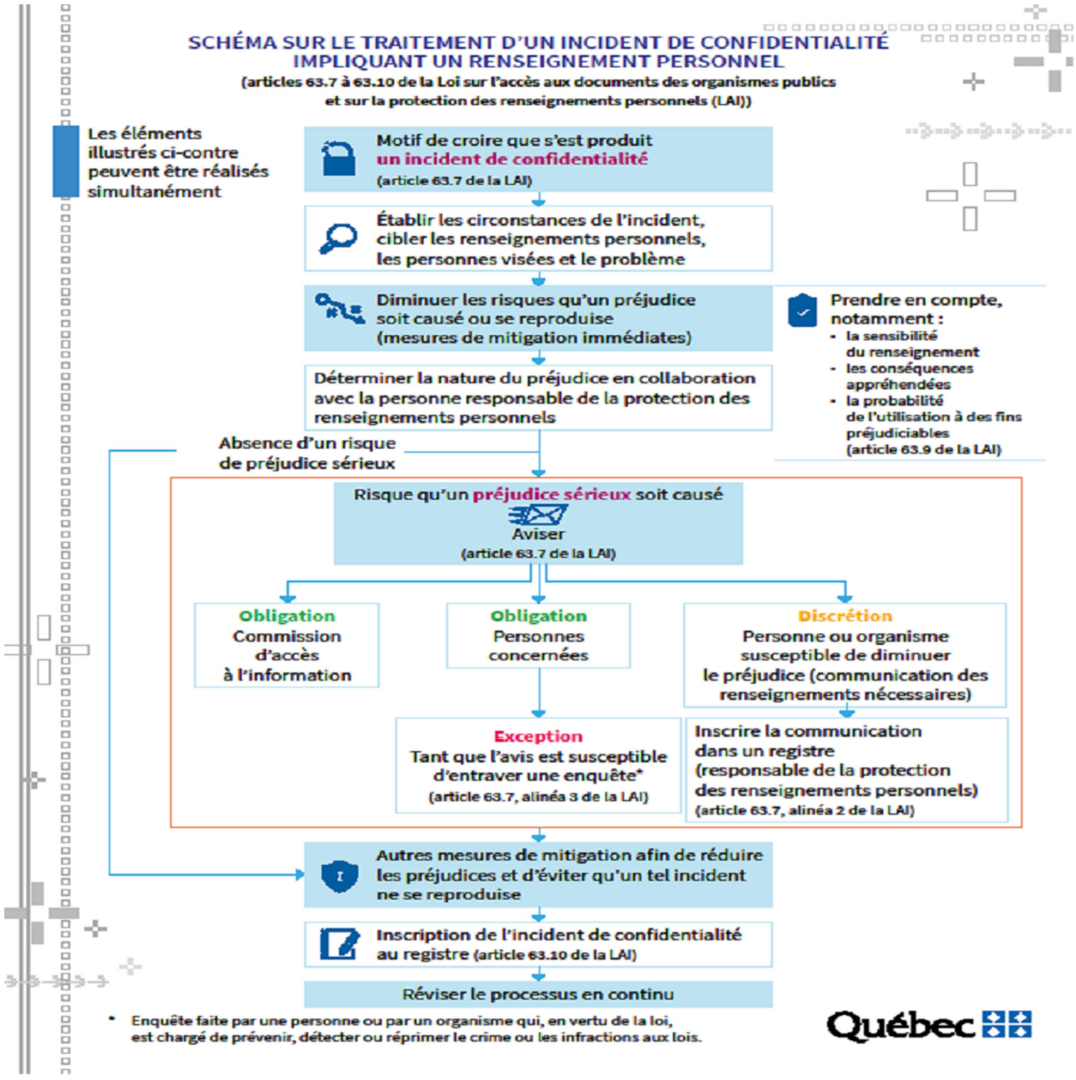


Figure 11 – Mécanisme de traitement d'un incident de confidentialité.
Procédure à suivre pour respecter les exigences légales en matière de gestion des incidents de confidentialité. Procédure publiée par le Secrétariat à l'accès et à la réforme des institutions démocratiques, 2021. Cette procédure qui se limite aux renseignements personnels peut s'étendre à l'ensemble des données confidentielles du CIUSSS de l'Estrie – CHUS.

Le Secrétariat à l'accès et à la réforme des institutions démocratiques[12] a publié en 2021 un modèle de traitement d'un incident de confidentialité, lequel comprend une évaluation du préjudice à la personne concernée (voir Figure 11). Ce modèle propose une procédure en plusieurs étapes qui respecte les articles 63.7 à 63.10 de la ***Loi 25***.

Ce modèle peut s'étendre à l'ensemble des données confidentielles d'un établissement de santé. Il est suggéré que le CIUSSS de l'Estrie – CHUS élabore son modèle en y schématisant toutes ses procédures actuelles et celles à venir (en respect aux nouvelles obligations de la ***Loi 25***) sur la base du modèle du Secrétariat à l'accès et à la réforme des institutions démocratiques.

[12] Tiré de https://www.quebec.ca/gouvernement/travailler-gouvernement/services-employes-etat/conformite/protection-des-renseignements-personnels/incident-de-confidentialite

Documentation des incidents

L'établissement doit tenir un registre des incidents de confidentialité, même de ceux qui ne présentent pas un risque de préjudice sérieux pour les personnes. Ce registre comprend minimalement :

1. La description de l'incident,
2. Les parties impliquées,
3. L'analyse réalisée,
4. Les communications faites et
5. Les moyens mis en place pour éviter la récurrence.

Sur demande de la CAI, une copie de ce registre doit lui être transmise.

GESTION DES RISQUES DE RÉIDENTIFICATION DES PERSONNES

Le CIUSSS de l'Estrie – CHUS a mis en place un programme de gestion des risques de sécurité de l'information, lequel traite du risque d'identifier une personne lorsqu'il y a communication d'informations contenues aux dossiers des usagers et de la manière de gérer ce risque. Dans le contexte d'utilisation secondaire des données, le risque de réidentification des personnes par l'utilisation de techniques d'inférence et de corrélation de données, d'intelligence artificielle ou autre, est bien présent. Lorsqu'avéré, ce risque constitue un incident de confidentialité pour lequel des mécanismes de gestion particuliers doivent être mis en place.

Il est suggéré d'inclure le risque de réidentification des personnes en contexte d'utilisation secondaire des données dans le programme de gestion des risques de sécurité de l'information.

OUTIL DE GESTION DES RISQUES DE RÉIDENTIFICATION

Les techniques de dépersonnalisation et d'anonymisation ne sont pas sans faille. La possibilité de réidentifier les personnes demeure toujours présente, plus particulièrement depuis que l'évolution technologique a facilité la consultation et l'analyse de données massives par le biais de croisement de plusieurs banques de données sur lesquelles des techniques d'intelligence artificielle sont appliquées. **L'avènement des nouvelles technologies intelligentes impose la mise en place de mesures technologiques et organisationnelles de gestion des risques associés aux données confidentielles.**

Mesures technologiques

Dans le but de prévenir un incident de confidentialité causé par la réidentification d'une personne, l'établissement peut se servir de certaines techniques, comme le *data mapping*, basées sur des technologies d'identification automatique des risques. Plusieurs outils sont disponibles sur le marché et pratiquement tous prennent en compte les éléments suivants :

1. La capacité de saisir et de qualifier le risque;
2. L'évaluation de l'impact ou du préjudice sur la personne;
3. Le taux d'occurrence du risque;

4. L'évaluation du niveau de risque;
5. La gradation des actions à prendre en fonction du niveau de risque pour les personnes concernées.

Il est suggéré que le CIUSSS de l'Estrie – CHUS se dote d'un outil d'identification automatique des risques et qu'il l'utilise lorsque des données sensibles sont utilisées.

Mesures organisationnelles

Malgré l'efficacité des outils modernes d'identification automatique des risques de réidentification, certains risques ne peuvent être qualifiés qu'avec l'intelligence humaine. Leur analyse nécessite l'intervention d'un spécialiste ou d'un groupe de spécialistes. Le mandat de ces derniers consiste, entre autres, à identifier les risques non qualifiables technologiquement, à évaluer les approches adoptées pour empêcher la réidentification des personnes et à contribuer à la mise en œuvre des mesures d'atténuation des risques.

Il est suggéré que l'établissement nomme un spécialiste ou un comité dont le mandat est d'évaluer le risque de réidentification des personnes dans les diverses situations nécessitant la collecte, le stockage, l'utilisation, et l'élimination ou conservation de données sensibles. Ce spécialiste ou groupe de spécialiste jouera un rôle important dans le processus d'évaluation des facteurs relatifs à la vie privée (EFVP).

MESURES D'ATTÉNUATION DU RISQUE DE RÉIDENTIFICATION

La *Politique sur la gestion intégrée des risques* du CIUSSS de l'Estrie – CHUS traite de l'identification des risques majeurs de l'établissement, de leur priorisation et de leur évaluation. Elle présente en annexe des échelles d'évaluation des risques qui peuvent être utilisées dans l'évaluation des risques de réidentification des personnes en contexte d'utilisation secondaire des données.

Cette politique traite aussi des mesures d'atténuation (ou contrôle) visant à réduire les risques. Plusieurs mesures d'atténuation des risques sont déjà en place dans l'établissement, dont la mise en place de mesures préventives de la divulgation accidentelle de l'identification des personnes pour toute situation nécessitant une utilisation de données et la formation des utilisateurs d'informations quant à leurs responsabilités et obligations face à la confidentialité des informations, À ces mesures, il est suggéré d'ajouter d'autres mesures plus spécifiques à l'utilisation secondaire des données de l'établissement, notamment :

1. Évaluer régulièrement la robustesse des approches et stratégies adoptées pour empêcher la réidentification des personnes malgré l'utilisation de techniques comme la dépersonnalisation et l'anonymisation;
2. Sur la base des niveaux de risque attribués, effectuer une validation du risque de réidentification pour tout jeu de données produit à des fins d'analyse dans le but de prévenir la communication (fortuite) de données confidentielles;
3. Limiter le nombre de personnes qualifiées pouvant accéder aux données d'identification et les manipuler à celles qui ont complété une formation sur la confidentialité et la protection des données confidentielles (incluant les renseignements personnels et les renseignements de santé ou de services sociaux) et qui ont signé un engagement à la confidentialité avec l'établissement. Le renouvellement de cet engagement sur une base annuelle est suggéré.

ÉVALUATION DU RISQUE DÉCOULANT D'UNE VIOLATION DE DONNÉES CONFIDENTIELLES

Une violation de données confidentielles peut se définir comme « tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles »[13].

Des exemples de violation de données sont :

- Suppression accidentelle de données de santé conservées par un établissement de santé et non sauvegardées par ailleurs ;
- Perte d'une clef USB non sécurisée contenant un ou des jeux de données confidentielles ;
- Introduction malveillante dans une base de données et modification ou altération de certaines données.

L'évaluation du niveau de risque engendré par une violation de données se fait au cas par cas. Il est difficile de généraliser ce type d'évaluation. Toutefois, elle peut être basée sur certains critères[14] dont plusieurs sont considérés dans le développement de systèmes experts de gestion des risques. On y retrouve notamment :

1. Le type de violation, par exemple : une mise en cause de l'intégrité des données, une rupture de la confidentialité ou encore une perte de la disponibilité des données;
2. La nature des données affectées, notamment des données non sensibles, des données sensibles, des données relatives aux infractions et condamnations, des données personnelles;
3. Le volume de données ou nombre de personnes concernées, par exemple à large échelle, important, limité ou faible;
4. La probabilité de matérialisation du risque d'identifier les personnes concernées grâce aux données faisant l'objet d'une violation. Une adaptation des cinq niveaux présentés dans la Politique de gestion intégrée des risques du CIUSSS de l'Estrie – CHUS (E000-POL-03, Annexe E) est proposée :
    a. *Probabilité improbable* – identification peu probable des personnes concernées sans déployer des moyens considérables;
    b. *Probabilité faible* – identification difficile des personnes concernées mais possible dans certains cas;
    c. *Probabilité modérée* – Identification occasionnelle des personnes concernées par le biais de techniques sophistiquées;
    d. *Probabilité élevée* – Identification fréquente des personnes concernées avec des techniques simples;
    e. *Probabilité très élevée* – Identification fréquente à certaine, directe ou extrêmement simple;

[13] Tiré de cnil.fr

[14] Digitemis cybersecurity & privacy web site.

5. Les impacts possibles pour les personnes concernées (gravité et vraisemblance). Une adaptation des cinq niveaux présentés dans la Politique de gestion intégrée des risques du CIUSSS de l'Estrie – CHUS (E000-POL-03, Annexe E) est proposée :
    a. *Impacts très faibles* – les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté;
    b. *Impacts faibles* – les personnes concernées connaîtraient des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés;
    c. *Impacts modérés* – les personnes concernées pourraient connaître des conséquences significatives, qu'elles pourront surmonter malgré quelques difficultés;
    d. *Impacts élevés* – les personnes concernées connaîtraient des conséquences significatives, qu'elles devraient pouvoir surmonter mais avec des difficultés réelles et significatives;
    e. *Impacts très élevés* – les personnes concernées connaîtraient des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter.
6. Les catégories de personnes concernées, par exemple des membres du personnel, des usagers, des clients, des mineurs, des personnes vulnérables;

À partir de ces critères, le risque identifié serait classé dans l'un des quatre niveaux de risque inhérent présentés dans la Politique E000-POL-03, soit très élevé, élevé, modéré ou faible. Il revient à l'établissement de mettre en place les mesures d'atténuation visant à réduire au minimum, voire à faire disparaître, et d'en mesurer l'efficacité en estimant le risque résiduel selon la méthode présentée dans la Politique E000-POL-03, et ce, à la satisfaction des personnes concernées.

GOUVERNANCE DE LA PROTECTION DES DONNÉES

COMITÉ DIRECTEUR DE LA GESTION DES DONNÉES

Ce comité agit sur le plan stratégique :

- Il facilite la consultation stratégique et horizontale, la collaboration et la prise de décisions sur toutes les initiatives nouvelles ou modifiées qui concernent la protection des données confidentielles;
- Il énonce une orientation stratégique pour établir les priorités et gérer les risques pour toutes les questions liées à la protection des données confidentielles;
- Il énonce des orientations stratégiques sur la gestion des conflits d'intérêt en situation d'utilisation des données, incluant les mesures coercitives;
- Il oriente la mise en place de mécanismes d'autorisation de la distribution, publication ou communication de données de l'établissement, incluant les données confidentielles ou de rapports quelconques issus des données de l'établissement;
- Il oriente la communication Internet des mécanismes de protection des données de l'établissement aux usagers et à la communauté interne de l'établissement;

- Il reçoit et analyse le tableau de bord annuel d'indicateurs stratégiques des audits et de suivis réguliers des mécanismes de surveillance mis en place. Il approuve les approches d'amélioration recommandées par le Comité de coordination de la sécurité, de la gestion des accès et de la PRP.

COMITÉ DE COORDINATION DE LA SÉCURITÉ, DE LA GESTION DES ACCÈS ET DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Ce comité approuve les mécanismes de protection des données confidentielles et de gestion des risques qui en découlent et assure le suivi de leur mise en œuvre. Il fait rapport des résultats au Comité directeur de la gestion des données :

- Il s'assure que les mécanismes administratifs internes existants de gestion des conflits d'intérêt s'appliquent à l'utilisation des données et qu'ils répondent aux orientations du Comité directeur de la gestion des données;
- Il détermine les règles de distribution, de publication ou de communication des données de l'établissement ou des rapports quelconques issus des données de l'établissement. Il assure le suivi de la mise en place des mécanismes assurant le respect de ces règles;
- Il détermine les procédures de gestion de l'utilisation inappropriée des données de l'établissement : mécanismes de surveillance, déclaration d'une utilisation inappropriée, étude des cas déclarés, mesures d'évitement de la récurrence, mesures de représailles au contrevenant;
- Il détermine, en collaboration avec les directions concernées, le contenu de la communication Internet des informations liées à la confidentialité et à la gouvernance des données de l'établissement, conformément à la *Loi 25*. Il collabore à la définition des mécanismes de communication avec les usagers et membres du personnel qui désirent obtenir plus d'information ou des réponses à leurs questions;
- Il élabore le tableau de bord annuel d'indicateurs stratégiques des audits et de suivis réguliers des mécanismes de surveillance mis en place. Il recommande les approches d'amélioration au Comité directeur de la gestion des données.
- Il collabore étroitement avec les personnes responsables de la protection des renseignements personnels de l'établissement dans le cadre d'un mandat élargi à la protection des données confidentielles;
- Il collabore à toute autre activité reliée à la protection des données confidentielles de l'établissement.

CENTRE DORISE ET PILOTES DE SYSTÈMES

L'application des mécanismes de protection des données identifiés par le Comité de coordination de la sécurité, de la gestion des accès et de la PRP relève du **Centre DORISE** pour les banques qui sont sous sa responsabilité et des **pilotes de systèmes** pour les systèmes sources et banques qui sont sous leur responsabilité. Des groupes de travail axés sur des initiatives nouvelles en matière de protection des données confidentielles peuvent être organisés pour des fins d'évaluation, de mise en œuvre ou de suivi. Le Centre ou les pilotes de systèmes recommandent au Comité de coordination de la sécurité, de la gestion des accès et de la PRP les approches à adopter par

l'établissement aux fins d'examen et collaborent avec les intervenants compétents pour mettre en œuvre les recommandations.

RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

La responsabilité de protection des renseignements personnels (PRP) du CIUSSS de l'Estrie – CHUS revient au Président-directeur général. Ce dernier a délégué cette fonction à un groupe d'intervenants qui oeuvrent en concertation et collaboration pour couvrir les divers angles de la PRP : clinique, administratif, juridique et autre. Les principales obligations des responsables de la PRP sont extraits des lois traitant de ce sujet, notamment la ***Loi 25***. Les diverses tâches de ces responsables sont transversales à l'établissement et sous la direction de son PDG. Dans le contexte de l'utilisation secondaire des données, les responsables de la PRP élargissent leurs fonctions à la protection des données confidentielles et se rattachent à la gouvernance de gestion des données mise en place dans l'établissement, plus particulièrement en collaborant directement avec le Comité de coordination de la sécurité, de la gestion des accès et de la PRP.

Publié par : La Presse canadienne avril 2019

CHAPITRE 3.2 – SÉCURITÉ DES DONNÉES

OBJECTIFS DU CHAPITRE

Le présent chapitre vise deux objectifs. Le premier est de sensibiliser le lecteur à l'importance accordée à la sécurité des données. Le second est d'indiquer au lecteur les éléments de gestion de la sécurité des données sur lesquels il doit porter une plus grande attention. Ces éléments se retrouvent plus en détail dans deux documents produits et publiés par la Direction adjointe des mesures d'urgence, de la sécurité civile et des enjeux organisationnels du CIUSSS de l'Estrie – CHUS. Ces documents sont :

1. Le Cadre de gestion en sécurité de l'information;
2. Le Cadre normatif en sécurité de l'information.

PRINCIPES DIRECTEURS DE LA SÉCURITÉ DES DONNÉES

Cinq grands principes directeurs guident la pratique de la sécurité des données au CIUSSS de l'Estrie – CHUS. Ils sont :

1. **La sécurité des données est une obligation de moyens**. Les mécanismes organisationnels, technologiques, humains et juridiques qui visent à assurer la sécurité des données sont mis en place, évalués régulièrement et font l'objet d'une reddition de compte;
2. **La sécurité des données repose sur un cadre légal et réglementaire** que l'établissement applique en mettant en place la gouvernance et les mécanismes de gestion nécessaires pour protéger les données, en conformité avec les règles de confidentialité et de respect de la vie privée, les ententes contractuelles et les exigences d'affaires de l'organisation;
3. **La sécurité des données est assurée tout au long de leur cycle de vie :** 1) au niveau des systèmes d'information qui collectent et hébergent les données, 2) au niveau des outils qui traitent et exploitent les données et 3) au niveau des réseaux sur lesquels transitent les données;
4. **Les données sont disponibles en temps opportun aux utilisateurs autorisés**, en conservant leur intégrité et en respectant leur confidentialité tout au long de leur cycle de vie. Les risques relatifs aux données sont identifiés, contrôlés et gérés de manière coordonnée dans l'ensemble de la communauté du CIUSSS;
5. **Les utilisateurs de données sont imputables.** Ils sont formés à la sécurité des données, ils connaissent les différentes politiques, règlements et procédures entourant la sécurité des données et y adhèrent. Ils sont informés des mises à jour des documents concernant la sécurité des données. Ils accèdent aux jeux de données qui leur sont alloués selon les droits qui leur sont accordés. Ils manipulent et analysent les données de manière éthique dans un environnement de confiance qui les protège.

OBLIGATIONS DE L'ÉTABLISSEMENT

Les obligations de l'établissement en matière de sécurité des données sont celles en vigueur en sécurité de l'information, appliquées aux banques de données et à leur contenu, ainsi qu'aux systèmes physiques et logiques d'exploitation des données, notamment :

- Se conformer au cadre légal et réglementaire de la sécurité de l'information;

- Inclure les données dans la politique, le cadre de gestion et l'éventuel cadre normatif en sécurité de l'information de l'établissement;
- Inclure les données dans le programme de formation en sécurité de l'information ainsi que dans les activités de sensibilisation en matière de sécurité de l'information;
- Appliquer les mécanismes de sécurité de l'information aux données et en assurer le suivi;
- Assurer la gestion des risques de sécurité des données et mettre en place les mécanismes de mitigation;
- Documenter les incidents de sécurité liés aux données, et mettre en place les mécanismes assurant la non-récurrence et en évaluer l'efficacité;
- Inclure les données dans la reddition de compte faite auprès de la direction responsable de la sécurité de l'information.

CONTEXTE LÉGAL ET RÉGLEMENTAIRE DE LA SÉCURITÉ DE L'INFORMATION

Le contexte légal et réglementaire qui s'applique à la sécurité de l'information s'applique aussi à la sécurité des données. Pour des fins de compréhension, ce contexte est divisé en quatre groupes de lois et règles.

Groupe 1 : Les lois

Le ministère de la Santé et des services sociaux (MSSS) et son réseau sont assujettis au cadre légal et réglementaire présenté à l'annexe F. À ce cadre, s'ajoute :

1. La Loi sur la protection des renseignements personnels dans le secteur privé, dans les situations de partage de données de l'établissement avec le secteur privé œuvrant en innovation et avec d'autres partenaires privés,

et

2. Le projet de loi 3 (***Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives***) qui vise à rendre plus fluide le partage des données de santé ou de services sociaux tout en permettant aux usagers d'assurer un meilleur contrôle des informations relatives à leur dossier médical.

Groupe 2 : Les exigences émanant du ministère de la cybersécurité et du numérique (MCN) et du Secrétariat du Conseil du trésor (SCT)

Les dispositions légales et administratives en sécurité de l'information, publiées par le MCN, et la directive gouvernementale sur la sécurité de l'information, publiée par le SCT, confèrent à l'ensemble des ministères et organismes qui relèvent du Dirigeant principal de l'information (DPI) du gouvernement du Québec de nouvelles responsabilités en matière de sécurité de l'information.

Groupe 3 : Les règles émises par le ministère de la Santé et des services sociaux (MSSS)

Le MSSS a émis plusieurs règles particulières, notamment la *Règle particulière sur la sécurité organisationnelle*[15], les attentes du Dirigeant réseau de l'information (DRI) et les exigences touchant les Centres de traitement informatique (CTI) du réseau de la santé et des services sociaux (RSSS).

Groupe 4 : Les politiques, règles, exigences, directives et normes émises par le CIUSSS de l'Estrie - CHUS

[15] Gestion des ressources informationnelles, Vol. 04, Ch. 02, Suj. 01, Doc. 02, MSSS, 2017-06-27.

Le CIUSSS de l'Estrie – CHUS a mis en place une Politique, un Cadre de gestion et un Cadre normatif en sécurité de l'information qui dictent les règles, exigences, directives et normes à respecter en matière de sécurité de l'information et des données.

MÉCANISMES DE GESTION DE LA SÉCURITÉ DES DONNÉES

Les mécanismes de gestion de la sécurité traités dans ce chapitre sont tirés de la définition de la sécurité de l'information publiée par le Secrétariat du Conseil du trésor (SCT) du gouvernement du Québec **:**

« La sécurité de l'information repose sur trois éléments fondamentaux : la disponibilité, l'intégrité et la confidentialité de l'information. Ces éléments sont d'autant plus importants qu'ils sont à la base du respect de la vie privée et de la protection des renseignements personnels. On définit également la sécurité de l'information comme étant l'ensemble des moyens organisationnels, technologiques, humains et juridiques permettant d'assurer la réalisation des objectifs répondant à l'exigence de respecter chacun de ces éléments fondamentaux. »

L'ajout des notions « *Sensibilité des données* », « *Authentification des utilisateurs* », « *Non-répudiation à l'utilisation des données* » et « *Irrévocabilité des certificats d'accès* » aux trois éléments de la définition vient préciser davantage les moyens d'assurer la sécurité des données. [16]

Les mécanismes de gestion de la sécurité des données impliquent à la fois les ressources humaines et les ressources informationnelles. La présente section se concentre sur trois des quatre mécanismes de la définition du SCT, soit :

- Les mécanismes organisationnels;
- Les mécanismes liés aux technologies;
- Les mécanismes liés aux facteurs humains.

Les mécanismes juridiques correspondent au respect du cadre légal et réglementaire traité plus haut. Chaque mécanisme possède ses propres règles qui, lorsque mises en commun, créent un modèle complet de gestion de la sécurité des données.

MÉCANISMES ORGANISATIONNELS

Les mécanismes organisationnels couvrent diverses mesures que l'établissement doit prendre pour assurer la sécurité des données qu'il gère. Deux catégories sont d'intérêt pour les données :

- La gestion des vulnérabilités et
- La gestion des identités et des accès.

Gestion des vulnérabilités

Les vulnérabilités de l'environnement informationnel de l'établissement ont un impact sur la sécurité et peuvent nuire à l'intégrité des données. Il existe plusieurs types de vulnérabilités, notamment :

[16] La non-répudiation est l'une des propriétés de l'information considérées en cybersécurité. Elle consiste en l'assurance qu'une action sur la donnée réalisée au nom d'un utilisateur, après authentification, ne saurait être répudiée par ce dernier.

- Les vulnérabilités qui touchent **les systèmes et leur environnement** (configuration architecturale, design, paramétrage, connectivité, etc.);
- Les vulnérabilités qui concernent **l'accès et l'utilisation des données**;
- Les vulnérabilités qui touchent **la gestion des données**.

Le CIUSSS de l'Estrie – CHUS, dans son programme de gestion de la sécurité de l'information, a mis en place des mécanismes de gestion des vulnérabilités de son écosystème informationnel transactionnel. L'ajout de quelques mécanismes liés aux données viendrait compléter ce programme, dont :

- Les mécanismes de gestion des vulnérabilités des banques de données et des systèmes physiques et logiques d'exploitation des données;
- Les mécanismes de surveillance des accès, des utilisations et de protection des données, notamment :
    - Les mécanismes d'accès aux banques, systèmes de stockage des données, pipelines de données et jeux de données, selon les conditions d'autorisations et les privilèges accordés aux utilisateurs;
    - Les mécanismes de chiffrement des données, incluant la gestion des clés de chiffrement;
    - Les mécanismes de traçabilité des données tout au long de leur cycle de vie, par le biais de la gestion des métadonnées.

Audits de sécurité des données et registre

Les audits de sécurité de l'information ont pour but d'évaluer l'efficacité des mesures de protection techniques et opérationnelles de l'information mises en place dans l'établissement. Le SCT a publié en 2016 un ***Guide d'audit de la sécurité de l'information*** visant à couvrir les étapes de réalisation d'un audit de sécurité de l'information.

Au CIUSSS de l'Estrie – CHUS, de nombreux systèmes transactionnels et processus de gestion de ces systèmes et contenus font partie d'un Programme d'audit. Ce programme serait complété par :

- L'ajout des équipes responsables des banques de données et des systèmes d'exploitation des données de l'établissement à la liste des détenteurs de l'information responsables de la gestion de ces systèmes dans l'établissement;
- L'ajout des banques de données et des systèmes physiques et logiques d'exploitation des données à la liste des systèmes d'information audités;
- L'ajout des mécanismes d'accès, de protection et de traçabilité des données à la liste des processus audités.

La collaboration des équipes responsables des banques de données, notamment l'équipe CPSS et le Centre DORISE, est requise à l'opérationnalisation des audits de sécurité des données.

Si le CIUSSS de l'Estrie – CHUS ne possède pas de registre des audits de sécurité de l'information, il est suggéré d'en créer un et d'y ajouter les métadonnées reliées 1) aux audits eux-mêmes (date, heure, système audité, etc.), 2) aux rapports d'audits (date de publication, titre, auteur, collaborateurs, etc.) et 3) aux rapports de suivi (date de publication, titre, auteur, collaborateurs, etc.). Par contre, si un registre existe, il est suggéré d'y ajouter ces mêmes métadonnées. Elles documentent les actions prises pour évaluer l'efficacité des mesures adoptées pour protéger les données et les systèmes d'information de l'établissement.

Gestion des identités et des accès (GIA)

La règle particulière sur la sécurité organisationnelle du *Cadre normatif de la sécurité de l'information du Réseau*, développé par le MSSS, comprend la gestion des identités des personnes (ou authentification des personnes) qui accèdent aux actifs informationnels ainsi que le contrôle des accès auxdits actifs.

Des mécanismes de gestion des identités et des accès aux systèmes d'information transactionnels (SIT) sont déjà en opération dans l'établissement[17]. L'ajout des banques de données et systèmes d'exploitation des données à la liste des SIT, ainsi que l'ajout des mécanismes plus spécifiques aux modalités d'accès aux données des banques de données, complèteraient l'éventail des systèmes et mécanismes de gestion des identités et des accès à considérer dans le Programme de gestion de la sécurité de l'information de l'établissement.

Mécanismes à ajouter concernant la gestion des identités

Des mécanismes internes de gestion des identités sont déjà en vigueur dans l'établissement. À ces mécanismes, les nouveaux mécanismes à ajouter sont :

- Un dispositif d'identification qui confirme sans équivoque l'identité d'un utilisateur de données, qu'il soit interne ou externe à l'organisation, et qui journalise les droits d'accès aux données de l'établissement qui lui sont accordés;
- Un mécanisme qui informe les utilisateurs de données dûment identifiés quant à leurs responsabilités à l'égard de leur dispositif d'identification;
- Un mécanisme permettant de se prémunir contre le refus d'un utilisateur de reconnaître ses responsabilités à l'égard de son dispositif d'identification. Par exemple, le dispositif n'est pas alloué à l'utilisateur qui n'accepte pas ses responsabilités;
- Un mécanisme permettant de se prémunir contre le partage d'identités, de détecter les identités partagées et d'imposer des retraits d'accès et autres conséquences;
- Un registre des utilisateurs de données ou un annuaire d'utilisateurs des données ou tout autre mécanisme semblable.

Mécanismes à ajouter concernant la gestion des accès

L'établissement choisit de gérer les accès aux données sur la base de rôles attribués. Ce modèle est connu sous le nom de *The principle of least privilege*. Il s'agit d'un modèle dans lequel un utilisateur se voit accorder le niveau d'accès requis comprenant le minimum de privilèges nécessaires pour accomplir son travail. Il est tout indiqué que le registre des utilisateurs de données inclue les privilèges accordés aux utilisateurs.

Puisque la diversité des demandes d'accès aux données augmente, il est proposé de complexifier le mécanisme d'accès en permettant la gestion granulaire des accès. Cette dernière ajoute aux conditions d'accès de base des conditions supplémentaires, comme limiter la période d'accès, limiter l'accès à certaines catégories de données, identifier les lieux d'accès et autres fonctionnalités.

[17] Conformément à la directive *(CTI) Directive sur la sécurité 04 02 02.*

MÉCANISMES LIÉS AUX TECHNOLOGIES

Cote DIC de classement des banques et des systèmes d'exploitation des données

Plusieurs normes internationales[18] sont déjà utilisées en sécurité de l'information. Au Québec, le SCT a publié un modèle d'évaluation du niveau de criticité des actifs informationnels, assurant la disponibilité, l'intégrité et la confidentialité (DIC) des contenus de ces systèmes d'information. Il s'agit du processus de catégorisation DIC que les établissements de santé appliquent à leurs actifs informationnels.[19] L'annexe F présente la grille de priorisation.

Le CIUSSS de l'Estrie – CHUS applique aussi cette catégorisation à ses banques de données et systèmes d'exploitation des données, que ces derniers soient physiques ou logiques. Selon le niveau DIC qui leur est assigné, des moyens sont mis en place pour sécuriser leur contenu.

> *Disponibilité des données (D)*

La disponibilité garantit que les utilisateurs autorisés ont un accès rapide, au bon moment et ininterrompu aux données contenues dans une banque ou un système d'exploitation de données. Pour ce faire, tout en réduisant les risques inhérents, l'établissement doit minimalement se doter de moyens pour :

- Éviter les pertes de données;
- Récupérer les données en cas de défectuosité des infrastructures d'hébergement et d'exploitation des données.

> *Intégrité des données (I)*

L'intégrité garantit que, lors de leur traitement, de leur hébergement ou de leur transmission, les données n'ont subi aucune altération ou destruction volontaire ou accidentelle, et ont conservé un format permettant leur utilisation[20].

Pour préserver l'intégrité des données, l'établissement doit minimalement prendre les moyens nécessaires pour :

- Empêcher toute modification des données par des utilisateurs non autorisés;
- Empêcher toute modification non autorisée ou involontaire des données par des utilisateurs autorisés;
- Garantir l'authenticité et l'intégralité des données au moyen de processus standardisés tels que le contrôle des erreurs et la validation des données.

Une application de vérification de type *File integrity manager* (FIM) permet de détecter toutes modifications apportées aux fichiers des systèmes afin de déterminer s'ils ont été modifiés ou non après leur création, hébergement, transmission ou toute autre étape de leur cycle de vie.

---

[18] Norme ISO 27001, ISO 27002, ISO 27018 : une extension à l'infonuagique, et ISO 27701 : une extension à la gestion de la confidentialité, le NIST (*National Institute of Standards and Technology*, le COBIT (*Control OBjectives for Information and related Technology*) et le GTAG (*Global Technology Audit Guide*).

[19] Ce processus est décrit en détail dans le *Guide de catégorisation de l'information version 1.5., MSSS, 2016.*

[20] Tiré de la définition de l'intégrité citée dans l'encyclopédie libre Wikipédia.

> *Confidentialité (C)*

La confidentialité limite l'accès aux données seulement aux personnes ou entités désignées et autorisées par la loi et les règles internes de l'établissement. Elle empêche toute intrusion, accès, copie, téléchargement non autorisé ou autre à des données qui ont préalablement été qualifiées de sensibles et confidentielles.

Pour préserver la confidentialité des données, l'établissement doit minimalement prendre les moyens nécessaires pour :

- Faire signer à tout utilisateur de données un formulaire de consentement à la confidentialité;
- Journaliser les accès et privilèges octroyés aux utilisateurs et réaliser des audits régulièrement;
- Dépersonnaliser les données confidentielles par chiffrement, anonymisation ou agrégation, tant les données en mouvement que les données en repos, avant d'en permettre l'accès en mode libre-service, et ce, en conformité avec les lois et les règlements internes de l'établissement;
- Assurer une gestion rigoureuse des accès accordés, limités, refusés ou retirés et les journaliser;
- Limiter/refuser l'accès à certains types de données afin d'assurer la protection de la vie privée.

Dimension Sensibilité (S) des données

La dimension sensibilité réfère au caractère sensible des données et informations utilisées, et à l'impact potentiel sur le respect de la vie privée des personnes concernées. Cette dimension est considérée dans l'évaluation des facteurs relatifs à la vie privée (EFVP) et dans l'évaluation du préjudice causé par un incident de confidentialité.

En vertu de la *Loi 25*, « un renseignement personnel est sensible lorsque par sa nature notamment médicale, biométrique ou autrement intime ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée »[21].

Cette même notion revient dans le *Projet de loi 3* qui désigne comme confidentiels les renseignements de santé ou de services sociaux. Leur nature médicale fait d'eux des renseignements sensibles.

Tant dans la *Loi 25* que dans le *Projet de loi 3* **:**

- L'évaluation des facteurs relatifs à la vie privée (EFVP) doit être proportionnée à la sensibilité des renseignements concernés *;*
- L'évaluation du risque qu'un préjudice soit causé à une personne dont un renseignement est concerné par un incident de confidentialité doit considérer notamment la sensibilité du renseignement concerné *;*

L'application de ces articles de loi aux données de l'établissement implique que ce dernier doit minimalement :

[21] Loi 25, art.12, alinéa 3.

- Se doter de critères de classification du niveau de sensibilité d'une donnée et coder ce niveau ;
- Se doter d'un outil de marquage (Tag) des données stockées dans les banques de données qui attribue le code correspondant au niveau de sensibilité désigné.

Non répudiation et irrévocabilité des accès

L'ajout des notions de **non-répudiation à l'utilisation des données** et **irrévocabilité des certificats d'accès** à la catégorisation DIC vient ajouter des moyens d'assurer une meilleure sécurité des données.

L'établissement choisit les moyens informatiques et/ou organisationnels d'assurer qu'une opération effectuée sur les données a bel et bien été effectuée par un utilisateur dûment authentifié. Il choisit aussi les moyens informatiques et/ou organisationnels d'assurer que l'utilisateur ne peut nier qu'il a effectué ladite opération sur les données.

Il revient aux gestionnaires responsables des systèmes transactionnels et des banques de données et au Centre DORISE, de se concerter pour déterminer les moyens à adopter.

Particularités de l'infonuagique

Lorsque les données et les services se transportent dans les nuages informatiques et que des étapes de leur traitement pourraient donner lieu à des hébergements dans différents lieux, dans une même juridiction ou dans différentes juridictions, il pourrait s'avérer difficile de prévoir quelles lois et réglementations leur seraient applicables.

L'intégration de l'infonuagique dans l'architecture technologique d'un établissement nécessite une réflexion quant à la nature des données et des traitements qu'il est acceptable de rendre disponibles via cette technologie. Cette réflexion se base sur plusieurs éléments, notamment :

1. Sur les informations du Guide de l'infonuagique- Volume 1 – Notions fondamentales, publié par le SCT;
2. Sur certaines règles dictées par le MSSS[22] aux établissements de santé et de services sociaux, telles que :
    - Les données cliniques, médicales ou sociales des patients et les données qui affichent une confidentialité de niveau 4 demeurent au Canada, à moins d'un avis juridique contraire;
    - L'organisme s'assure que le service infonuagique respecte le cadre législatif en lien avec les données de santé, notamment en ce qui a trait à la législation sur la protection des renseignements personnels et des renseignements de santé ou de services sociaux.
3. Sur le respect du cadre législatif québécois, notamment la *Loi 25* et le *Projet de loi 3* qui prévoient que l'établissement doit, avant 1) de communiquer des renseignements personnels ou des renseignements de santé ou de services sociaux à l'extérieur du Québec, ou 2) de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de les détenir, de les utiliser ou de les communiquer pour son compte, s'assurer que lesdits renseignements bénéficieront d'une **protection adéquate,** notamment au regard des principes de protection

[22] *Recours aux services infonuagiques Version : 1.0, MSSS, 2017-08-25*

des renseignements personnels ou de santé ou de services sociaux généralement reconnus.[23] Ces exigences législatives s'appliquent à tout lieu d'hébergement des données confidentielles, dont notamment les sites de relève, ainsi qu'aux sous-contractants du prestataire de services, le cas échéant.

Bien que cette même mesure ne touche que les renseignements personnels et de santé ou de services sociaux, celle-ci prévoit également des obligations de confidentialité pour des données autres que ces renseignements. Ainsi, une bonne pratique serait d'étendre cette mesure de protection à l'ensemble des données confidentielles[24].

4. Sur l'observation au minimum des trois règles suivantes :

   Règle 1 : L'adoption de l'infonuagique pour des projets touchant des données sensibles ou des systèmes de missions essentielles fait partie d'une politique claire et entérinée par la haute direction de l'établissement;

   Règle 2 : Le fournisseur d'infonuagique choisi est accrédité par Infrastructure Technologique Québec (ITQ) en vertu de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LGGRI);

   Règle 3 : Le cadre de gestion des risques de l'établissement et la grille d'analyse utilisés pour la catégorisation des actifs informationnels sont adaptés aux caractéristiques de l'infonuagique.

MÉCANISMES LIÉS AUX FACTEURS HUMAINS

Programme de sensibilisation et de formation à la sécurité des données

Du fait que les attaques exploitant le facteur humain sont de plus en plus présentes, il importe de promouvoir au sein des utilisateurs de données de la communauté du CIUSSS de l'Estrie-CHUS une culture de sécurité, de gestion des risques liés aux données, de confidentialité des données et de respect de la vie privée.

Ainsi, les concepts de sécurité liés à l'utilisation des données pour des fins autres que celles pour lesquelles les données ont été collectées, font partie du Programme continu de formation et de sensibilisation du personnel du CIUSSS de l'Estrie – CHUS en matière de sécurité et de respect de la confidentialité.

Ce programme, tel que préconisé par le *Guide de sensibilisation à la sécurité de l'information-PR-070* du SCT, s'adresse à l'ensemble de la communauté du CIUSSS de l'Estrie-CHUS utilisant ou ayant accès à des actifs informationnels peu importe le statut (employé, étudiant, contractuel, chercheur ou autre). Il doit minimalement comprendre :

- Les principes de dépersonnalisation, d'anonymisation et de chiffrement des données ainsi que leurs bénéfices;

[23] Loi 25; art. 27 et PL 3, art 39.

[24] Un renseignement autrement confidentiel est un renseignement qui peut porter préjudice à une organisation, à une entreprise, une association, à un regroupement d'individus ou autre.

- L'importance de travailler dans un environnement de confiance et sécuritaire;
- Les mécanismes de gestion proactive de la sécurité tout au long du cycle de vie des données;
- La gestion des identités et des accès, ainsi que la détection rapide des problématiques.

GESTION DES RISQUES DE SÉCURITÉ DES DONNÉES

Conformément à la *Loi sur les services de santé et les services sociaux* (LSSSS), le CIUSSS de l'Estrie – CHUS a publié le 4 avril 2018 sa *Politique sur la gestion intégrée des risques*[25] et mis en place son *Programme de gestion intégrée des risques* applicable à l'ensemble des installations de l'établissement.

Les risques liés aux données s'ajoutent aux « risques technologiques et informationnels » du programme. Les fiches 44 et 45 du programme ont été modifiées. À la fiche 44 s'ajoutent les risques liés à la désuétude et à la consolidation des technologies de l'information soutenant la gestion des données, et à la fiche 45 s'ajoutent les risques concernant l'atteinte à la disponibilité, l'intégrité, la confidentialité des données et l'atteinte à la vie privée.

La pratique de la sécurité des données se base sur la réalisation des principales étapes du modèle présenté à la Figure 12. Ce modèle s'harmonise avec les bonnes pratiques en sécurité de l'information appliquées au CIUSSS de l'Estrie – CHUS.

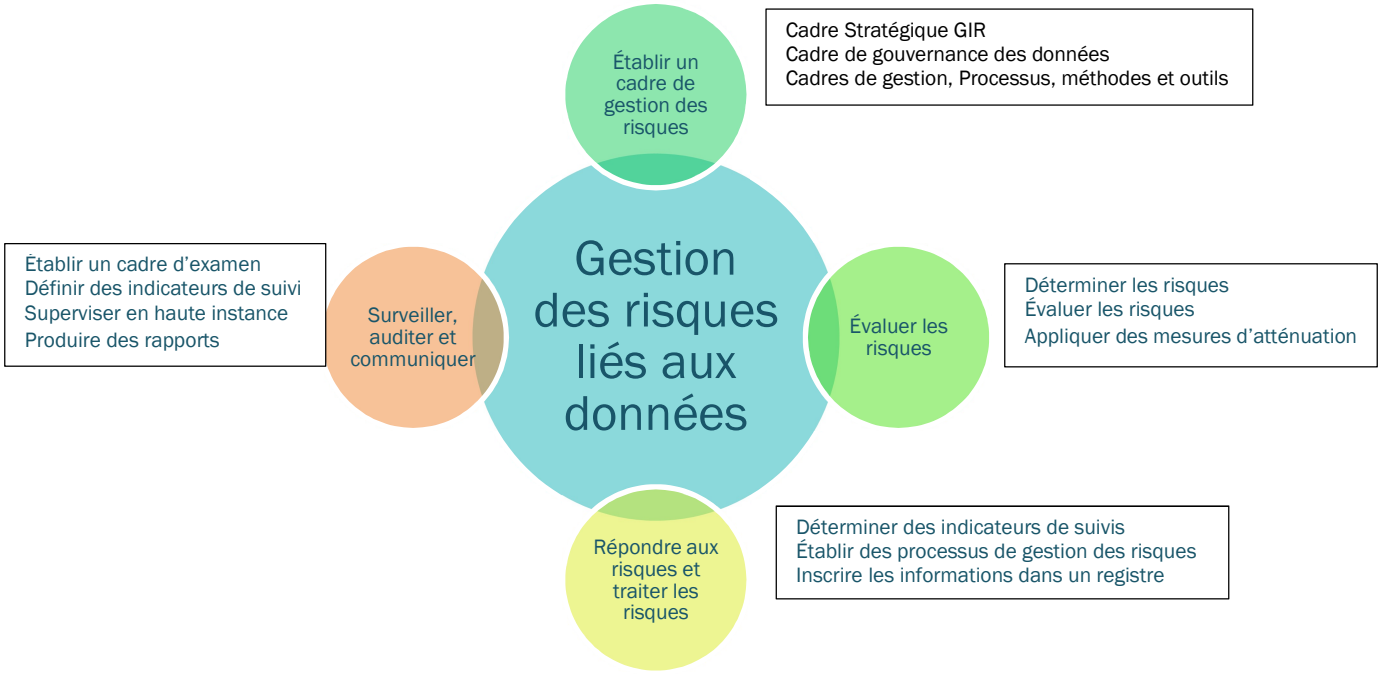


Figure 12 – Modèle de gestion des risques liés aux données.

[25] Politique E000–POL-03.

Le modèle comprend 4 étapes importantes : (1) Établir un cadre de référence de gestion des risques, (2) Évaluer les risques, (3) Répondre aux risques et traiter les risques et (4) Surveiller, auditer et communiquer.

Selon ces bonnes pratiques, les mesures de sécurité sont proportionnelles à la valeur des informations à protéger. Elles sont établies en fonction du niveau de risques, de leur probabilité d'occurrence et de leurs conséquences sur les activités de l'établissement. Ces mesures s'appliquent aussi aux données stockées dans les banques. Elles sont utilisées dans le modèle présenté ici comme mesures d'atténuation des risques.

Les risques de sécurité de l'information sont déjà considérés dans le processus de gestion intégrée des risques de sécurité des ressources informationnelles de l'établissement. Dans la gestion des risques en lien avec les données stockées dans les banques, les éléments suivants sont particulièrement importants à considérer.

Quant aux **risques** :

- L'utilisation inappropriée des équipements et outils d'exploitation des données;
- L'atteinte à la disponibilité et à l'intégrité des données en mouvement et au repos;
- Les accès non autorisés aux données confidentielles;
- Les bris de confidentialité des usagers et du personnel;
- La diffusion non autorisée de données confidentielles;
- L'envoi de jeux de données ou de fichiers de données à la mauvaise personne.

Quant aux **activités du processus de gestion intégrée des risques** :

- Suivre les règles de sécurité de l'information dans la conception des systèmes d'information, des banques de données et des pipelines de données ainsi que dans leur fonctionnement et leur interopérabilité lorsqu'intégrés dans un écosystème de gestion des données ;
- Établir un plan de relève/recouvrement des banques de données et pipelines de données et le rendre disponible ;
- Rédiger un document de priorisation des opérations et fonctions essentielles à restaurer en cas de désastre;
- Établir un plan d'amélioration continue de la sécurité des banques, pipelines et outils d'exploitation des données et le rendre disponible ;
- Rédiger et rendre disponible un document décrivant les rôles et responsabilités des personnes impliquées dans la gestion de la sécurité des données et l'annexer au Cadre de gouvernance des données ;
- Établir un inventaire des systèmes sources, banques de données, systèmes d'exploitation des données et pipelines de données permettant d'obtenir une vue complète de l'environnement des données de l'établissement.

INCIDENTS DE SÉCURITÉ DES DONNÉES

La DRIT et la Direction adjointe des mesures d'urgence, de la sécurité civile et des enjeux organisationnels collaborent déjà entre elles et avec les autres directions concernées pour mettre en place un processus de gestion des incidents relatifs à la sécurité des systèmes et de l'information. Les incidents de sécurité des systèmes et de l'information sont consignés dans le registre des incidents de sécurité de l'information. Ce même registre consigne les incidents de sécurité des

données et les incidents de confidentialité de l'information et des données. La section du registre consignant les incidents de confidentialité est conforme aux exigences de la ***Loi 25***. Le processus interne de déclaration d'un incident de sécurité de l'information est appliqué aussi aux incidents de sécurité des données et aux incidents de confidentialité.

GOUVERNANCE DE LA SÉCURITÉ DES DONNÉES

PRÉSIDENCE-DIRECTION GÉNÉRALE ADJOINTE

Relevant du Président-directeur général (PDG) de l'établissement, la responsabilité de la sécurité de l'information est déléguée à la Présidence-direction générale adjointe de l'établissement. Cette dernière soutient la gouvernance de la gestion des données décrite au chapitre 3. Le président-directeur général adjoint préside le *Comité directeur de la gestion des données*.

COLLABORATEURS À LA GESTION DE LA SÉCURITÉ DES DONNÉES

En plus des divers comités associés à cette gouvernance, plusieurs partenaires collaborent à la gestion de la sécurité des données :

- **Le chef de la sécurité de l'information organisationnelle** (CSIO) de l'établissement qui s'assure de la sécurité des systèmes et de leur contenu;
- **Le groupe de soutien à la recherche CRED** qui assure la sécurité des environnements utilisés en recherche dont certains sont la propriété du CIUSSS de l'Estrie – CHUS (ex : Vision C+);
- **Le responsable de la protection des renseignements personnels** qui assure la protection des renseignements personnels. Cette responsabilité est assumée par les chefs et la coordonnatrice des archives;
- **Le responsable de l'accès aux documents** qui assure la confidentialité des documents de l'établissement et qui gère l'accès à ces documents. Cette responsabilité est assumée par les chefs et la coordonnatrice des archives pour le volet clinique et par les services juridiques pour le volet administratif;
- **Le responsable de la gestion intégrée des risques** qui voit à la bonne marche du Programme de gestion intégrée des risques de l'établissement;
- **Le Centre DORISE** qui joue le rôle d'intendant principal de la gestion des données. Il applique les règles et procédures liées à la sécurité des données contenues dans les banques et bases de données ainsi que dans les systèmes d'information sous sa responsabilité;
- **Les détenteurs de données** des différentes directions qui assurent la sécurité des données collectées et stockées dans les systèmes d'information sources dont ils ont la responsabilité;
    - Le détenteur de données est le gestionnaire désigné comme responsable de la gestion du système d'information source localisé dans sa direction et qui collecte des données. Le détenteur de données est habilité à prendre toute décision concernant le niveau fonctionnel du système dont il est responsable en vue d'assurer l'intégrité et la confidentialité de son contenu.
- **Les membres du personnel** du CIUSSS de l'Estrie – CHUS, car la sécurité de l'information est transversale à l'organisation et est l'affaire de tous les membres de la communauté du CIUSSS de l'Estrie-CHUS qui, de près ou de loin, collectent, utilisent ou conservent des données.

AUTRES INSTANCES DE GOUVERNANCE

Les rôles et responsabilités des intervenants déjà impliqués dans la gestion de la sécurité de l'information sont décrits dans la Politique de sécurité de l'information et dans son Cadre de gestion. Leurs compétences font en sorte qu'ils peuvent étendre leur rôle à la sécurité des données.

Comité de coordination de la sécurité, de l'accès et de la protection des renseignements personnels

Au sein de la gouvernance des données, il revient au *Comité de coordination de la sécurité, de l'accès et de la protection des renseignements personnels*, en collaboration avec les partenaires, de coordonner la mise en œuvre et le suivi des divers mécanismes assurant la sécurité des données ainsi que la gestion des risques qui y sont associés. Ce comité assume les responsabilités légales du *Comité sur la sécurité de l'information*, du *Comité sur la gestion des accès* et du *Comité sur la protection des renseignements personnels* exigé par la *Loi 25*.

Le Comité assume la responsabilité de la qualification du niveau de sensibilité des données dans les systèmes d'information de l'établissement. En fonction des résultats d'une analyse de sensibilité et d'une analyse d'impact, il choisit une méthode de marquage (Tag) des données sensibles.

Centre DORISE et détenteurs de données

Le Centre DORISE et les détenteurs de données sont les instances opérationnelles qui mettent en œuvre les activités de sécurité des données des banques et des systèmes d'information dont ils ont la responsabilité, notamment :

- Le marquage des données sensibles dans les systèmes d'information et banques dont ils sont responsables en utilisant la méthode choisie par le *Comité de coordination de la sécurité, de la gestion de l'accès et de la protection des renseignements personnels*;
- L'inscription du niveau de sensibilité des données au registre de catégorisation des actifs informationnels de l'établissement. Cette information permet la sélection des mécanismes de traitement propices à la protection des données lors de la création des jeux de données.

Service de sécurité de l'information du CIUSSS de l'Estrie – CHUS

Aux obligations qui incombent au Service de sécurité de l'information s'ajoutent les quelques responsabilités suivantes :

- Collaborer à la classification des banques et systèmes d'exploitation des données par une analyse DIC;
- Créer une fiche de risques de sécurité des données (classification, tolérance et mitigation des risques) ou, s'il en existe une sur les risques de sécurité de l'information, y intégrer les risques de sécurité des données;
- Collaborer avec le responsable de la protection des renseignements personnels, les détenteurs de données et le Centre DORISE à l'évaluation des facteurs de risques liés à la vie privée devant être réalisée pour tout projet de l'établissement qui collecte, utilise, conserve, communique ou détruit des données;

- Collaborer à l'élaboration d'une entente de confidentialité soulignant l'engagement de tout utilisateur de données à assurer la confidentialité des données;
- S'assurer de la responsabilité des fournisseurs de systèmes d'information en cas d'incidents de sécurité des données ;
- Contribuer à l'analyse de préjudice des systèmes que l'établissement souhaite externaliser en infonuagique;
- Élaborer les règles de sécurité liées à la migration des données vers l'infonuagique s'il y a lieu;
- Mettre en place un registre des vérifications et des mécanismes d'évaluation et de surveillance des risques de sécurité des données.

CHAPITRE 3.3 – ACCÈS AUX DONNÉES

DÉFINITIONS

La gestion des accès est l'un des principaux mécanismes de sécurité qui assurent la confidentialité de l'information. Elle ne rend l'information disponible qu'aux personnes désignées et autorisées. Cette gestion comprend aussi l'authentification des personnes autorisées à accéder à l'information. La journalisation de ces deux mécanismes conduit à la non-répudiation des actions qu'un utilisateur effectue sur les données. Ces termes sont définis dans le chapitre 1, alors que la présente section définit des termes spécifiques à la gestion de l'accès.

Accès à l'information : Possibilité de consulter un document, en format papier ou électronique, ou d'obtenir l'information contenue dans celui-ci[26]. La demande d'accès est formulée au responsable de l'accès à l'information et de la PRP du CIUSSS de l'Estrie – CHUS. Le processus à suivre est déjà en place et pleinement fonctionnel.

Accès aux données : Possibilité de consulter une base de données ou d'obtenir des données contenues dans celle-ci[27]. Il existe deux moyens d'obtenir des données stockées dans les banques de données de l'établissement. Le premier est d'effectuer une requête d'accès directement aux directions détentrices de données. C'est le cas entre autres pour les chercheurs, les gestionnaires et les intervenants cliniques de l'établissement. Le second est d'effectuer une requête au responsable de l'accès à l'information et de la PRP de l'établissement et de suivre le processus d'accès à l'information. C'est le cas entre autres par exemple pour les journalistes et le Protecteur du citoyen.

Accès aux systèmes d'information : Possibilité de consulter de l'information électronique contenue dans un système informatique, et organisée sous une forme compréhensible (statistiques, graphiques, rapports) en réponse à une requête.

Les systèmes d'information (SI) sont généralement dédiés à des secteurs d'activités bien précis. Par exemple, on retrouve des SI de gestion, tels SIRH[28] et SGDT[29], qui produisent des budgets, des comptes rendus de projet et des rapports de ressources, entre autres, tout comme on peut retrouver des systèmes d'information clinique, tels Ariane, OACIS, Cristal Net, EPIC et autres, qui produisent des fiches et rapports cliniques utiles aux intervenants dans la gestion des soins qu'ils dispensent au quotidien.

PRINCIPES DIRECTEURS

1. Les données sont accessibles via les directions détentrices de données;

   Plusieurs directions du CIUSSS de l'Estrie – CHUS produisent des données et les rendent disponibles aux utilisateurs. , Le Centre DORISE de la DQEPP exploite les données pour soutenir la recherche et pour élaborer des tableaux de bord et des rapports de gestion. Ce centre est un point d'accès important aux données.

   Toute demande d'accès est adressée à la direction détentrice de données ou au Centre DORISE, selon les besoins.

[26] Source : Portail Québec

[27] Inspiré de Portail Québec

[28] Système d'information ressource humaine.

[29] Système de gestion de données techniques.

2. L'accès aux données est limité dans le temps ;

   La durée d'accès est évaluée selon la nature de la demande (projet de recherche, tableau de bord périodique, rapport de gestion, autre) et selon le statut du demandeur dans l'établissement (chercheur, gestionnaire, clinicien, professionnel, autre).

3. Seules les données pertinentes sont rendues accessibles;

   Les données pertinentes sont celles qui permettent de répondre directement aux besoins spécifiques des utilisateurs identifiés dans leur demande d'accès.

4. L'accès aux données confidentielles n'est possible que sur autorisation préalable;

   L'exploration de données dans des banques ou comptoirs de données contenant des données confidentielles est permise aux personnes autorisées conformément aux processus internes de l'établissement. Ces processus établis pour assurer la confidentialité des renseignements personnels sont appliqués à l'ensemble des données confidentielles de l'établissement.

5. Les utilisateurs de données sont imputables.

   Les utilisateurs de données connaissent les différentes politiques et procédures entourant l'accès aux données et y adhèrent. Ils signent un formulaire d'entente de confidentialité.

OBLIGATIONS DE L'ÉTABLISSEMENT

RÈGLES D'UTILISATION DES DONNÉES

Toute personne autorisée à accéder aux données et à les utiliser a le devoir de respecter certaines règles :

- Elle est responsable de suivre les lois, politiques, procédures et règles associées aux données et s'engage à n'utiliser ces dernières qu'uniquement aux fins pour lesquelles l'accès lui a été accordé;
- Elle adopte un comportement éthique et respecte les règles de confidentialité et de protection des données confidentielles mises en place dans l'établissement;
- Elle est tenue d'utiliser les données aux conditions qui lui sont communiquées;
- Elle a la responsabilité de signaler en toute confidentialité toute utilisation inappropriée ou abusive des données dont elle a connaissance, conformément au processus interne en vigueur dans l'établissement. L'utilisation inappropriée de données confidentielles est traitée comme un incident de confidentialité.

L'ACCÈS AUX RENSEIGNEMENTS PERSONNELS

Les usagers du CIUSSS de l'Estrie – CHUS n'ont accès aux données les concernant que dans le contexte prévu par la *Loi sur les services de santé et les services sociaux* et la *Loi 25,* et en application des politiques, règles et procédures de l'établissement.

Au sens de la *Loi 25*, les **renseignements personnels** nécessitent le consentement exprès[30] de la personne concernée pour être partagés et utilisés sauf exceptions expressément prévues par la Loi[31]. L'article 5 du Projet de loi 3 va dans le même sens avec les **renseignements de santé ou de services sociaux**[32]. Tel que défini au premier chapitre de ce document, la **donnée confidentielle** comprend le renseignement personnel et le renseignement de santé ou de services sociaux.

L'individu qui souhaite utiliser des données confidentielles détenues par le CIUSSS de l'Estrie – CHUS à des fins d'étude, de recherche ou de production de statistiques et qui n'a pas obtenu le consentement exprès de la ou des personnes concernées, doit effectuer une évaluation des facteurs relatifs à la vie privée et soumettre son projet et son évaluation pour approbation, selon les procédures internes de l'établissement. L'évaluation doit tenir compte du risque lié à la confidentialité que comporte le projet en question. Elle doit aussi être proportionnée à la sensibilité des données concernées, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support. Si cela ne suffit pas, une analyse plus poussée peut être exigée par les autorités de l'établissement. Par la suite, conformément aux lois en vigueur, l'individu doit obtenir l'autorisation du Directeur des services professionnels pour accéder auxdites données.

Dans le contexte où les données sont sous une forme ne permettant pas d'identifier la personne concernée, l'accès ou l'utilisation de cette forme de données est privilégié; il ne nécessite alors aucun consentement puisqu'il n'enfreint en rien le respect de la vie privée de la ou des personnes concernées.

Dans le cadre d'un projet de recherche avec cohorte de patients, la collecte de données requiert un consentement explicite, libre et éclairé des personnes acceptant de participer à ce type de projets. Ce volet est traité dans le Cadre réglementaire de la recherche du CIUSSS de l'Estrie – CHUS et ne fait pas partie du présent document.

MÉCANISMES D'ACCÈS AUX DONNÉES

MÉCANISMES D'ACCÈS

Mécanismes d'accès à l'information

Il existe au CIUSSS de l'Estrie – CHUS des mécanismes d'accès à l'information bien rodés pour le public ou pour des instances en autorité comme la Commission d'accès à l'information (CAI), le Curateur public, le Commissaire aux plaintes, le Bureau du coroner, le Protecteur du citoyen ou encore un organisme accréditeur. La personne responsable de l'accès à l'information et de la PRP assure la bonne marche de ces mécanismes. Ces derniers sont utilisés à la suite d'une demande d'accès.

[30] Un consentement doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Il est demandé à chacune de ces fins, en termes simples et clairs. Ce consentement doit être manifesté de façon expresse (par écrit) dès qu'il s'agit d'un renseignement personnel sensible. Un consentement ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé, que cette durée ait été prédéterminée ou non. Lorsque la demande de consentement est faite par écrit, elle doit être présentée distinctement de toute autre information communiquée à la personne concernée.

[31] Les deux exceptions les plus importantes se retrouvent 1) dans les articles 59.5, 125, Loi 25 et 2) dans les articles 59, 59.1, 66, 67, 67.2.1 et 68, Loi 25.

[32] Tout renseignement détenu par un organisme est confidentiel et, sous réserve du consentement exprès de la personne qu'il concerne, il ne peut être utilisé ou communiqué que conformément à la présente loi (art. 5, al.1, PL 3).

Mécanismes d'accès aux données pour la communauté interne de l'établissement

L'utilisation des données par la communauté interne du CIUSSS de l'Estrie – CHUS autres que les chercheurs, comme les gestionnaires, les dispensateurs de soins et services, les professionnels et autres membres du personnel, se centre sur l'élaboration de tableaux de bord et de rapports, entre autres, pour la prise de décision éclairée et l'amélioration continue des services et de la performance.

Deux mécanismes d'accès aux données sont envisagés : l'accès rapide et l'accès régulier.

1. **L'accès rapide** (aussi appelé « Accès en mode libre-service ») : accès simplifié, direct et renouvelable, concédé à la communauté interne du CIUSSS de l'Estrie – CHUS. Les jeux de données sont préconçus et renouvelés automatiquement par une mise à jour incrémentielle[33]. Ils sont rendus disponibles dans un environnement de confiance. L'accès est possible en tout temps aux personnes autorisées.
2. **L'accès régulier** : accès à un ou des jeux de données préparés à la suite d'une demande faite à une direction détentrice de données ou au Centre DORISE de la DQEPP. Les jeux de données sont rendus disponibles aux personnes autorisées dans un environnement de confiance. L'extraction des données sur un autre médium n'est pas prévue, bien que possible, selon la nature de la demande. Les jeux de données à utilisation fréquente ou périodique peuvent être conservés pour un accès rapide.

Des règles de base prévalent pour tout type d'accès comme le montre le tableau de l'Annexe G.

L'analyse des données et la génération des tableaux de bord et des rapports sont réalisées dans un environnement de confiance sécurisé, connecté à un logiciel d'analyse. Les utilisateurs, une fois autorisés, n'ont qu'à se connecter au logiciel d'analyse pour accéder aux jeux de données et procéder aux analyses.

Certaines situations requièrent l'analyse de données comprenant des données confidentielles, soit des renseignements personnels ou des renseignements de santé ou de services sociaux ou encore les deux types de renseignements, par exemple le suivi d'événements touchant des usagers, l'amélioration de la qualité des soins pour un groupe d'usagers, ou le suivi des plaintes. L'accès à ces données n'est autorisé que si l'intervenant démontre que cet accès est nécessaire à l'exercice de sa fonction dans l'établissement. Une fois l'autorisation accordée, l'intervenant n'accède qu'aux données pertinentes à la réalisation de sa fonction dans l'établissement.

[33] La mise à jour incrémentielle d'un jeu de données consiste à renouveler le jeu de données en remplaçant son contenu avec les données les plus récentes. Seules les données qui ont été modifiées dans les systèmes transactionnels depuis la dernière mise à jour du jeu de données sont chargées dans ce dernier.

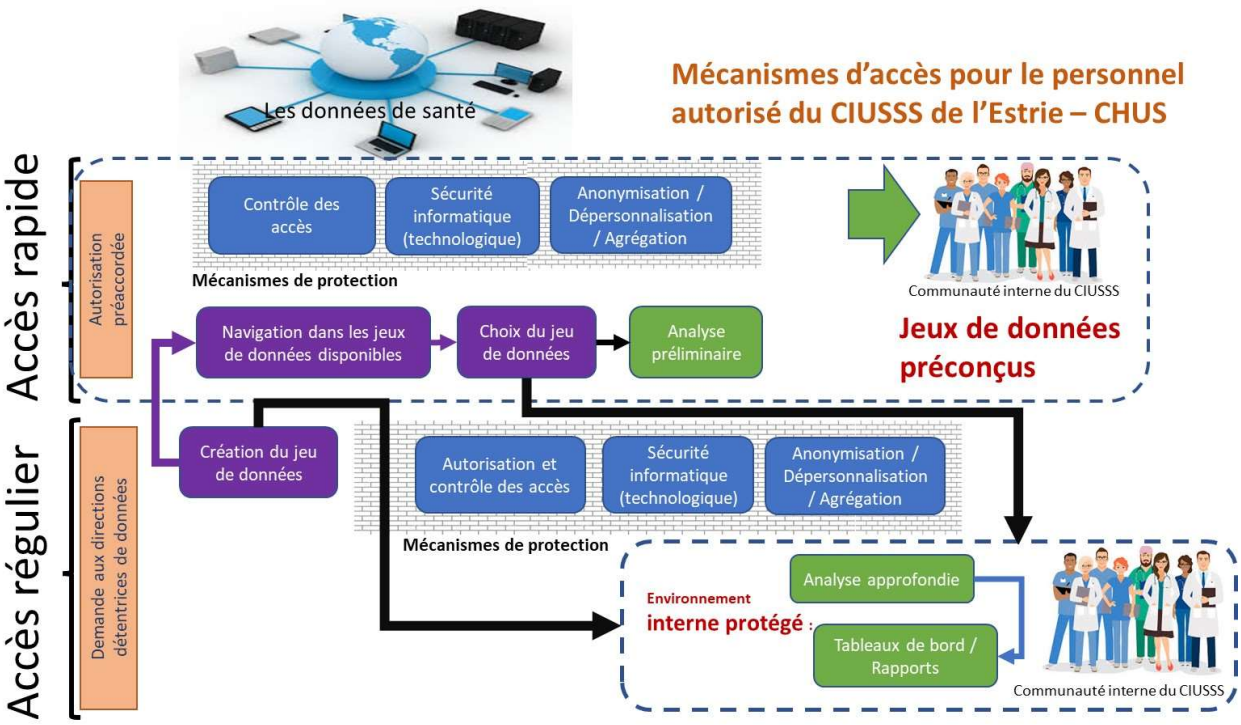


Figure 13 – Mécanismes d'accès aux données par la communauté interne de l'établissement.
Ces mécanismes d'accès particuliers s'appliquent aux membres de la communauté interne du CIUSSS de l'Estrie – CHUS autorisés. Deux types de mécanismes d'accès sont permis : l'accès rapide et l'accès régulier. Les dispositifs de protection forment un « mur de protection » qui vise à protéger les données tout en y permettant l'accès sous réserve de remplir certaines conditions. Les données d'origine sont des données qui peuvent être traitées, mais qui n'ont pas été anonymisées, ni dépersonnalisées ou qui n'ont pas été agrégées. Certaines contiennent des renseignements personnels et/ou des renseignements de santé ou de services sociaux. L'extraction de données n'est pas prévue – les données sont analysées dans un environnement de confiance sécurisé. L'autorisation d'accéder aux données et la gestion des privilèges d'accès sont la responsabilité des directions détentrices des données, qui incluent le Centre DORISE.

Mécanismes d'accès aux données pour la recherche

Catégories de chercheurs

L'accès aux données provenant des systèmes sources de l'établissement n'est autorisé que pour les **chercheurs du CIUSSS de l'Estrie – CHUS**, c'est-à-dire des scientifiques qui ont un statut de chercheur dans le CIUSSS, à qui l'établissement a octroyé des privilèges de recherche dans l'un ses centres de recherche : le Centre de recherche du CHUS (CRCHUS), le Centre de recherche sur le vieillissement (CdRV), l'Institut universitaire de première ligne en santé et services sociaux (IUPLSSS) et l'Unité de recherche du CSSS de la Haute-Yamaska.

Les **chercheurs externes**, c'est-à-dire les chercheurs du secteur public qui n'ont pas de privilèges de recherche au CIUSSS de l'Estrie – CHUS, qui désirent accéder aux données du CIUSSS pour réaliser un projet doivent s'allier avec un chercheur du CIUSSS. Ce dernier est responsable de suivre la démarche d'autorisation du projet et de procéder à la demande d'accès aux données en identifiant clairement son partenaire externe.

Les **chercheurs en entreprise de recherche**, c'est-à-dire les scientifiques œuvrant dans le secteur privé qui n'ont pas de privilèges de recherche au CIUSSS de l'Estrie – CHUS, qui désirent utiliser les données du CIUSSS de l'Estrie – CHUS pour réaliser un projet de recherche sont soumis aux mêmes conditions que les chercheurs externes.

Les **scientifiques en entreprise d'innovation**, c'est-à-dire les scientifiques et experts œuvrant dans le secteur privé d'innovation qui désirent utiliser les données du CIUSSS de l'Estrie – CHUS, doivent convenir d'une entente formelle avec l'établissement.

Mécanismes d'accès envisagés

Les mécanismes d'autorisation et de contrôle des accès tiennent compte du statut du chercheur dans l'établissement, des privilèges de recherche qui lui sont octroyés, de la nature du projet présenté et des partenaires du projet.

Préalablement au processus d'évaluation en trois étapes en vigueur dans l'établissement, un chercheur dont le projet requiert des renseignements personnels ou des renseignements de santé ou services sociaux doit déposer avec le descriptif de son projet une évaluation des facteurs relatifs à la vie privée (EFVP) des personnes concernées par ces renseignements.

Deux mécanismes d'accès aux données sont envisagés : l'accès rapide et l'accès régulier.

1. **L'accès rapide** (aussi appelé « Accès en mode libre-service ») : accès rapide et direct à des données anonymisées, agrégées ou non, pour des fins d'exploration. Ce mode d'accès ne permet pas l'extraction ni la publication de données. Une autorisation du Centre DORISE est requise pour l'exploration des données. L'autorisation est accordée au cas par cas, selon la nature de la demande.

   Le mécanisme d'accès pour l'exploration permet au chercheur de savoir si l'établissement possède les données requises et en quantité suffisante pour mettre en œuvre son protocole de recherche. Cette possibilité d'exploration des données doit être disponible en tout temps aux chercheurs autorisés qui en ont besoin.

2. **L'accès régulier** : accès accordé au chercheur autorisé à la suite d'une évaluation en trois étapes de son projet, tel que décrit dans la politique des privilèges de recherche du CIUSSS de l'Estrie – CHUS. Les jeux de données sont préparés par le Centre DORISE et rendus disponibles dans un environnement de confiance. Les mécanismes de protection sont multiples et comprennent, entre autres, le contrôle des accès, les autorisations de transfert de données, s'il y a lieu, le consentement et la transformation des données, s'il y a lieu. L'extraction des données sur un autre médium n'est pas favorisée, bien que possible, selon la nature du projet.

   Certains projets requièrent l'analyse de données confidentielles. Des autorisations spécifiques sont requises, et une évaluation des facteurs relatifs à la vie privée (EFVP) doit avoir été effectuée préalablement, conformément au processus d'évaluation en trois étapes du projet.

Des règles de base prévalent pour tout type d'accès comme le montre le tableau de l'Annexe G.

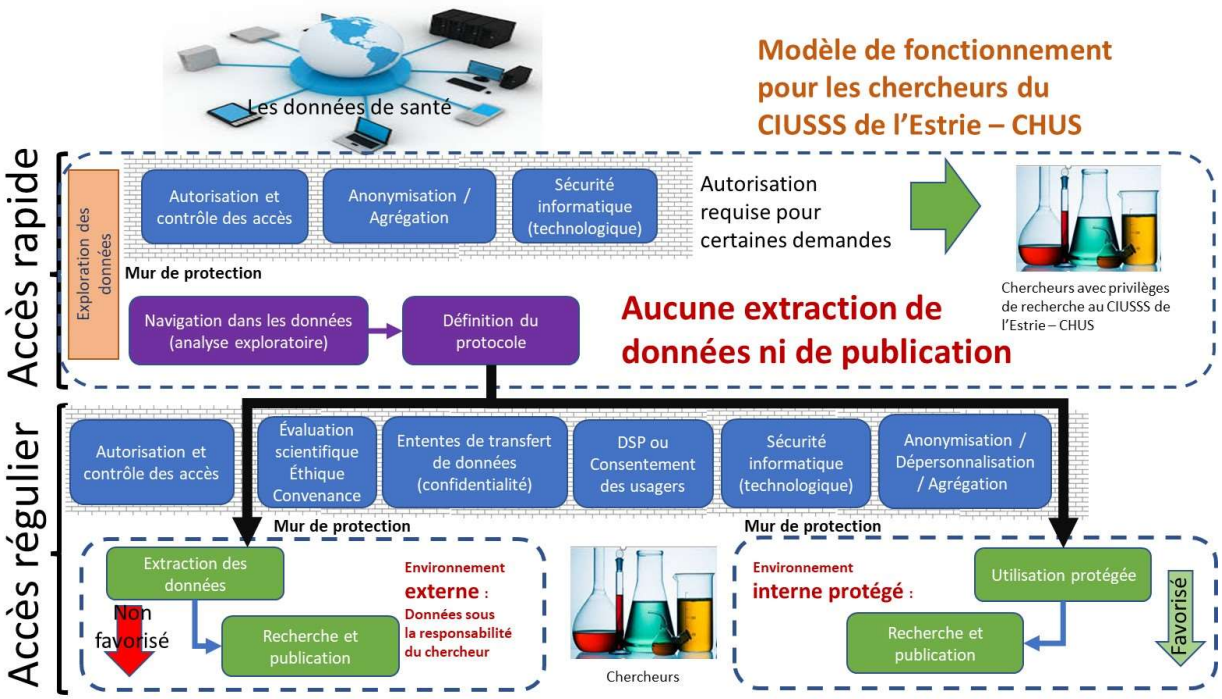


Figure 14 – Mécanismes d'accès aux données pour les chercheurs du CIUSSS de l'Estrie – CHUS.
Les chercheurs du CIUSSS de l'Estrie – CHUS sont des scientifiques qui ont un statut de chercheur au CIUSSS, à qui l'établissement a octroyé des privilèges de recherche. Deux mécanismes sont envisagés : l'accès rapide (aussi appelé accès en mode libre-service) et l'accès régulier. Les dispositifs de protection forment un « mur de protection » et visent à protéger les données tout en y permettant l'accès sous réserve de remplir certaines conditions. L'analyse de données pouvant comprendre des données confidentielles est possible sous autorisation spécifique, mais leur exploration en mode libre-service n'est pas permise. L'analyse et la visualisation des données dans un environnement de confiance est favorisée davantage que l'extraction des données. Cette dernière requiert une autorisation spécifique.

Mécanismes d'accès aux données pour les entreprises d'innovation

Les scientifiques et experts œuvrant dans les **entreprises d'innovation** qui désirent utiliser les données du CIUSSS de l'Estrie – CHUS doivent convenir d'une entente formelle avec l'établissement. Le Service des partenariats économiques de la Direction des ressources financières (DRF) de l'établissement se charge d'établir les dispositions de l'entente, notamment les modalités de collaboration, les exigences règlementaires, la répartition de la propriété intellectuelle et les conditions de financement. Il collabore étroitement avec le Bureau des affaires juridique (BAJ) et le Bureau d'autorisation des projets de recherche (BAPR) qui enclenche le processus d'évaluation du projet d'innovation en suivant le processus d'évaluation du projet imposé aux chercheurs. Le *Comité de coordination de la sécurité, de la gestion des accès et de la PRP* doit approuver le contenu de l'entente avant de procéder à la signature et donner les autorisations.

Le CIUSSS de l'Estrie – CHUS, dans le cas où il désire mandater une firme pour développer un outil innovant, doit :

1. Convenir d'une entente formelle avec l'entreprise d'innovation. Son Service des partenariats économiques de la DRF, accompagné du BAJ et du BAPR, se charge d'établir les dispositions de l'entente. Le *Comité de coordination de la sécurité, de la gestion des accès et de la PRP*

doit approuver le contenu de l'entente avant de procéder à la signature et donner les autorisations;

2. Nommer un chargé de projet qui assure le bon déroulement du projet et la communication avec l'entreprise;
3. Nommer un comité directeur du projet qui convient avec l'entreprise des travaux à réaliser, assure le suivi de la réalisation des livrables et dénoue les impasses qui se présentent. Le président de ce comité rend compte de l'avancement des travaux au signataire de l'entente;
4. S'assurer que le document de présentation du projet subisse une évaluation minimalement sur les plans de l'éthique et de la convenance, sous la direction du BAPR;

Mécanisme d'accès envisagé

Les mécanismes d'autorisation et de contrôle des accès doivent tenir compte de la nature de l'entente entre l'établissement et l'entreprise d'innovation, de la nature du projet présenté et des partenaires associés au projet.

Un seul mécanisme d'accès aux données est envisagé dans ce cas-ci : l'accès régulier aux données.

L'accès régulier : accès accordé à l'entreprise d'innovation à la suite d'une évaluation éthique et de convenance de son projet, conformément aux processus internes du CIUSSS de l'Estrie – CHUS. Seules les données anonymisées, dépersonnalisées ou agrégées sont rendues disponibles à l'entreprise. Dans le cas de données dépersonnalisées, les clés de chiffrement demeurent sous le contrôle de l'établissement.

Selon la nature du projet :

1. Les jeux de données sont préparés par le Centre DORISE et rendus disponibles dans un environnement de confiance;
2. Les données sont collectées directement des dispositifs médicaux;
3. Les données sont collectées durant les opérations cliniques.

Les mécanismes de protection sont multiples comme le montre la Figure 15. L'extraction des données sur un autre médium, préalablement au chargement dans la technologie en développement, n'est pas favorisée, bien que possible.

Certains projets requièrent l'analyse de données confidentielles. Les mécanismes d'accès envisagés tiennent compte de la possibilité d'accéder à ce type de données en retirant des mécanismes de protection, ceux qui sont directement liés aux données (Anonymisation / Dépersonnalisation / Agrégation). Une évaluation des facteurs relatifs à la vie privée (EFV) et des autorisations spécifiques sont requises de la part de l'établissement, conformément au processus d'évaluation pré-projet.

Des règles de base prévalent pour tout type d'accès comme le montre le tableau de l'Annexe G.

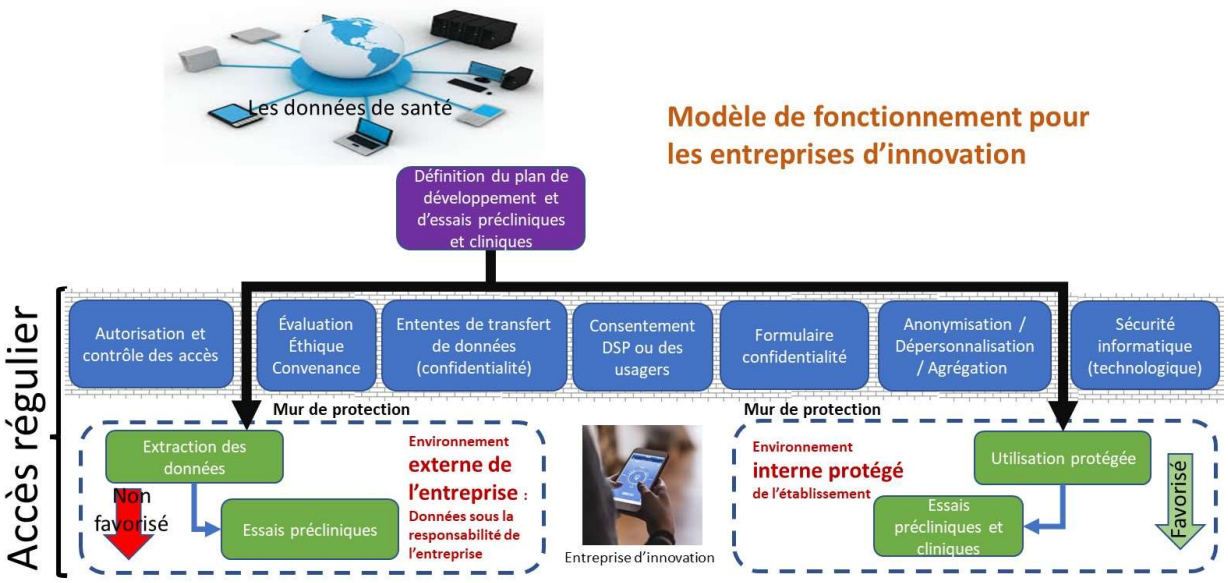


Figure 15 – Mécanismes d'accès aux données pour les entreprises d'innovation.
L'accès régulier est le seul mécanisme d'accès aux données pour les entreprises d'innovation. Les dispositifs de protection forment un « mur de protection » et visent à protéger les données tout en y permettant l'accès sous réserve de remplir certaines conditions. L'analyse de données confidentielles est possible sous autorisation spécifique. L'analyse et la visualisation des données dans un environnement de confiance est favorisée davantage que l'extraction des données. Cette dernière requiert une autorisation spécifique.

Mécanismes d'accès à d'autres données de l'établissement

Particularité des données génétiques

Le CIUSSS de l'Estrie – CHUS ne possède pas de banque formelle de données génétiques. Les centres de recherche du CIUSSS possèdent plusieurs banques d'échantillons recueillis lors de projets de recherche. Ces banques sont des outils de recherche en génétique, tout comme le sont les spectromètres de masse du Service de génétique médicale. L'accès à ces outils est encadré par les centres de recherche à la suite de l'approbation des projets de recherche.

Particularité des données sous la Loi sur la Protection de la Jeunesse

La *Loi sur la protection de la jeunesse* encadre l'utilisation des dossiers des jeunes. Dans un contexte de recherche, la banque de données informationnelles (BDI) du système clinico-administratif PIJ (Projet Intégration Jeunesse) constitue la principale source d'information pour les chercheurs. Elle comprend des données codées et désidentifiées. L'annexe H offre plus de détails.

La banque PIJ est gérée par le Centre DORISE. L'accès aux données pour une utilisation secondaire requiert l'autorisation du Centre. Une demande formelle d'accès aux données de la banque doit être acheminée au Centre. Elle sera évaluée par le Centre, en collaboration avec la Direction de la Protection de la Jeunesse de l'établissement. Le processus d'approbation des demandes de renseignements varie selon :

- Le type de données demandé;
- L'utilisation prévue des données;

- Le degré de sensibilité associé à ces données.

Concernant la recherche, le processus interne d'approbation des projets de recherche doit être suivi. Des privilèges sont octroyés aux chercheurs selon les autorisations accordées lors des analyses à trois étapes.

Particularité des données de santé publique

Le CIUSSS de l'Estrie – CHUS ne possède pas de banque de données de santé publique utilisable dans un contexte d'utilisation secondaire des données. Les chercheurs en santé publique collectent des données provenant de banques externes pour répondre à leurs questions de recherche.

La banque de l'Enquête de santé populationnelle estrienne est une banque dédiée au projet de recherche sur la santé de la population estrienne. Elle n'est pas disponible pour réaliser d'autres projets de recherche (voir Annexe H).

Appariement des données de l'établissement avec des données d'autres banques externes

Nombreux sont les projets qui requièrent d'apparier les données du CIUSSS de l'Estrie – CHUS avec des données d'autres banques externes, par exemple les banques du Guichet d'accès aux données de recherche de l'Institut de la statistique du Québec (ISQ), les banques d'autres établissements de santé ou d'autres universités, ou encore des banques d'autres provenances. La présente section résume l'annexe I qui détaille les mécanismes d'appariement ainsi que les responsabilités de l'utilisateur et du Centre DORISE du CIUSSS de l'Estrie – CHUS.

Au CIUSSS de l'Estrie – CHUS, c'est le Centre DORISE qui est le maître d'œuvre du processus d'appariement. L'utilisateur travaille en étroite collaboration avec le centre tout au long du processus. Comme le Centre DORISE n'a pas la responsabilité de toutes les banques de données de l'établissement, il doit communiquer avec les directions détentrices de données pour les informer du besoin d'apparier leurs données avec d'autres données et de les impliquer dans le processus de création du ou des fichiers d'appariement.

- Dans le cas où **l'appariement se réalise à l'ISQ ou chez un partenaire externe**, le Centre DORISE est responsable de la préparation des données, de l'organisation du fichier d'appariement, de sa transmission ou de sa disponibilité à l'ISQ ou au partenaire externe.
- Dans le cas où **l'appariement se réalise au CIUSSS de l'Estrie – CHUS**, le Centre DORISE est responsable de la préparation des données, de l'organisation du fichier d'appariement, de la définition des exigences en termes de formats de données et de l'organisation du fichier de chaque partenaire, de la réception des fichiers externes, du processus d'appariement, de la création du fichier de résultats et de sa transmission ou de sa disponibilité à chaque partenaire externe. Dans le cas où les données à apparier sont sous la responsabilité d'une ou plusieurs directions détentrices de données, le Centre DORISE les informe de la demande d'appariement et les implique dans le processus d'appariement.

Les méthodes d'appariement de base utilisées par le Centre DORISE sont celles utilisées par l'ISQ, soit l'appariement déterministe et l'appariement probabiliste. L'Annexe I détaille davantage ce sujet.

RÈGLES D'ACCÈS AUX DONNÉES

Règles générales

Le CIUSSS de l'Estrie – CHUS agit comme fiduciaire des données qu'il collecte. Elles incluent, entre autres, les renseignements de santé ou de services sociaux et les renseignements personnels de ses usagers, les données populationnelles de son territoire de desserte ainsi que les renseignements personnels de ses employés. L'accès aux données du CIUSSS s'aligne avec les règles internes de l'établissement, dont celles qui sont liées à la sécurité et à la confidentialité des données. Elles sont :

- **Les données collectées** et produites par le CIUSSS de l'Estrie – CHUS **demeurent à l'intérieur de l'établissement de santé***;*
- **Les données communiquées sont uniquement les résultats des requêtes** ou des données anonymisées ou dépersonnalisées ou agrégées. Aucune communication ni copie de données brutes du CIUSSS de l'Estrie – CHUS dans une base de données externe n'est permise, sauf si une autorisation spécifique à cet effet a été accordée par les autorités de l'établissement;
- Les jeux de données utilisés pour les analyses demeurent disponibles aux chercheurs dans le respect du cadre législatif et réglementaire en vigueur;
- L'accès aux données est d'abord basé sur la fonction de l'utilisateur (*role-based access*). Un mécanisme d'accès plus sophistiqué de type *fine-grained* peut s'avérer utile pour les utilisateurs chercheurs et les utilisateurs externes à l'établissement, selon le type de données recherchées;
- La sécurité et la confidentialité des données ainsi que la protection des données confidentielles sont assurées conformément aux règles internes de l'établissement et celles du Gouvernement du Québec;
- **La sécurité est intégrée dans le design** de l'écosystème d'analyse des données de l'établissement selon l'approche *Security by design*. Ceci inclut les règles d'accès aux données.

Règles d'accès à l'information

Les règles liées aux mécanismes d'accès à l'information en usage dans l'établissement et conformes au cadre légal et réglementaire en vigueur sont respectées dans le processus d'accès à l'information.

Règles d'accès aux données

Certaines règles d'accès particulières aux mécanismes d'accès proposés ci-haut s'ajoutent aux règles générales. Pour :

- La communauté interne de l'établissement (voir Figure 16 et le tableau de l'Annexe G);
- Les chercheurs (voir Figure 17 et le tableau de l'Annexe G);
- Les scientifiques et experts des entreprises d'innovation (voir Figure 18 et le tableau de l'Annexe G).

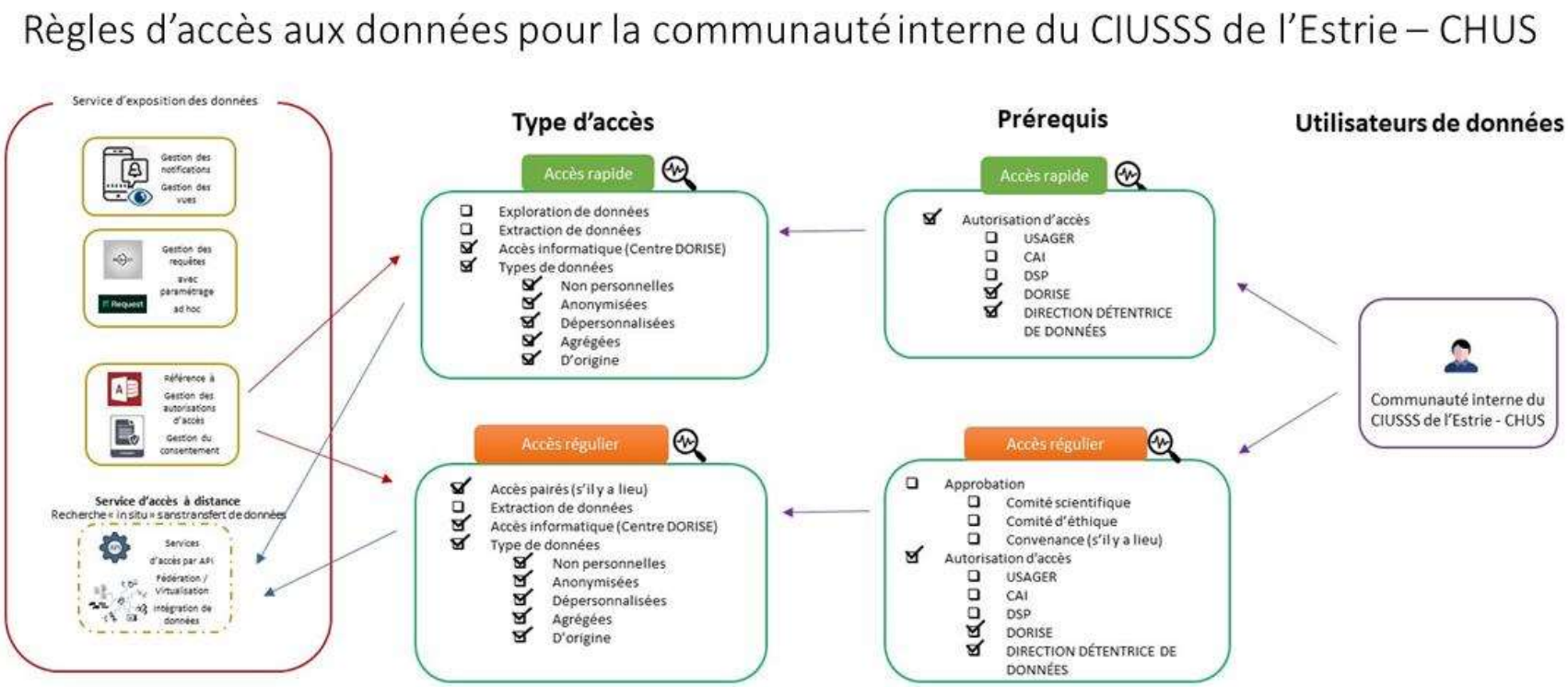


Figure 16 – Règles d'accès aux données pour la communauté interne de l'établissement.
Les règles d'accès aux données demeurent les mêmes peu importe le type d'accès envisagé. L'accès rapide correspond à l'accès en mode libre-service. Il est utilisé pour analyser des jeux de données préconçus par le Centre DORISE. Ce dernier autorise les accès et les contrôles. Les données de toutes formes peuvent faire partie des jeux de données. Quant à l'accès régulier, ce dernier requiert les mêmes autorisations que l'accès rapide. Les données de toutes formes peuvent aussi faire partie des jeux de données analysés. Les données d'origine sont des données qui n'ont subi aucune transformation. L'analyse des données dans un environnement sécurisé de confiance est préconisée.

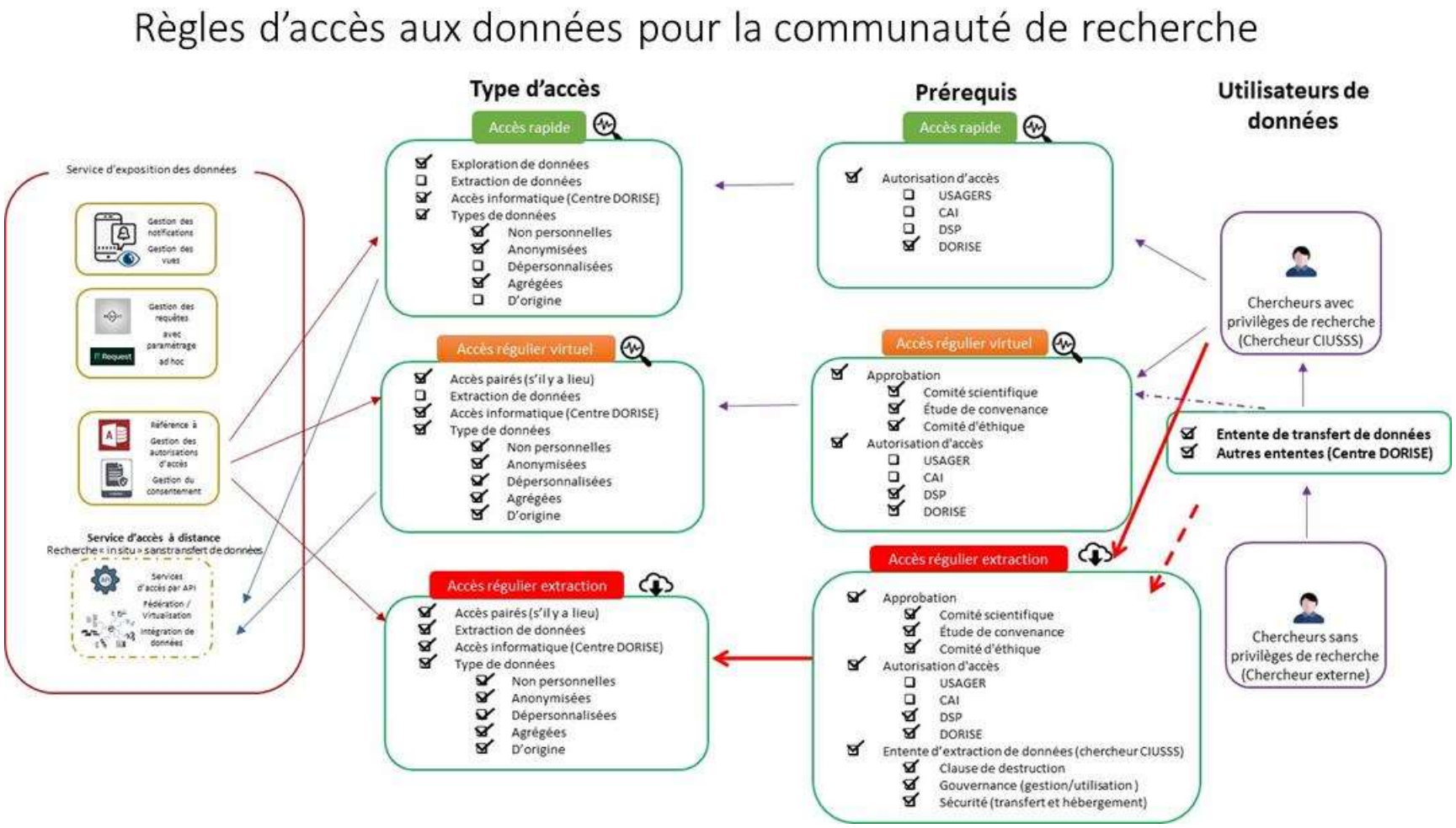


Figure 17 – Règles d'accès aux données pour les chercheurs.
Les règles d'accès aux données diffèrent selon le type d'accès envisagé. L'accès rapide, qui correspond à l'accès en mode libre-service, est dédié à l'exploration de données anonymisées, agrégées ou non, et non personnelles. L'accès rapide aux données n'exige que l'autorisation du Centre DORISE, tandis que l'accès régulier exige davantage de prérequis. L'accès régulier avec extraction de données (accès régulier extraction) exige, en plus des prérequis de l'accès régulier avec visualisation seulement (accès régulier virtuel), une entente d'extraction de données accordée au chercheur CIUSSS affilié au projet. Les données d'origine sont des données qui n'ont subi aucune transformation.

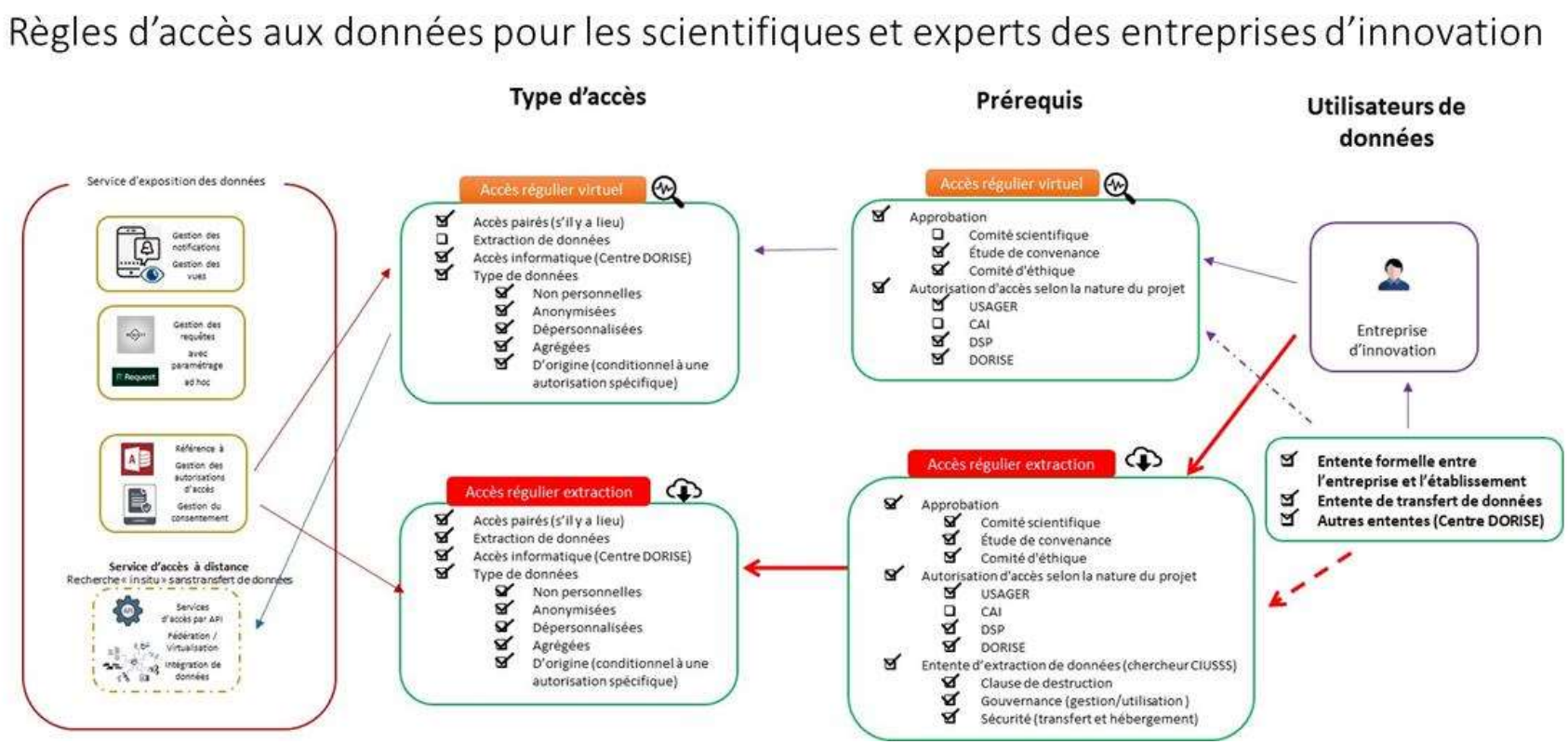


Figure 18 – Règles d'accès aux données pour les entreprises d'innovation.

Les règles d'accès aux données diffèrent selon le type d'accès envisagé. L'accès rapide, qui correspond à l'accès en mode libre-service, n'est pas prévu pour les entreprises d'innovation. Seul l'accès régulier prévaut. Ce dernier exige davantage de prérequis. L'accès régulier avec extraction de données (accès régulier extraction) exige, en plus des prérequis de l'accès régulier avec visualisation seulement (accès régulier virtuel), une entente d'extraction de données accordée à l'entreprise. L'accès aux données d'origine, c'est-à-dire, aux données n'ayant subi aucune transformation, exige une autorisation spécifique de la part de l'établissement.

PARTAGE DES DONNÉES

PARTAGE DE DONNÉES AVEC DES PARTENAIRES INTERNES ET EXTERNES

Partage entre membres de la communauté interne du CIUSSS de l'Estrie – CHUS

Il est recommandé aux membres de la communauté interne du CIUSSS de l'Estrie – CHUS travaillant à un même projet d'accéder aux mêmes jeux de données par le biais de l'écosystème d'analyse de données de l'établissement, sous la supervision du Centre DORISE, et d'éviter le transfert des jeux de données d'un membre à un autre. Cette stratégie permet de conserver l'intégrité et la qualité des données analysées.

La demande d'accès faite au Centre DORISE doit comprendre les noms des membres de la communauté interne de l'établissement qui accèderont aux jeux de données requis dans le même environnement.

Partage avec des partenaires externes à la communauté du CIUSSS de l'Estrie – CHUS

Il est recommandé que toute demande de partage de données du CIUSSS de l'Estrie – CHUS faite par un partenaire externe soit acheminée au *Comité de coordination de la sécurité, de la gestion des accès et de la PRP* pour analyse et recommandation. Le Comité travaille en étroite collaboration avec le Bureau d'autorisation des projets de recherche (BAPR), le Bureau des affaires juridiques (BAJ) et le Service des partenariats économiques**.** Chaque demande est évaluée au cas par cas. Le comité applique les règles énoncées dans le présent chapitre, notamment :

1. Favoriser l'accès aux données via un environnement sécurisé plutôt que de transférer les données au partenaire externe. L'accès aux données confidentielles respecte les conditions de la ***Loi 25*** et du ***Projet de loi 3*** à la suite de son adoption;
2. Partager uniquement les résultats des requêtes, ne pas partager les données;
3. S'il est nécessaire de partager des données, l'établissement partage des données qui ont été anonymisées ou dépersonnalisées ou agrégées, sauf si une autorisation spécifique au partage de données d'origine ou brutes a été accordée par les autorités de l'établissement;
4. Le partage de données confidentielles respecte les conditions de la ***Loi 25*** et du ***Projet de loi 3*** à la suite de son adoption.

Le Comité est tenu de respecter les règles et processus de sécurité de l'information énoncés dans le Cadre de gestion de la sécurité de l'information.

GOUVERNANCE DE LA GESTION DES ACCÈS AUX DONNÉES

COMITÉ DIRECTEUR DE LA GESTION DES DONNÉES

Ce comité définit les orientations stratégiques en matière de gestion des accès et des transferts des données du CIUSSS de l'Estrie – CHUS, et les transmet au *Comité de coordination de la sécurité, de la gestion des accès et de la PRP*.

Il approuve les mécanismes proposés et les rôles et responsabilités des intervenants sur le terrain. Il prend connaissance des rapports de gestion et règle les problématiques transversales à l'organisation.

Il entérine les recommandations du *Comité de coordination de la sécurité, de de la gestion des accès et de la PRP* concernant l'accès aux données par les partenaires externes et/ou le partage de données aux partenaires externes.

COMITÉ DE COORDINATION DE LA SÉCURITÉ, DE LA GESTION DES ACCÈS ET DE LA PRP

Ce comité assure la gestion tactique de l'accès aux données :

- Il propose au *Comité directeur de la gestion des données* les mécanismes de gestion des accès et des transferts de données à mettre en place;
- Il définit les rôles et responsabilités des intervenants terrain en matière de gestion des accès;
- Il met en place des mécanismes de suivi des accès (Statistiques d'accès, Log Book, rapports d'audits, etc.);
- Il soutient les intervenants terrain dans leurs activités de gestion des accès;
- Il résout les problématiques locales d'accès et propose au Comité directeur des solutions aux problématiques transversales à l'organisation qu'il met en place;
- Il prend en charge l'analyse de toute demande de partage de données du CIUSSS faite par un partenaire externe. Il transmet sa recommandation au *Comité directeur de la gestion des données* pour entérinement. Il travaille en étroite collaboration avec le BAPR, le BAJ et le Service des partenariats économiques et au besoin, il consulte d'autres collaborateurs de l'établissement, notamment :
    - La responsable de la sécurité de l'information;
    - Le Centre DORISE de la DQEPP;
    - Un représentant de la direction des ressources informationnelles et technologiques;
    - Le responsable de l'accès et de la PRP, selon la nature de la demande;
    - La Direction des services professionnels;
    - Le Comité d'éthique de la recherche, selon la nature de la demande.

INTERVENANTS-TERRAIN RESPONSABLES DE LA GESTION DES ACCÈS

Directions détentrices de données

Les directions détentrices de données assurent la gestion des accès aux banques de données dont elles ont la responsabilité, selon les privilèges octroyés lors de l'approbation des demandes d'accès. Elles enregistrent les conditions d'accès dans un registre des accès et assurent leur mise à jour à fréquence régulière. Ces conditions comprennent, entre autres, qui a eu accès à quels renseignements, à quel moment et pour combien de temps. Les directions font rapport au *Comité de coordination de la sécurité, de la gestion des accès et de la PRP*.

Centre DORISE

Le Centre DORISE assure la gestion des accès à l'écosystème d'analyse de données dont il a la responsabilité, selon les privilèges octroyés lors de l'approbation des demandes d'accès. Le Centre enregistre les conditions d'accès dans un registre des accès et assure leur mise à jour à fréquence régulière. Ces conditions comprennent, entre autres, qui a eu accès à quels renseignements, à quel moment et pour combien de temps.

Dans le contexte de la recherche, il est suggéré que l'accès aux diverses banques de données de l'établissement soit centralisé au Centre DORISE.

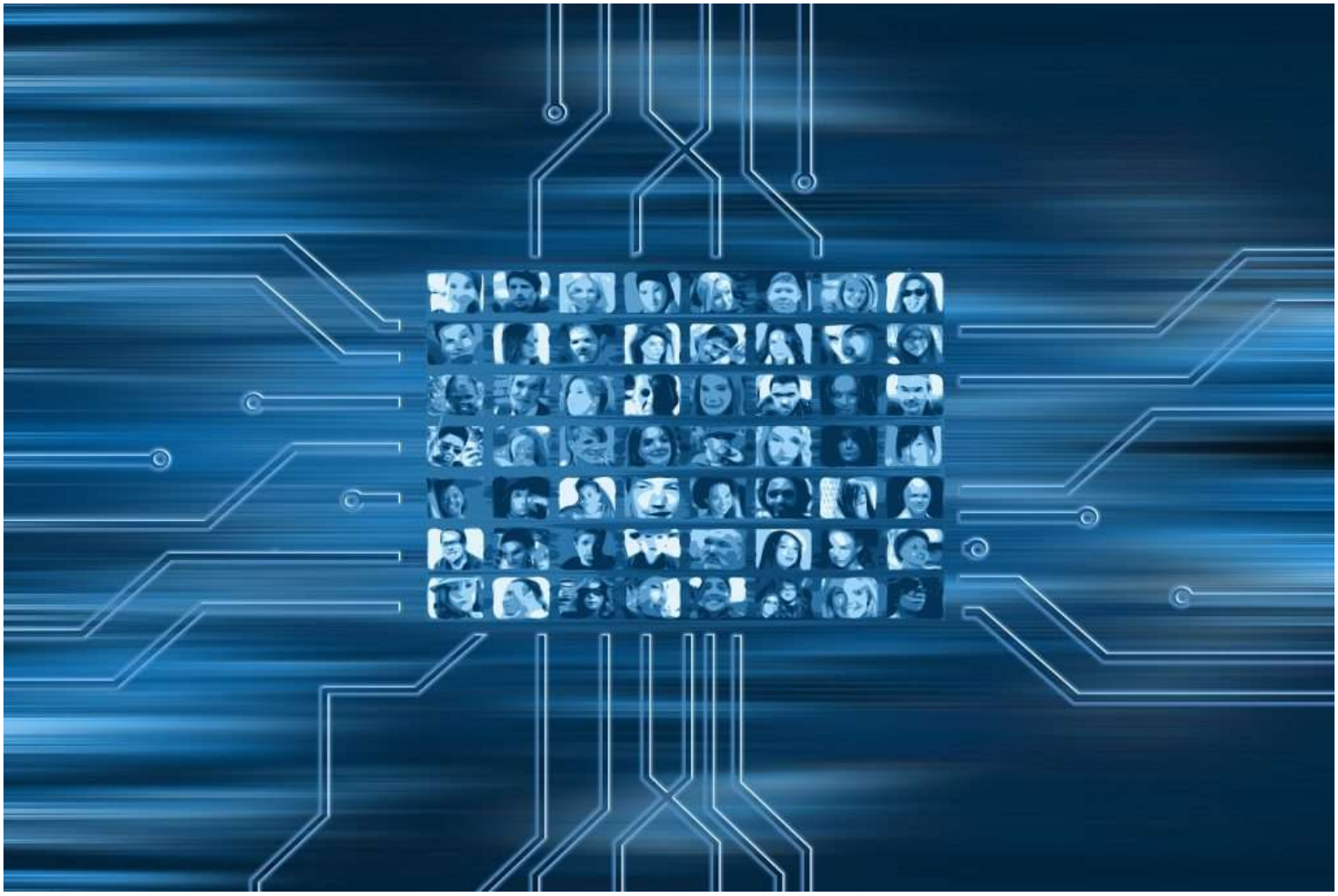
Le Centre DORISE définit les moyens d'accéder aux banques de données. Il octroie le code d'accès à la suite d'une évaluation des risques de bris de confidentialité. Le code d'accès est individualisé et confidentiel. Il ne peut être transmis ni utilisé par une tierce personne. L'utilisateur à qui le code est octroyé en assume l'entière responsabilité.

Le Centre DORISE collabore avec le responsable de la sécurité de l'information dans l'organisation d'audits de vérification des mécanismes d'accès pour assurer l'efficacité de ces mécanismes ainsi que la sécurité des données.

Le Centre DORISE détermine aussi les mécanismes d'anonymisation et/ou de dépersonnalisation des données confidentielles demandées lors de la demande d'accès afin d'assurer leur protection et leur confidentialité. Il conserve les clés de dépersonnalisation dans un lieu sûr inaccessible aux utilisateurs.

Le Centre DORISE prend en charge l'opérationnalisation des demandes d'accès aux données par les partenaires externes, à la suite d'une recommandation du *Comité de coordination de la sécurité, de la gestion des accès et de la PRP* entérinée par le *Comité directeur de la gestion des données*.

SECTION 4 – OPTIMISER L'UTILISATION DES DONNÉES



Publié par : ZDNet, 2022

CHAPITRE 4.1 – LES NORMES

DÉFINITION

Une **norme** est une exigence qui applique aux données un certain nombre de caractéristiques ou d'attributs précis destinés à établir une compréhension commune de la signification et de la sémantique des données. Elle permet d'assurer une interprétation juste des données par les personnes qui les collectent et les utilisateurs de données (les décideurs, les gestionnaires, la communauté interne, les chercheurs, les usagers). Une même norme utilisée dans plusieurs systèmes d'information différents permet l'interopérabilité[34] de ces systèmes.

PRINCIPES DIRECTEURS

L'application des normes repose sur trois grands principes directeurs :

1. **Les normes contribuent à la gestion et à l'exploitation des données en tant qu'actif stratégique** afin de les rendre facilement repérables, accessibles, interopérables, réutilisables et adaptées à leur utilisation (conformément au principe FAIR)[35].
2. **Les normes soutiennent une gestion des données globale et transversale à l'organisation** permettant la compréhension commune des données pour l'ensemble de la communauté du CIUSSS de l'Estrie - CHUS.
3. **Les utilisateurs et partenaires connaissent les normes et les utilisent** dans le cadre de leurs activités autorisées en gestion de données, et ce, dans le respect des règles gouvernementales et des lois.

IMPORTANCE DES NORMES

La création d'un jeu de données de qualité est généralement complexe à cause de l'hétérogénéité des données. Toutefois, **il est possible de réduire cette complexité en utilisant des normes, soit à la collecte des données dans les systèmes sources ou à l'élaboration du modèle de données**.

La fiabilité des résultats d'une analyse de données dépend essentiellement de trois facteurs :

1. La qualité du jeu de données sélectionné;

   Le jeu de données comprend des données hétérogènes tant au niveau de leur nature qu'au niveau de leur structure puisqu'elles proviennent de systèmes sources variés, chacun possédant son propre format de données. Elles sont organisées et classées (données physiologiques, résultats de laboratoires, données diagnostiques, médicaments, etc.). Leur signification est comprise tant au niveau du texte que des valeurs et des unités. Les contextes dans lesquels les données ont été collectées sont connus (situation d'urgence, clinique externe, hospitalisation, diagnostic préliminaire, diagnostic final, autres).
2. La performance du modèle de données qui transforme efficacement les données pour obtenir une représentation assimilable par les algorithmes d'analyse tout en conservant leur complexité conceptuelle d'origine.

[34] Capacité des systèmes électroniques ou informatiques hétérogènes d'échanger de l'information. Réf. Oxford Language

[35] FAIR = Findable, accessible, interoperable, reusable

3. La puissance de l'algorithme d'analyse qui génère les résultats escomptés rapidement.

L'IMPORTANCE DES NORMES À LA COLLECTE DES DONNÉES :

L'utilisation des normes à la collecte des données dans les systèmes sources permet la saisie uniforme, juste et précise des données, ce qui améliore la qualité des données qui seront utilisées. Elle permet aussi d'améliorer la performance des modèles de données et des algorithmes d'analyse et d'en réduire la complexité. Il faut cependant choisir les normes, les adopter et les utiliser avec rigueur si l'on veut en tirer les meilleurs bénéfices.

Le plus grand bénéfice d'utiliser les normes à la collecte des données est de faciliter l'interopérabilité des systèmes utilisés tout au long du parcours de l'usager. Les systèmes qui utilisent une même norme peuvent s'échanger et traiter les mêmes données sans les transformer. Ces données ont la même signification pour la personne qui les consulte, peu importe le système qu'elle utilise. Ainsi, les données sont collectées une seule fois, mais elles sont utilisées à de nombreuses reprises tout au long du parcours de l'usager.

L'IMPORTANCE DES NORMES À L'UTILISATION DES DONNÉES :

Pour les utilisateurs de données, la qualité des résultats des analyses de données est directement reliée à la qualité des données utilisées. L'utilisation de normes réduit l'hétérogénéité des données et leur diversité sémantique. L'application d'une même norme sur un type de données, par exemple les données diagnostiques, permet à un utilisateur de comparer les données de même type provenant de plusieurs sources sans les transformer. Ces données ont la même signification, quelle que soit leur origine. Certaines normes permettent aussi une classification et une codification plus précises des données. Les normes sont donc un élément clé de la qualité des données. Sans elles, l'analyse, l'interprétation et l'intégration des données risque d'être erratique.

LE CHOIX DE NORMES

Il existe déjà un nombre important de normes établies en santé qui s'appliquent aux différents domaines d'activités de l'organisation. Le choix des normes à appliquer aux données s'appuie sur plusieurs critères, dont l'identification des différents types de données utilisés dans l'organisation. Ce choix résulte d'un processus d'examen des normes effectué par des experts de l'organisation. La Figure 19 montre plusieurs normes déjà en utilisation dans cinq catégories :

- Les normes de transfert;
- Les normes de contenu;
- Les normes de terminologie;
- Les normes d'interopérabilité;
- Les normes de sécurité.

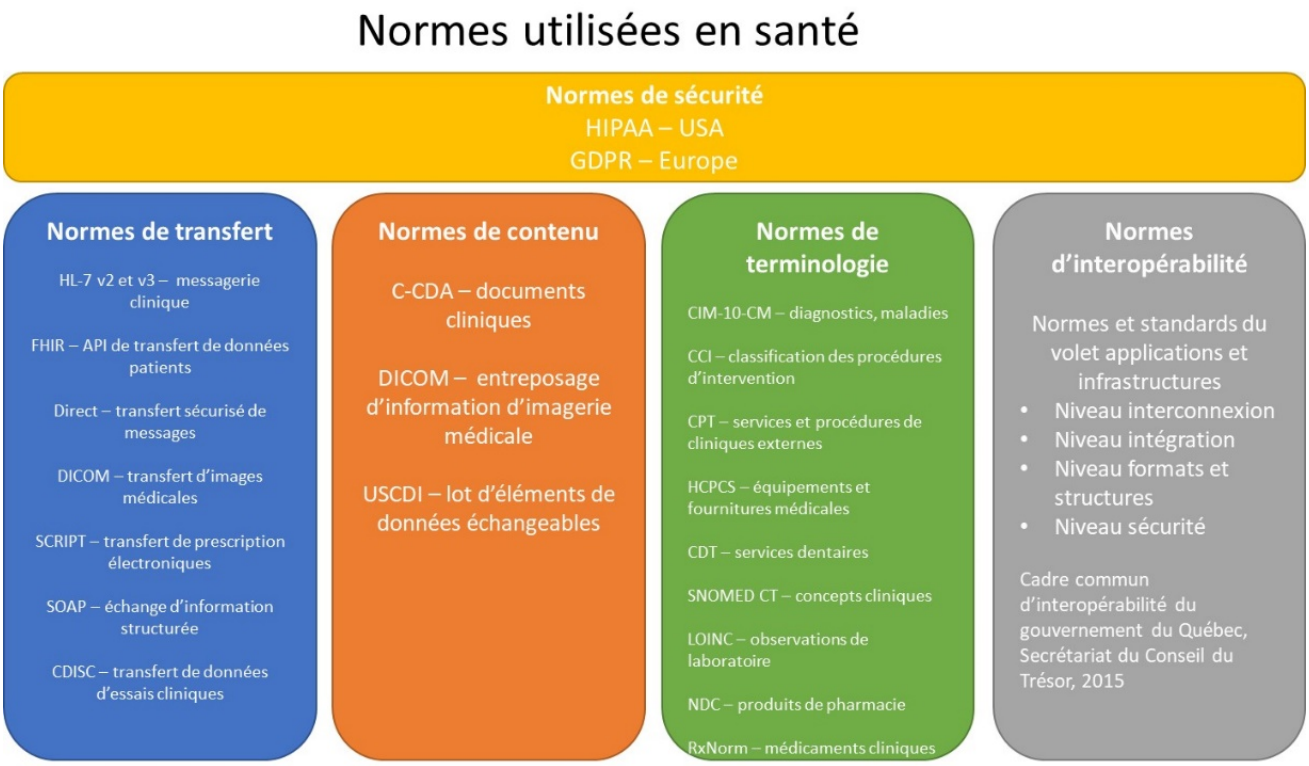


Figure 19 – Quelques normes utilisées en santé.
La figure ne comprend pas toutes les normes déjà en utilisation dans le domaine de la santé. Il faut aussi envisager qu'à ces normes s'ajoutent les cadres normatifs gouvernementaux et les directives ministérielles (ex : le cadre normatif de Med-Écho, les directives financières du AS-471, etc.). Un tel ajout élargit l'éventail de normes à considérer dans la sélection des normes à adopter.

Les critères de sélection des normes et les méthodologies d'application à adopter requièrent un examen attentif. Ils doivent prendre en considération différentes sources d'information qui ont une incidence sur la façon dont les normes peuvent être appliquées et maintenues, notamment l'évaluation de la technologie et des normes existantes et nouvelles, les exigences légales en vigueur relatives aux données de santé, les exigences opérationnelles actuelles et futures de l'organisation et d'autres normes interreliées.

Le processus d'examen des normes est rigoureux et basé sur des critères spécifiques et des lignes directrices connexes. La norme choisie doit répondre aux fins d'utilisation envisagées dans le ou les systèmes d'information sélectionnés. Trois catégories de critères sont considérées dans l'examen d'une norme :

- Les critères d'adaptation à la finalité,
- Les critères d'intendance et
- Les critères de qualité de la norme.

La Figure 20 détaille un exemple de critères appartenant à ces trois catégories[36].

D'autres critères additionnels peuvent être ajoutés pour réaliser une analyse plus approfondie.

[36] Tiré de « Guide de sélection des normes » publié par eHealth Ontario

Critères d'examen d'une norme	La norme est adaptée à la finalité	Elle est alignée sur l'architecture du système d'information sélectionné
		Elle est restreinte ou étendue à partir de normes d'interopérabilité existantes
		Elle appuie les exigences opérationnelles de l'organisation
		Elle appuie les exigences techniques de l'organisation
		Son niveau d'adoption dans l'organisation est élevé
		Elle prend en charge du texte codé plutôt que du texte libre
	Intendance	Coûts d'installation de la norme
		Structure de gouvernance appuyant l'utilisation de la norme
		Propriété intellectuelle et coûts de la licence
		Processus défini de maintenance
	Qualité de la norme	Soutien et formation lors de l'installation
		Elle permet de réaliser l'interopérabilité
		Outils d'installation et de maintenance
		Méthodologies pour les tests de conformité
		Stabilité éprouvées
		Capacité à être adaptée et personnalisée

Figure 20 – Résumé des critères de sélection d'une norme appliqués lors de l'examen des normes.

NORMES À UTILISER ET BONNES PRATIQUES À ADOPTER

Le choix de normes touchant les différentes dimensions du cycle de vie[37] des données et leur mise en œuvre fait partie des responsabilités de la gouvernance des données. L'application de normes prend tout son sens lorsqu'elle suit des règles alignées sur les bonnes pratiques. Cette section présente des exemples de normes à utiliser et un certain nombre de bonnes pratiques à suivre aux différentes étapes du cycle de vie des données.

INSCRIPTION ET COLLECTE DE DONNÉES DE L'USAGER

Que ce soit à l'inscription de l'usager ou à la collecte de ses données dans différents systèmes d'information, l'utilisation de normes revêt une grande importance car elle permet la saisie uniforme, juste et précise des données de l'usager tout au long de son parcours. C'est une manière pour l'organisation de développer une pratique uniforme garantissant la qualité, la sécurité et le partage des données de façon harmonisée.

Des normes à utiliser

- Les normes de contenu;
- Les normes de terminologie;

[37] Stratégie de gestion des données CIUSSSE-CHUS, page 64, figure 10.

- Le répertoire des municipalités du Québec du ministère des Affaires municipales et de l'Habitation du Québec pour l'inscription des villes;
- Le répertoire des codes postaux canadiens pour l'inscription des codes postaux;
- La base de données ouverte d'adresses publiques de Statistique Canada pour l'inscription des adresses civiques;
- Le registre des usagers du Québec pour l'inscription des nom, prénom et coordonnées de l'usager, si ce dernier est inscrit au registre;
- Le permis de conduire, la carte d'assurance maladie ou autre document officiel pour l'inscription des nom et prénom de l'usager, si ce dernier n'est pas inscrit au registre des usagers du Québec;
- Les normes de sécurité.

Des bonnes pratiques à adopter :

- Dès l'inscription de l'usager, un numéro d'identification unique (NIU) et sans équivoque doit lui être assigné de manière à lui rattacher toutes les données de santé collectées dans les différents systèmes sources utilisés tout au long de son parcours. L'utilisation de l'index-patient maître de l'organisation ou du numéro d'identification unique du registre des usagers du Québec facilite l'identification unique de l'usager;
- Les renseignements contenus dans les fichiers ou index des différents systèmes sources sont synchronisés, à jour, exacts et complets[38];
- La correction des données dans un système se réplique automatiquement dans tous les autres systèmes sources sollicités lors du parcours de l'usager.

CHARGEMENT DES DONNÉES

Un utilisateur de données qui désire exploiter des données d'un type particulier, par exemple les données correspondant à un diagnostic précis, à une maladie particulière, à un résultat de laboratoire spécifique, pour des fins de recherche, évaluation, gestion ou autre, effectuera un chargement des données recherchées de plusieurs systèmes d'information sources vers une banque de données centrale. Ce chargement respecte l'ensemble des règles en vigueur dans l'organisation où l'utilisateur se trouve. Ces systèmes d'information sources peuvent être localisés dans un même établissement de santé ou, dans le cas des études multicentriques, ils peuvent être localisés dans plusieurs établissements de santé différents.

Des normes à utiliser

- Les normes de transfert des données. Ces normes visent à faciliter l'extraction et le transfert des données en précisant la position de chaque champ dans l'algorithme de transfert et la nature du contenu de chaque champ.
- Les normes de sécurité.

Des bonnes pratiques à adopter :

[38] Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, Chapitre A-2.1, art. 72. « Un organisme public doit veiller à ce que les renseignements personnels qu'il conserve soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis ou utilisés. ».

- Choisir et utiliser un nombre restreint d'algorithmes de transfert de manière à assurer une meilleure qualité de transfert des données et un meilleur contrôle du niveau de sécurité attendu lors du transfert des données.

STOCKAGE DES DONNÉES

Le stockage des données dans les bases de données des systèmes d'information sources ou dans des banques distinctes d'exploitation des données assure la disponibilité des données en tout temps pendant toute la période de conservation des données. L'utilisation de normes, jumelée à l'architecture et à la modélisation des données, permet d'établir des règles de traitement, de stockage et d'utilisation des données.

Du point de vue de l'utilisateur, ces normes peuvent sembler loin de ses objectifs, mais il n'en est rien. Ces éléments permettent de procéder au stockage et à l'intégration des données qui lui sont partagées.

Des normes à utiliser

- Les normes de contenu;
- Les normes de terminologie;
- Les normes de sécurité.

Des bonnes pratiques à adopter :

- Les banques de données servant à l'utilisation secondaire des données sont localisées sur des serveurs indépendants. Éviter d'utiliser les serveurs dans lesquels les bases de données des systèmes sources sont localisées pour éviter le ralentissement de ces systèmes transactionnels;
- Le rafraîchissement des banques de données à partir des systèmes sources est à une fréquence permettant l'utilisation des données les plus récentes ou à jour (stockage incrémental);
- Le transfert des données du système source vers la banque en mode « PUSH » est favorisé pour éviter de solliciter le système source avec des requêtes de transfert automatiques.

CONSERVATION DES DONNÉES

La *Loi sur les services de santé et les services sociaux* prévoit que l'établissement de santé se dote d'un calendrier de conservation des informations de santé qu'il collecte et utilise, et est tenu de respecter ce calendrier.

En ce qui a trait aux données collectées dans le cadre de la recherche, la Loi prévoit la destruction de ces données une fois la recherche complétée. Toutefois, plusieurs types de travaux de recherche nécessitent l'exploitation de données historiques. Ces données sont collectées pendant de nombreuses années et doivent être conservées pour des périodes qui dépassent nettement la période de conservation prévue au calendrier de conservation de l'établissement.

La *Loi 25* adoptée en octobre 2021 introduit deux types de méthodes permettant de diminuer la nature identificatoire des données personnelles : la dépersonnalisation (art. 65.1) et l'anonymisation (art. 73). **La dépersonnalisation** permet aux organismes publics et aux entreprises du secteur privé d'utiliser les données personnelles à des fins d'étude, de recherche ou de production de statistique. **L'anonymisation** des données personnelles est vue comme une alternative à leur destruction

lorsque les fins auxquelles elles ont été recueillies ou utilisées sont accomplies, et permettrait donc de conserver ces données indéfiniment. Une fois anonymisées, les données personnelles ne sont plus soumises aux règles du calendrier de conservation. Ceci s'applique aussi aux données de santé. Pour conserver des données de qualité, il importe d'utiliser des normes et d'adopter de bonnes pratiques de conservation.

Des normes à utiliser

- Les normes de contenu;
- Les normes de terminologie;
- Les normes de sécurité.

Des bonnes pratiques à adopter :

- Anonymiser les données inactives, c'est-à-dire les données pour lesquelles la période de conservation prévue au calendrier expire, au lieu de les détruire[39]. Transférer ces données dans une banque de données distincte disponible à l'utilisation secondaire. Dans ce cas, ces données sont considérées « publiques » et disponibles en tout temps à tout utilisateur;
- Dépersonnaliser les données actives et semi-actives, et les transférer dans une banque de données distincte disponible pour des fins d'étude, de recherche et de production de statistique. Les données de cette banque peuvent être intégrées aux données de la banque de données anonymisées;
- Utiliser les techniques de conservation les plus adéquates et les moins coûteuses, selon les catégories de données;
- Anonymiser les données collectées et utilisées pour la recherche une fois la recherche complétée au lieu de les détruire[40].

MÉTADONNÉES AU SERVICE DES UTILISATEURS

Pour l'utilisateur de données, comprendre et identifier correctement la provenance des sources de données, leur signification, les normes qui les régissent, le système source ou le dépôt duquel elles sont extraites, traitées, etc., sont des informations de première importance. Ces informations sont appelées métadonnées[41].

Les métadonnées sont des informations qui décrivent les données de manière cohérente**.** Elles ont de multiples utilités, notamment rendre plus fluide les flux de travail, protéger les données sensibles, lier les données entre elles pour les retrouver plus facilement, et assurer une gestion efficace des données. Les métadonnées contribuent au processus de normalisation, ainsi qu'au traitement et au regroupement des données dans une plateforme d'analyse. Elles facilitent le formatage des données afin d'en permettre la gestion, le visionnement intégré ainsi que l'exploration et l'exploitation par l'utilisateur.

---

[39] La Loi 25 élargit, dans son article 28, les modalités de disposition des renseignements personnels, en prévoyant la possibilité d'anonymiser ces renseignements afin de les conserver et les utiliser à des fins d'intérêt public. Dans ce cadre d'utilisation, le consentement de la personne n'est pas requis. Nb. Cette modalité prendra effet en septembre 2023.

[40] Loi 25 – art. 28 et 111.

[41] Métadonnée : Donnée qui renseigne sur la nature de certaines autres données et qui permet ainsi leur utilisation pertinente.
Référence : http://www.thesaurus.gouv.qc.ca/tag/terme.do?id=7979

Les métadonnées se trouvent dans un catalogue d'accompagnement d'un jeu de données ou dans un annuaire d'entrepôts de données. Ces catalogues et annuaires sont disponibles aux utilisateurs.

Des normes à utiliser

- Aucune.

Des bonnes pratiques à adopter :

- Se doter d'un cadre de gestion des métadonnées de l'établissement;
- Consigner les métadonnées dans des catalogues ou annuaires et rendre ces derniers aux utilisateurs. Former les utilisateurs à utiliser les métadonnées pour rechercher, regrouper et traiter les données pertinentes;
- Traiter les métadonnées de la même façon que le sont les données : assurer leur qualité, leur sécurité, leur confidentialité, leur protection.

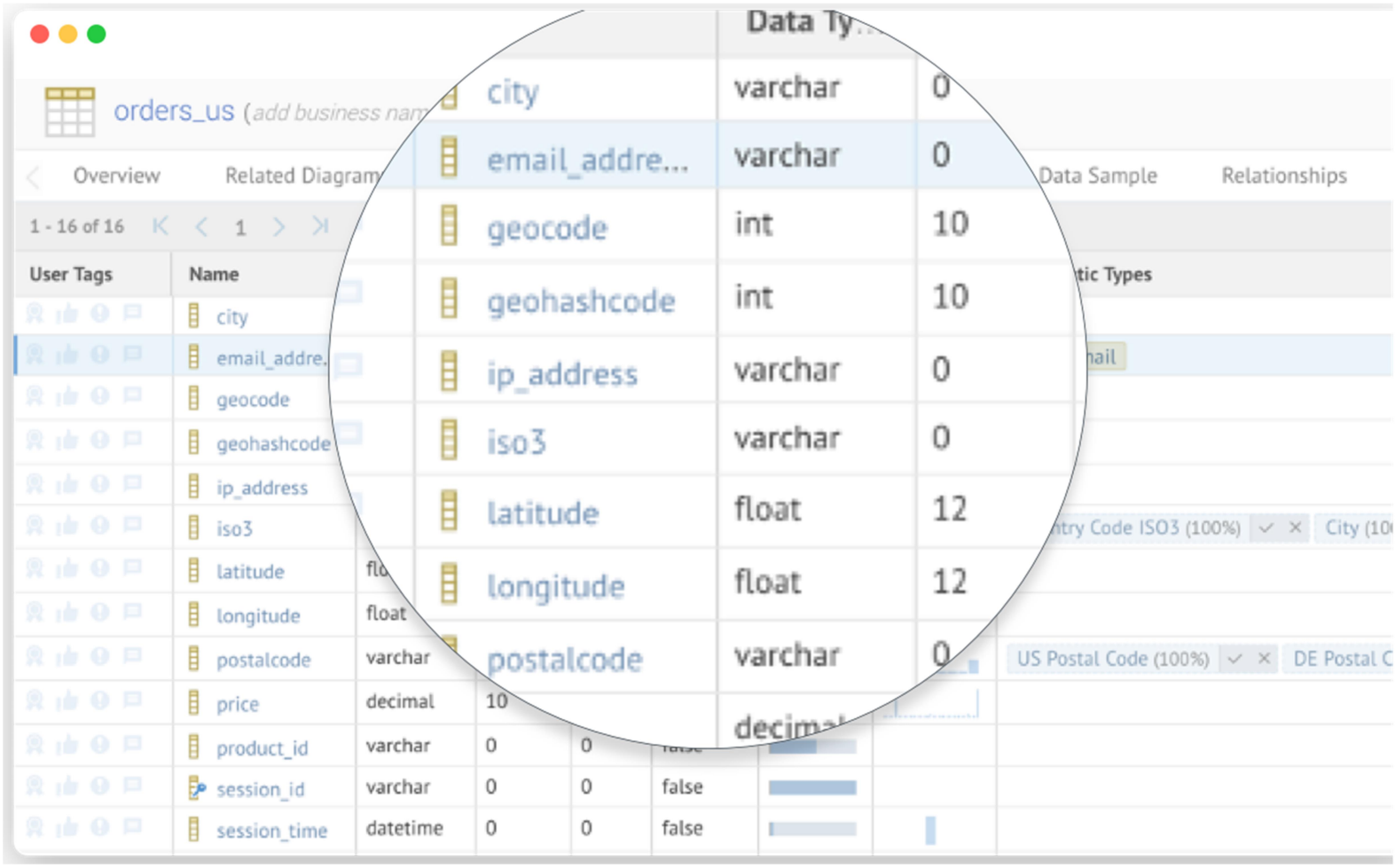
ASPECTS DE GOUVERNANCE

Le *Comité directeur de la gestion des données* dicte les orientations en matière de gestion des normes utilisées dans le contexte d'utilisation secondaire des données. Il s'assure de la concordance de ces normes avec celles utilisées dans les systèmes d'information transactionnels. Il approuve la nomination d'une personne du Centre DORISE agissant en tant que spécialiste des normes.

Le *Comité de coordination de la gestion, de la qualité et de l'éthique* coordonne le processus d'examen des normes. Il propose des choix de normes et coordonne leur application.

Le centre DORISE, en collaboration avec les détenteurs de données et autres partenaires, recense et répertorie les normes de l'établissement et les systèmes dans lesquels elles s'appliquent. Il rend disponible le répertoire des normes aux utilisateurs de données. Il coordonne la mise en œuvre des normes choisies dans le contexte d'utilisation secondaire des données.

Le spécialiste des normes du Centre DORISE travaille directement avec les directions concernées afin de les aider à choisir les normes les plus pertinentes. Il contribue aussi à restreindre ou étendre les normes en vue de les adapter aux divers contextes d'utilisation qui se présentent dans l'établissement.



Publié par : ZDNet. 2022

CHAPITRE 4.2 – QUALITÉ DES DONNÉES

ENJEUX DE QUALITÉ DES DONNÉES

Les enjeux de qualité des données sont très élevés dans une organisation comme le CIUSSS de l'Estrie – CHUS, principalement parce que les données collectées sont nombreuses, diversifiées et proviennent d'une grande quantité de systèmes d'information différents répartis dans l'ensemble de ses installations. De plus, les personnes qui collectent les données ont des profils différents. Elles ont leur propre vision de la qualité, soutiennent des activités diverses et répondent à des objectifs propres à leur environnement de travail. Les enjeux de qualité couvrent plusieurs perspectives d'ordre technologique, humain et organisationnel, ce qui rend leur gestion complexe, et à chacune de ces perspectives se rattachent des dimensions de la qualité.

La mise en place d'un programme de gestion de la qualité des données bien adapté à la réalité de l'organisation est une manière de traiter les enjeux de qualité. Les efforts en la matière visent à s'assurer que :

- Les données sont utilisées de façon harmonisée à tous les niveaux de l'organisation;
- Les utilisateurs de données travaillent avec des données pertinentes, précises, complètes, valides, exactes, crédibles, cohérentes et actuelles ;
- Les informations générées sont fiables pour la prise de décision éclairée et la gestion des activités cliniques, administratives et universitaires.

PROGRAMME DE GESTION DE LA QUALITÉ DES DONNÉES

En vertu de la stratégie de gestion des données, des activités fondamentales doivent assurer la qualité des données; de ces activités découle un programme de gestion de la qualité des données. Ce programme revêt les caractéristiques suivantes :

1. Il est transversal à l'organisation ;
2. Il s'adapte aux besoins variés de l'organisation ;
3. Il assure un même niveau de qualité partout dans l'organisation ;
4. Il facilite la mise en place de processus d'amélioration continue de la qualité ;
5. Il permet d'instaurer une culture de la qualité des données à travers l'organisation.

VISION

La vision du programme de gestion de la qualité des données au CIUSSS de l'Estrie – CHUS est :

Les données sont de la meilleure qualité possible tout au long de leur cycle de vie.

Cette vision renforce celle de la Stratégie de gestion des données et cadre avec l'objectif de l'un des trois moteurs opérationnels :

Assurer la qualité des données de leur collecte jusqu'à leur exploitation par les utilisateurs.

Le cycle de vie des données présenté dans la Stratégie de gestion des données de l'organisation comprend sept étapes fondamentales qui nous interpellent sur le plan de la qualité. Elles font référence non seulement aux données elles-mêmes, mais aussi aux systèmes d'information qui les capturent, les hébergent et les rendent disponibles.

PRINCIPES DIRECTEURS

1. La qualité des données est garantie à leur collecte, automatique ou manuelle, dans les systèmes d'information sources.
2. L'analyse de données de qualité est garante d'une bonne prise de décision et de résultats fiables.
3. La qualité des données est une préoccupation à tous les niveaux de l'organisation.
4. Les utilisateurs de données, qu'ils soient des cliniciens, des gestionnaires, des chercheurs ou autres, ont un niveau de confiance élevé dans la qualité des données qu'ils utilisent, transforment ou exploitent.

OBJECTIFS

1. Développer une approche de gestion qui rend les données conformes aux besoins et exigences des utilisateurs ;
2. Définir des normes, exigences et spécifications visant le contrôle de la qualité des données durant tout leur cycle de vie ;
3. Définir et appliquer des processus de mesure, de monitorage et de reddition de compte des niveaux de qualité des données ;
4. Identifier et encourager les opportunités d'améliorer la qualité des données soit par des processus de gestion ou des activités d'amélioration des systèmes d'information.

CADRE DE QUALITÉ DES DONNÉES

Miser sur un cadre de qualité des données reconnu et éprouvé et l'adapter à la réalité de l'organisation facilite la mise en œuvre d'un programme de gestion de la qualité des données. En effet, le cadre de qualité établit les grandes phases de transformation des données en information et regroupe les activités à réaliser dans chacune de ces phases.

Le cadre est à la fois un outil de gestion qui établit les fondements des processus de gestion de la qualité et un outil de communication qui encourage l'implication des parties prenantes tout au long de la mise en œuvre du programme.

Le cadre propose un certain nombre de processus de gestion de la qualité des données à mettre en place. D'autres processus jugés importants par l'établissement peuvent s'ajouter aux processus du cadre ou même en remplacer certains, selon les priorités de l'établissement. La mise en œuvre de l'ensemble des processus choisis constitue la base d'un programme de gestion de la qualité des données.

L'adoption du programme de gestion de la qualité et du cadre qui le sous-tend est la responsabilité du *Comité directeur de la gestion des données*.

L'atteinte de la qualité des données et son maintien nécessitent :

- La mise en œuvre :

- D'indicateurs clés de la qualité pour mesurer des critères intrinsèques aux données elles-mêmes;
- Des critères de services liés à l'utilisation de ces données;
- Des critères de sécurité liés à l'ensemble du dispositif de gestion des données (évaluation/audit/validation, contrôle, révision, accès);

- L'allocation de ressources qui assurent la mise en œuvre et le suivi des activités convenues dans le cadre de qualité.

Processus de gestion de la qualité des données

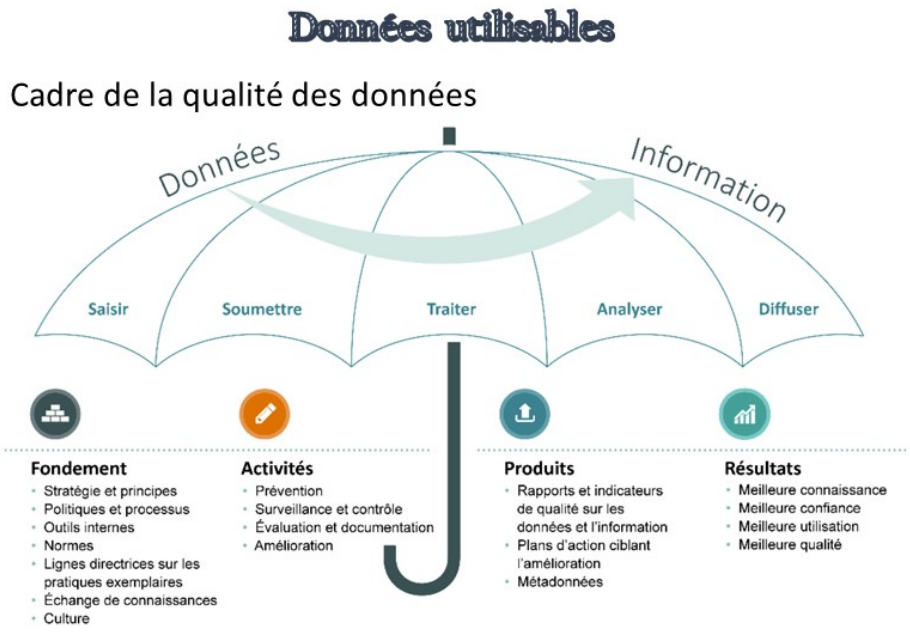


Figure 21 – Aspects de la gestion des données selon le cadre de l'ICIS.
Le cadre comprend le processus de transformation des données en informations, c'est le cycle de vie de l'information. Il comprend aussi quatre aspects de la gestion de la qualité des données applicables à leur cycle de transformation (voir Annexe J).

Le cadre de qualité des données retenu par le CIUSSS de l'Estrie-CHUS est celui de l'Institut canadien de l'information de la santé (ICIS). Il est celui qui se rapproche le plus près du domaine de la santé et qui reflète davantage le fonctionnement d'un établissement de santé.

Comme le montre la Figure 21, le cadre de l'ICIS suggère un cycle de vie de l'information en cinq étapes pour transformer les données en information. Le cadre présente aussi quatre aspects de la gestion de la qualité des données au cours du cycle de transformation : Fondement, Activités, Produits et Résultats.

Pour arriver à transformer les données en information(s), des actions doivent être mises en place à chaque étape du cycle de vie de l'information. Le tableau qui suit définit les étapes de transformation.

Nom de l'étape	Signification
Saisir	Collecter les données, manuellement ou automatiquement, durant la prestation des soins et services. Les personnes collectant les données jouent un rôle fondamental d'assurance de la qualité des données et de conformité aux normes de l'établissement.
Soumettre	Chargement sécuritaire des données provenant de multiples systèmes d'information sources dans des banques physiques ou virtuelles tout en maintenant l'intégrité et la confidentialité des données durant le transfert.
Traiter	Préparer les données chargées pour des fins d'analyse en les vérifiant, les nettoyant, les transformant au besoin et/ou les agrégeant.
Analyser	Effectuer l'analyse des données pour la génération de produits répondant aux besoins des utilisateurs de données, comme des tableaux de bords et des rapports. Les outils d'analyse sont choisis avec soin dans la perspective de partager les produits générés. À cette étape, les données traitées peuvent être rendues disponibles à des spécialistes pour analyse avec leurs propres outils spécifiques.
Diffuser	Produire et distribuer des produits d'information dont se servent les utilisateurs de données du CIUSSS de l'Estrie – CHUS. Cette étape inclut : (a) la publication, communication et promotion des résultats d'analyse (b) la formation des utilisateurs de données à comprendre l'information produite (c) le soutien des utilisateurs de données à accroître leur capacité à utiliser les données et les analyses dans leur travail journalier.

Le cadre de gestion de la qualité comprend les actions les plus déterminantes, choisies par l'équipe de rédaction, qui répondent aux différentes significations mentionnées dans le tableau.

Dimensions de la qualité des données

Mesurer le niveau de qualité des données aide une organisation à repérer d'éventuelles erreurs qui doivent être corrigées, et à évaluer si les données présentes dans ses systèmes informatiques sont adaptées à ses besoins. Pour y arriver, il importe d'identifier des critères définissant la qualité. Ces critères sont appelés « dimensions de la qualité ». Elles servent à mesurer la qualité en portant un jugement objectif ou subjectif selon la dimension choisie.

Les dimensions de la qualité sélectionnées proviennent d'une étude exhaustive des cadres de qualité qui ont été consultés (voir la liste à l'annexe K). Elles sont détaillées à l'annexe L. Ces dimensions sont considérées comme celles qui reflètent le plus le fonctionnement interne de l'établissement. La représentation du modèle provient du Cadre de la qualité SISMACQ de l'Institut national de la santé publique du Québec (INSPQ).

Ainsi, le cadre adopté comprend quatre grandes dimensions d'égale importance pour évaluer la qualité des données, soit **l'exactitude, la cohérence, la conformité et l'utilisabilité**, comme le montre la Figure 22.

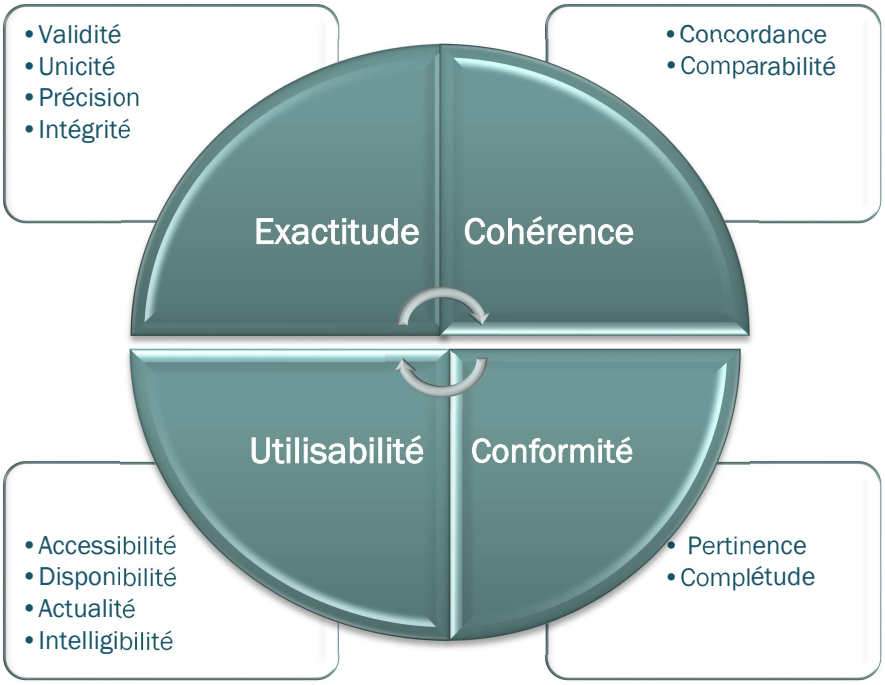


Figure 22 – Cadre de qualité des données adopté par le CIUSSS de l'Estrie – CHUS.

Le cadre de qualité comprend quatre grandes dimensions : l'exactitude, la cohérence, la conformité et l'utilisabilité. Chaque dimension possède sa propre définition qui fait ressortir des caractéristiques distinctives, listées dans les encadrés, desquels sont produits des indicateurs.

La première dimension (Exactitude) réfère aux critères intrinsèques des données d'un jeu de données ou d'une seule banque de données. La seconde (Cohérence) réfère à la combinaison ou l'agrégation de données provenant de sources diverses. La troisième (Conformité) réfère à la capacité de répondre au besoin de l'utilisateur. La quatrième dimension (Utilisabilité) réfère à la facilité avec laquelle les données peuvent être utilisées par l'utilisateur. Ces dimensions ne sont pas indépendantes – les unes réfèrent aux autres et c'est l'ensemble de ces dimensions qui assure la qualité des données utilisées par un utilisateur.

Les dimensions de la qualité procurent une façon de mesurer et de gérer la qualité des données et des informations contenues dans les actifs informationnels. Elles permettent de classer les données et de définir le niveau de qualité que l'établissement souhaite obtenir. Ce niveau de qualité est défini par le *Comité de gestion et d'assurance qualité des données* et adopté par le *Comité de coordination de la gestion, de la qualité et de l'éthique*. Toute modification au cadre de qualité ou changement de dimension de la qualité doivent être approuvés par le *Comité directeur de la gestion des données*.

Chaque grande dimension est évaluée à partir de caractéristiques ciblées à partir desquelles sont définis des indicateurs de qualité. D'autres caractéristiques peuvent s'ajouter à celles du cadre ou même les remplacer, selon les priorités et l'organisation interne de l'établissement. Ces caractéristiques se déclinent en indicateurs qui permettront la mesure. Pour plus d'informations, voir les cadres de gestion concernés.

GOUVERNANCE DE LA QUALITÉ

COMITÉ DIRECTEUR DE LA GESTION DES DONNÉES

Ce comité agit sur le plan stratégique :

- Il prend en charge la responsabilité de la gestion transversale de la qualité des données;
- Il adopte le programme de gestion de la qualité, approuve toute modification et soutient sa mise en œuvre;
- Il adopte le cadre de qualité et ses dimensions, et approuve toute modification
- Il communique la vision de la gestion de la qualité des données, voit à l'application des principes directeurs et établit les stratégies visant l'atteinte des objectifs de gestion de la qualité des donnés;
- Il répond au PDG de l'établissement qui est l'ultime responsable de la qualité des données produites par l'établissement.

COMITÉ DE COORDINATION DE LA GESTION, DE LA QUALITÉ ET DE L'ÉTHIQUE

Ce comité agit sur le plan tactique :

- Il voit à l'application des règles de qualité des données à travers l'organisation;
- Il élabore le programme de gestion de la qualité des données et identifie les moyens les plus efficaces d'assurer la meilleure qualité des données;
- Il adopte le niveau de qualité que l'établissement souhaite obtenir, tel que proposé par le *Comité de gestion et d'assurance qualité des données*;
- Il approuve les plans d'action qui lui sont présentés;
- Il assure le suivi des indicateurs de qualité et propose des solutions dans les situations problématiques;
- Il soutient les activités de supervision du *Comité de gestion et d'assurance qualité des données*.

COMITÉ DE GESTION ET D'ASSURANCE QUALITÉ DES DONNÉES

Ce comité agit sur le plan opérationnel :

- Il assure le suivi de la mise en œuvre du programme de gestion de la qualité des données;
- Il élabore les plans d'action et assure le suivi des activités de gestion de la qualité effectuées au Centre DORISE et dans les directions détentrices de systèmes sources ou de banques de données (pilotes de systèmes);
- Il définit le niveau de qualité que l'établissement souhaite obtenir;
- Il construit le tableau de bord de la qualité à partir des indications du *Comité de coordination de la gestion, de la qualité et de l'éthique*;
- Il s'assure que des mécanismes de mise à jour et de correction des données sont mis en place;

- Il suit l'évolution des indicateurs de la qualité des données et intervient dans les situations problématiques ou escalade la problématique au *Comité de coordination de la gestion, de la qualité et de l'éthique*;
- Il détermine les processus de validation du respect des règles de qualité des données et de correction lorsque des données erronées sont détectées.

CENTRE DORISE

Le Centre DORISE joue un rôle prépondérant dans l'utilisation secondaire des données. Entre autres, il assure le profilage des données et contrôle le processus ETL menant à la création des jeux de données. Le centre occupe une position de choix dans le constat du niveau de qualité des données qu'il exploite.

En gestion de la qualité, le centre :

- Met en œuvre le programme de gestion de la qualité des données;
- Contribue à la réalisation des plans d'action élaborés par le *Comité de gestion et d'assurance qualité des données*;
- Met à jour le tableau de bord de suivi de la qualité;
- Effectue des analyses de la qualité et réalise des audits;
- Collabore avec les pilotes de systèmes qu'il soutient dans l'application des processus de gestion de la qualité et dans la résolution de cas plus problématiques.

PILOTES DE SYSTÈMES

Les pilotes de systèmes s'assurent que les données collectées dans les systèmes sources sous leur responsabilité sont de la meilleure qualité possible :

- Ils valident la qualité des données de leur système source et effectuent les corrections des données invalides;
- Ils réalisent des audits internes dans les systèmes sous leur responsabilité;
- Ils fournissent les informations à intégrer dans le tableau de bord de suivi de la qualité.
- D'autres responsabilités leur incombent :
    - L'application du cadre normatif existant, ou, s'il n'en existe pas, la collaboration au développement d'un cadre normatif pour chacun des systèmes sources dont ils sont responsables;
    - La formation et le soutien des professionnels qui collectent des données dans les systèmes sources;
    - La conception de rapport de validation de la qualité périodique pour chacun des systèmes sources dont ils ont la responsabilité et la soumission des rapports au Centre DORISE;
    - La correction des erreurs et la rétroaction aux professionnels qui ont collecté les données ayant subi une correction;
    - La validation de la saisie des données (champs valideurs);
    - Le suivi de la qualité à partir d'indicateurs de qualité.

Publié par : ZDNet. 2022

CONCLUSION

RETOUR SUR LE DOCUMENT

Le présent document comprend beaucoup d'informations qui dépassent la gouvernance. Les principes directeurs qu'il énonce, les modèles et mécanismes de gestion qu'il présente, ainsi que les programmes et processus qu'il suggère, sont des outils pour les équipes de rédaction des cadres de gestion qui soutiendront la gouvernance sur les plans tactique et opérationnel.

Ce cadre de gouvernance est intimement lié à la *Stratégie de gestion des données* de l'établissement. Il soutient cette dernière en proposant une structure de gouvernance centralisée qui façonne la gestion des données dans toute l'organisation. Il présente les principaux mécanismes de gouvernance à mettre en place pour assurer la saine gestion des données de l'établissement.

Le point d'ancrage de ce document est le respect de la vie privée des usagers et des membres du personnel du CIUSSS de l'Estrie – CHUS. Son moteur est l'utilisation sécuritaire, confidentielle, éthique et transparente de données normées et de qualité, ainsi que la protection des renseignements personnels et des renseignements de santé ou de services sociaux. Son action repose sur l'accès autorisé aux données, l'engagement des personnes à respecter les règles d'utilisation des données et l'adoption d'une culture axée sur les données.

VISION DU FUTUR

Le futur est déjà en marche, un futur dans lequel la gestion de la performance, de la qualité et de la fluidité des soins, ainsi que la gestion de la recherche et de l'innovation, reposeront essentiellement sur l'analyse des données et l'intelligence artificielle.

Les établissements de santé qui ont emprunté le virage numérique devront miser sur un centre d'analyse des données performant doté des outils les plus modernes, ainsi que d'un écosystème d'analyse des données dernier cri. Des spécialistes qui détiennent une expertise en science des données, en ingénierie des données et en analyse des données constitueront les pivots de ce centre.

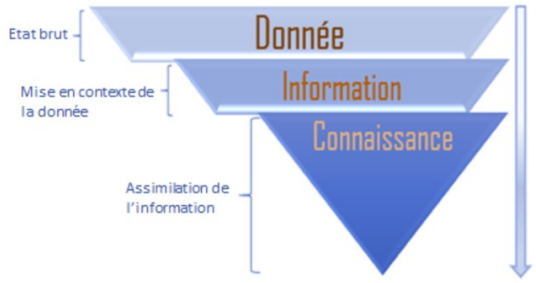
Les politiques, règlements et directives, ainsi que les cadres légaux continueront d'évoluer, et viendra le jour où l'analyse des données sera une seconde nature pour toute organisation consciencieuse qui souhaite continuer d'améliorer ses façons de faire et de tendre vers l'excellence.

ANNEXE A – DÉFINITIONS

Définition d'une donnée

Il existe de nombreuses définitions du terme « donnée ». La définition que nous avons retenue permet aussi de définir ce qu'est une information et comment est générée la connaissance[42].

Processus de transformation d'une donnée en connaissance



Une donnée est un résultat d'une observation ou d'une expérience faite délibérément[43]. La donnée est brute. Elle n'a pas de sens, si elle n'est pas mise en contexte. Elle est inconséquente en soi, elle n'apporte rien. Elle est le plus bas niveau du processus de transformation vers la connaissance.

La mise en contexte d'une donnée génère une information. Lorsqu'elle est basée sur des faits véritables, elle devient une information fiable.

Lorsque l'information est assimilée et comprise, elle génère la connaissance. C'est cette dernière qui éclaire nos actions et nos décisions.

Types de données

La littérature foisonne d'information concernant les différents types de données et leur définition. Parfois, un même type de données peut avoir différentes nomenclatures. De telles différences relèvent la plupart du temps de la sémantique et de la culture. Dans cette annexe, nous allons nous concentrer sur les types de données que le CIUSSS de l'Estrie – CHUS utilise tout au long de ses activités. Les définitions utilisées ici sont inspirées de plusieurs documents, dont le Projet de Loi 3 : Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives, le *Règlement général sur la protection des données - RGPD (Règlement (UE) 2016/679* du Parlement européen (https://www.cnil.fr/fr/reglement-europeen-protection-donnees)) et la *Loi 25.* Dans cette annexe, le terme « renseignement » est remplacé par le terme « donnée ».

> *Données liées aux activités opérationnelles*

Dans le cadre de ses activités opérationnelles, le CIUSSS de l'Estrie – CHUS collecte trois catégories de données : 1) des données de santé ou de services sociaux, 2) des données personnelles et 3) des données non personnelles. Ces dernières peuvent être des données de gestion, financières, technologiques, démographiques, statistiques, etc.

5. **Une donnée de santé ou de services sociaux**, tel que défini par le Projet de loi 3, est toute donnée détenue par un organisme du secteur de la santé et des services sociaux qui est liée à une personne. Cette donnée peut permettre ou non d'identifier la personne et elle répond à l'une des caractéristiques suivantes :
    - Elle concerne l'état de santé physique ou mentale de cette personne et ses facteurs déterminants, y compris ses antécédents médicaux ou familiaux;
    - Elle concerne tout matériel prélevé dans le cadre d'une évaluation ou d'un traitement, incluant le matériel biologique, ainsi que tout implant, orthèse, prothèse ou autre aide suppléant à une incapacité de cette personne;

[42] Processus de transformation d'une donnée en connaissance est tiré de DataTame.fr

[43] Tiré du dictionnaire Larousse.

- Elle concerne les services de santé ou les services sociaux offerts à cette personne, notamment la nature de ces services, leurs résultats, les lieux où ils ont été offerts et l'identité des personnes ou des organismes qui les ont offerts;
- Elle a été obtenue dans l'exercice d'une fonction prévue par la *Loi sur la santé publique* (chapitre S-2.2);
- Elle comprend toute autre caractéristique déterminée par règlement du gouvernement;
- Elle permet l'identification d'une personne (nom, prénom, date de naissance, coordonnées, numéro d'assurance maladie, toute autre donnée de même nature)[44].

À noter que la dernière caractéristique de cette liste cadre avec la définition d'une donnée personnelle, tel que décrit ci-dessous. En d'autres termes, le PL-3 considère qu'une donnée personnelle est aussi une donnée de santé et de services sociaux.

6. **Une donnée personnelle** est toute donnée qui concerne une personne et qui permet de l'identifier directement ou indirectement. Une donnée personnelle peut correspondre aux noms, prénoms, adresses (physique et électronique), numéro de téléphone, lieu et date de naissance, numéro de sécurité sociale, numéro d'assurance maladie, sexe, profession unique, code postal, plaque d'immatriculation d'un véhicule, photo, empreinte digitale, ADN, facteurs spécifiques aux aspects physique, physiologique ou mental, identité économique, culturelle ou sociale, et autres.

   Toute donnée qui permet d'identifier directement une personne est appelée **donnée d'identification directe** ou **identifiant direct**. Des exemples sont : le nom, le prénom, l'adresse courriel, le numéro d'assurance sociale et le numéro d'assurance maladie.

   Aussi, toute donnée qui peut vraisemblablement permettre d'identifier une personne par le biais d'une combinaison de plusieurs données, par exemple l'âge, le sexe, la date de naissance, le lieu de résidence et des caractéristiques personnelles distinctives, est appelée **donnée d'identification indirecte** ou **identifiant indirect**.

7. **Une donnée non personnelle** est une donnée qui n'est pas liée à une personne et qui ne permet pas de l'identifier lorsqu'utilisée seule ou en combinaison avec d'autres données accessibles. Ce type de donnée est aussi appelé **une donnée non identificatoire**[45].

Sensibilité des données

Les données personnelles et de santé ou services sociaux sont qualifiées de **données sensibles**. Elles suscitent un haut degré d'attente raisonnable en matière de vie privée, à cause de leur nature ou en raison du contexte de leur utilisation ou de leur communication[46]. Le degré de sensibilité d'une donnée est qualitatif et dépend d'une foule de facteurs et du contexte d'utilisation. Par exemple, certaines données, dont en particulier le numéro de sécurité sociale ou les données biométriques (empreinte digitale, échantillon ADN, etc.), sont qualifiées de particulièrement sensibles, car leur croisement permet de raccorder assez facilement différents fichiers de données entre eux et d'opérer leur interconnexion, résultant en l'identification des personnes. Il est plus difficile d'y arriver avec des données qualifiées de moins sensibles, comme l'origine raciale ou ethnique, le statut d'immigration, les opinions politiques, les convictions religieuses ou

[44] PL-3 : Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives, art. 2.

[45] Groupe en éthique de la recherche, EPTC 2 (2018) – Chapitre 5 : Respect de la vie privée et confidentialité, Gouvernement du Canada.

[46] Loi-25, art. 12.

philosophiques, l'affiliation syndicale ou à d'autres autres organismes d'intérêt. D'autres données sensibles mentionnées dans le PL-3 sont :

1. Les données génétiques;
2. Les données d'adoption;
3. Les données sur les infractions ou condamnations;
4. Les données pouvant révéler certaines informations qui socialement peuvent soulever la controverse (IVG, VIH, aide médicale à mourir etc.).

Données liées aux activités d'exploitation

Les données collectées durant les activités opérationnelles de l'établissement sont aussi utilisées pour être exploitées à des fins de recherche, de gestion, d'enseignement et d'évaluation. Dans ce contexte particulier d'utilisation, ces mêmes données sont classées différemment. On y retrouve les données brutes et les données dérivées. Les données brutes peuvent être transformées et organisées de manière à réduire, voire éliminer, les risques d'identifier les personnes. Selon la technique utilisée, les données sont dites anonymisées ou dépersonnalisées. Enfin, les données peuvent aussi être agrégées.

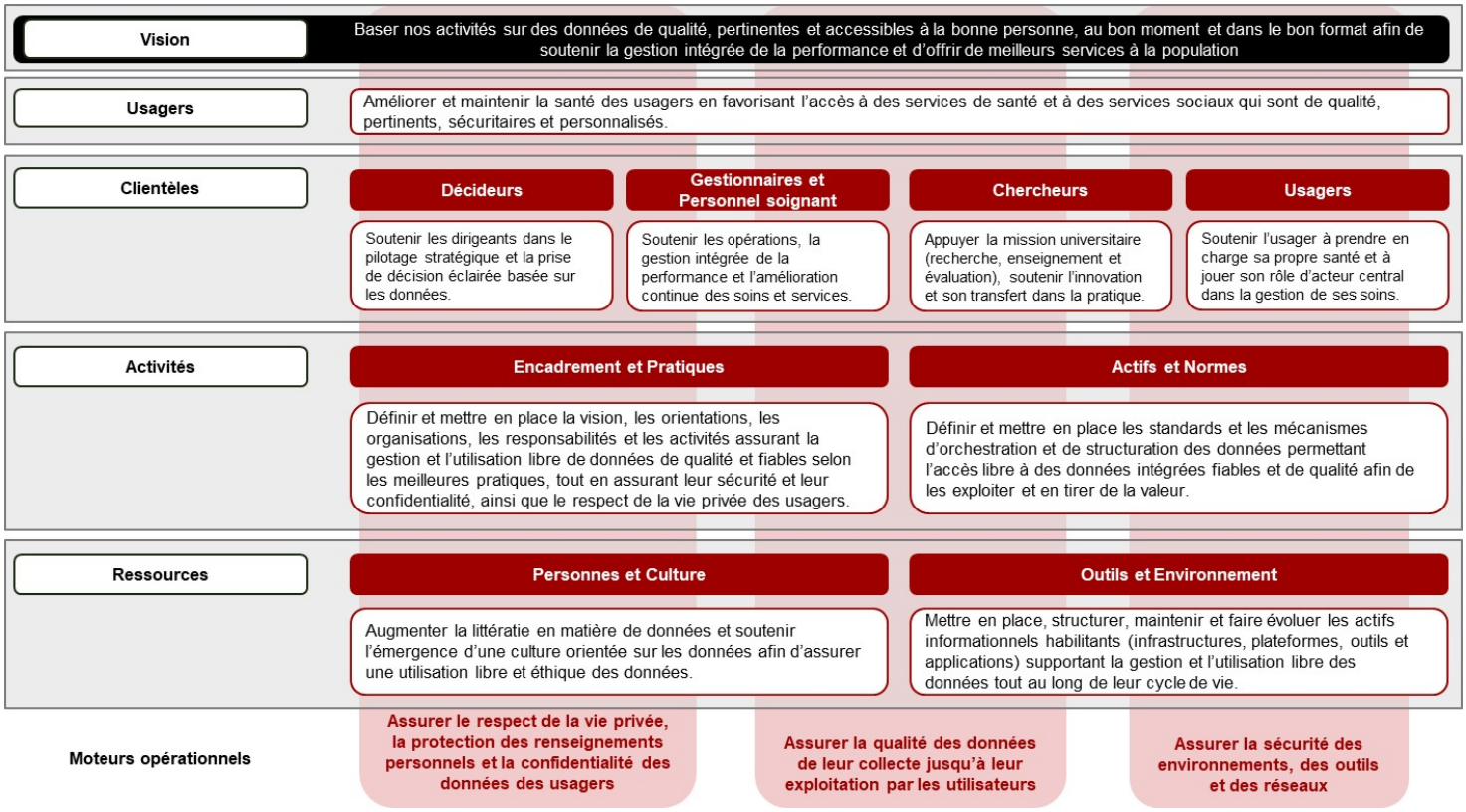
1. **Une donnée brute** est toute donnée qui n'a subi aucune transformation depuis sa collecte dans les systèmes d'information sources. Elle est exploitée telle quelle.
2. **Une donnée dérivée** est toute donnée générée à la suite de l'application sur un groupe de données brutes d'une formule, d'un algorithme de calcul ou de tout autre type d'agrégation, de rapports ou d'analyse. Par exemple, l'indice de masse corporelle est une donnée dérivée d'une formule appliquée sur deux données brutes : le poids et la taille d'une personne.
3. **Une donnée anonymisée** est toute donnée dont tous les identifiants directs sont irrévocablement retirés et pour lesquels aucun code permettant une réidentification ultérieure n'est conservé. Des techniques sont utilisées sur les identifiants indirects restants de manière à minimiser le risque de réidentification de la personne. Ce processus est irréversible et rend anonyme une donnée personnelle[47].
4. **Une donnée dépersonnalisée** est toute donnée dont les identifiants directs ont été retirés et remplacés par un code. Si la liste de correspondance entre le code désigné et le vrai nom de la personne est accessible, il est possible de réidentifier la personne. Le code peut être une série de chiffres ou une série de lettres et symboles ou encore un mélange des deux. Ce processus est réversible et dépersonnalise une donnée personnelle.
5. **Une donnée agrégée** est toute donnée qui est le résultat d'une combinaison de données individuelles présenté comme un tout.

[47] Loi 25, art. 28.

ANNEXE B – STRATÉGIE DE GESTION DES DONNÉES

TABLEAU SYNOPTIQUE

Tableau synoptique de la Stratégie de gestion des données du CIUSSS de l'Estrie – CHUS.



ANNEXE C – GOUVERNANCE DES DONNÉES

Comités prévus par la Loi

Comité d'éthique de la recherche

Le *Comité d'éthique de la recherche* (CÉR) du CIUSSS de l'Estrie – CHUS est un comité désigné par le ministre de la Santé et des Services sociaux. Son mandat est d'évaluer les projets relevant de l'article 21 du Code civil du Québec (ci-après C.c.Q.). Le CÉR a l'obligation de se conformer aux exigences édictées par le *Plan d'action ministériel en éthique de la recherche et en intégrité scientifique* (1998) (ci-après PAM) et de rendre des comptes annuellement au ministère de la Santé et des Services sociaux (MSSS). Son rôle est d'appliquer la politique interne d'éthique à la recherche. Son mode de fonctionnement est décrit dans le Règlement sur le Comité d'éthique de la recherche du Centre universitaire intégré de santé et des services sociaux de l'Estrie – Centre hospitalier universitaire de Sherbrooke.

Le CÉR relève directement du Conseil d'administration. La Direction de la coordination de la mission universitaire (DCMU) assume la responsabilité du processus d'évaluation des projets de recherche, collabore avec le CÉR et le soutient dans son mandat.

Comité sur la sécurité de l'information

Selon la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LGGRI), c'est le PDG qui est responsable de préserver la sécurité de l'information dans son établissement de santé. Le terme sécurité revêt trois grandes composantes : la disponibilité, l'intégrité et la confidentialité de l'information collectée et gérée par l'établissement. À l'interne du CIUSSS de l'Estrie – CHUS, ces responsabilités sont déléguées à la présidence-direction générale adjointe (PDGA). Au lieu de mettre en place un *Comité sur la sécurité de l'information*, tel que prescrit par la LGGRI, la PDGA a mandaté le *Comité de coordination de la sécurité, de l'accès et de la protection des renseignements personnels* pour assumer les fonctions du Comité sur la sécurité de l'information au sein de la gouvernance des données.

Comité sur l'accès à l'information et sur la protection des renseignements personnels

Au sens de la *Loi 25*, c'est le PDG de l'établissement qui veille à assurer le respect et la mise en œuvre des obligations de ladite loi. Il peut en déléguer la responsabilité à un cadre de son établissement. Au lieu de mettre en place un *Comité sur l'accès à l'information et sur la PRP*, tel que prescrit par la *Loi 25*, le PDG a mandaté le *Comité de coordination de la sécurité, de l'accès et de la PRP* pour assumer les fonctions du *Comité sur l'accès à l'information et sur la PRP* au sein de la gouvernance des données.

Font partie de ce Comité le responsable de l'accès aux documents, le responsable de la protection des renseignements personnels, le responsable de la sécurité de l'information (RSI) et le responsable de la gestion documentaire.

Comités de la gouvernance

Comité directeur de la gestion des données

La responsabilité de la gestion des données de l'établissement est confiée à la Présidence-direction générale adjointe. Sous l'autorité du PDGA, le *Comité stratégique de la mission universitaire* (CSMU) assume le mandat du *Comité directeur de la gestion des données*.

Le comité se concentre sur les différents aspects stratégiques de la gouvernance des données, dont la supervision des travaux de mise en œuvre du plan d'action de la Stratégie de gestion des données du CIUSSS de l'Estrie – CHUS et le pilotage des activités qui en découle.

Plus spécifiquement, le comité :

- Approuve le plan de communication de la Stratégie de gestion des données et le soutient de manière à assurer l'adoption de la stratégie par la communauté du CIUSSS;
- Supervise l'élaboration du Cadre de gouvernance des données ainsi que les cadres de gestion qui l'accompagnent et il voit à leur évolution;
- Élabore des stratégies et approuve des plans de mise en œuvre et des plans de mitigation des risques;
- Supervise l'élaboration d'ententes et contrats de partage des données avec des partenaires publics ou privés, des consultants ou fournisseurs, et les approuve;
- Recommande les actions à tenir en cas de manquement à la Politique et au Cadre de gestion de la sécurité de l'information ainsi qu'au Cadre de gouvernance des données;
- Assure la mise en place des mécanismes de suivi des différents comités et en fait rapport aux hautes instances de l'établissement.

Les activités du comité touchent non seulement la gestion globale des données et de l'information de l'établissement, mais aussi l'ensemble des systèmes d'information qui y sont rattachés. Le comité s'assure que toutes les parties prenantes de la communauté du CIUSSS de l'Estrie – CHUS comprennent bien leurs rôles et responsabilités en matière de gestion des données et des systèmes.

> *Composition du comité*

Président du Comité : Directrice de la DCMU et le Président-directeur général adjoint (PDGA) concernant le mandat de Comité directeur de gestion des données.

Membres du comité : Les membres de ce comité sont ceux du Comité stratégique de la mission universitaire (CSMU) du CIUSSS de l'Estrie – CHUS.

Comité de coordination de la gestion, de la qualité et de l'éthique des données

Le *Comité de coordination de la gestion, de la qualité et de l'éthique des données* convient de la mise en œuvre et du suivi des orientations ou décisions du *Comité directeur de la gestion des données dans* les domaines relevant de sa responsabilité et en fait rapport à ce dernier.

Il s'assure de l'application des différents cadres de gestion des données en lien avec ses responsabilités, notamment le cadre de gestion des métadonnées, celui de la gestion de la qualité des données ainsi que les politiques et procédures d'application qui les concernent. Il s'associe au CÉR pour toute demande d'exploitation des données par la recherche.

Il est l'instance qui s'assure de la gestion et du suivi des priorités de développement du Centre d'expertise en valorisation des données de santé du CIUSSS (DORISE) qui relève de la Direction de la qualité, de l'éthique, de la performance et du partenariat (DQEPP).

> *Composition du comité*

Président du comité **:** Directeur-adjoint de la DAPO de la DQEPP

Membres du comité :

- Directrice adjointe Soutien et qualité DSP,
- Directeur adjoint DRF,
- Directeur adjoint DRIT,
- Représentant du comité d'éthique de la recherche (CÉR),
- Représentant de la santé publique,
- Conseiller en gestion de données de santé,
- Représentant du secteur clinique santé et un du secteur clinique social.

Comité de coordination de la sécurité, de l'accès et de la protection des renseignements personnels

Le *Comité de coordination de la sécurité, de l'accès et de la protection des renseignements personnels* (PRP) coordonne la mise en œuvre et le suivi des orientations du *Comité directeur de la gestion des données* concernant ses responsabilités. Il assume les responsabilités légales du *Comité sur la sécurité de l'information*. Entre autres, il propose un plan d'action sur cinq (5) ans visant l'atteinte des objectifs de la politique interne sur la sécurité de l'information. Il assure le suivi des travaux en sécurité de l'information et fait rapport à la Présidence-direction générale (PDG) de l'établissement ainsi qu'au ministère de la Santé et des Services sociaux (MSSS). Il soutient et facilite les rôles et responsabilités de la structure fonctionnelle de la sécurité de l'information tels que décrits dans le Cadre de gestion de la sécurité de l'information de l'établissement. Il travaille en étroite collaboration avec le responsable de la sécurité de l'information (RSI), le conseiller en gestion de la sécurité de l'information (CGSI) et l'officier de sécurité de l'information (OSI) dans l'application de leurs mandats confiés par la Loi.

Le comité de coordination assume également les responsabilités du *Comité sur l'accès et la protection des renseignements personnels*. Il soutient le PDG dans l'exercice de ses responsabilités et dans l'exécution de ses obligations. En plus d'exercer les fonctions spécifiques qui lui sont confiées par ladite loi (Septembre 2022), il agit à titre de conseiller-expert et assume l'évaluation des facteurs relatifs à la vie privée dans tous les projets de l'établissement. Dans ce contexte, le comité doit être avisé de tout projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui recueille, utilise, conserve, communique et élimine des renseignements personnels. Il est aussi responsable d'établir la Politique de confidentialité et de rédiger le Cadre de gestion sur l'accès et la protection des renseignements personnels ainsi que d'en assurer le respect au quotidien. Il travaille en étroite collaboration avec le responsable de la PRP, le responsable de l'accès aux documents, le responsable de la gestion des risques dans l'application de leurs mandats confiés par la Loi.

Le comité de coordination joue également un rôle-conseil auprès des directions en matière d'accès aux documents, d'accès aux données de santé et de protection des renseignements personnels. Il

mobilise la communauté du CIUSSS de l'Estrie – CHUS à l'importance de la confidentialité et du respect de la vie privée tant pour l'utilisation primaire de l'information que secondaire. Il est responsable de l'application opérationnelle et du respect de l'ensemble des règles et exigences définies au Cadre de gouvernance des données ainsi qu'aux différents cadres de gestion traitant de la sécurité de l'information, des règles d'accès aux données administratives, de santé (clinique) et de la protection des renseignements personnels, d'accès aux documents, et ce, en application de la Loi.

> *Composition du comité*

Président du comité : Directeur adjoint, MU-SC-EO – PDGA

Membres du comité :

- Directrice adjointe Soutien Qualité DSP,
- Responsable de la sécurité de l'information (RSI) – PDGA,
- Coordonnatrice archives, accueil admission, DSP,
- Directeur adjoint des directions DCMU, DRIT, DRHCAJ et DRF,
- Directeur adjoint – qualité des directions DSM, DSI et DQEPP.

Comité de gestion et de l'assurance qualité des données

Le *Comité de gestion et de l'assurance qualité des données* assume le mandat opérationnel d'amélioration continue de la qualité des données. Il établit les critères de qualité et les mécanismes de gestion de la qualité, élabore le plan d'action annuel et met en place un tableau de bord de suivi de la qualité des données.

Il collabore avec les pilotes de systèmes à la validation des mécanismes de gestion des données des systèmes sources (compilation, traitement, exploitation) conformément aux règles internes de l'établissement. Il collabore aussi à la validation des différents cadres et directives ministériels. Il en évalue les impacts sur la gestion des données à tous les niveaux de l'organisation et recommande les correctifs nécessaires aux processus de saisie, de traitement et d'analyse des données.

> *Composition du comité*

Président du comité : Chef de service du centre DORISE

Membres du comité :

- Coordonnatrice accueil, admission et archives,
- Adjoint au directeur DRF,
- Gestionnaire représentant DSP,
- Gestionnaire représentant du secteur santé publique,
- Gestionnaire représentant DRIT,
- Gestionnaire représentant du secteur santé,
- Gestionnaire représentant du secteur services sociaux.

Détenteurs de l'information

Les détenteurs de l'information sont les directions du CIUSSS de l'Estrie – CHUS qui utilisent des systèmes d'information sources, soit pour collecter des informations ou pour les manipuler afin de soutenir les activités de l'établissement. Les détenteurs de l'information jouent un rôle primordial dans la gestion de l'information qu'ils colligent et qu'ils détiennent. Ils s'assurent que les données qu'ils détiennent dans leurs systèmes d'information sont sécuritaires, disponibles, intègres, de qualité et confidentielles. Ils sont responsables de l'application des différents cadres de gestion ou cadres normatifs par l'ensemble de leur personnel et doivent faire rapport aux deux comités de coordination, selon les responsabilités de chacun, des problématiques rencontrées. Ils travaillent en collaboration avec le Centre DORISE dans l'évolution des cadres de gestion et des cadres normatifs.

Contributeurs à la gouvernance

Centre de données organisées du réseau informatique de la santé de l'Estrie

L'intendance des données est la composante opérationnelle principale de la gouvernance de données. La gestion d'une importante quantité de données conservées dans les banques de l'organisation et utilisées pour diverses fins exige que l'intendance des données soit transversale à l'organisation et soit bien appliquée et comprise par toute la communauté du CIUSSS de l'Estrie – CHUS.

Au sein de la gouvernance des données de l'établissement, le Centre DORISE de la DQEPP est désigné comme l'intendant principal des données. À ce titre, il applique les règles et politiques à suivre durant tout le cycle de vie des données afin de fournir des données de qualité, en toute sécurité et confidentialité et en respect de la vie privée. Il assure la gestion transversale des données depuis leur collecte dans les systèmes sources, jusqu'à leur exploitation par les utilisateurs, en passant par leur chargement dans les banques, leur transformation, leur stockage et leur archivage et leur élimination. Il assume ainsi l'application sur le terrain du Cadre de gouvernance des données, en plus d'appliquer les différents cadres de gestion, notamment le Cadre normatif de l'anonymisation des données, le Cadre de gestion de la qualité des données, le Cadre de gestion intégré des risques, le Cadre de gestion des accès, le Cadre de gestion des métadonnées et le Cadre sur les pratiques organisationnelles sur l'analyse avancée des données. Il convient des moyens pour actualiser les orientations prises concernant la sécurité, la qualité et l'accès aux données. Il réalise les audits internes de conformité, émet les avis et met en place les changements requis.

Le centre DORISE est la porte d'accès aux données de l'établissement. Il gère les demandes d'accès aux données (évaluation de l'admissibilité et de la faisabilité des demandes en collaboration avec le comité d'éthique à la recherche ainsi que le suivi des projets d'accès aux données autorisés).

La mission du centre DORISE est :

> *Promouvoir et soutenir l'utilisation des données de santé, créer et diffuser la connaissance et contribuer au développement d'innovations en valorisation des données dans l'établissement*

Il exécute cette mission notamment en :

- Soutenant les utilisateurs à l'utilisation des données dans les domaines suivants : clinique, gestion, recherche, enseignement et évaluation;

- Développant et instaurant des outils susceptibles de contribuer au développement de pratiques exemplaires et à l'amélioration des pratiques actuelles basées sur des données probantes;
- Contribuant à la recherche, au développement et à l'innovation en gestion des données;
- Développant des méthodes d'analyse de données soutenant le développement et l'évolution de l'établissement.

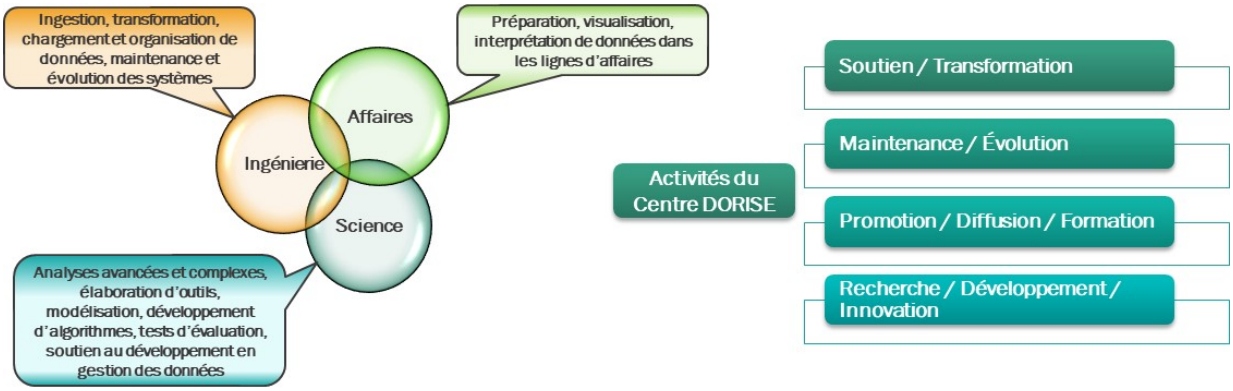


Figure 23 - Secteurs d'activités du centre DORISE

Le centre DORISE est composé d'un groupe d'experts regroupé dans trois secteurs névralgiques : l'intelligence d'affaires, l'ingénierie des données et des systèmes et la science. Ce dernier secteur contribue à soutenir la recherche, à développer des techniques de gestion des données et contribuer à l'innovation en gestion des données.

Directions contributrices

Plusieurs instances et directions du CIUSSS de l'Estrie – CHUS assument déjà des responsabilités en gestion de l'information et des systèmes. Une telle contribution permet d'assurer une gestion transversale des données et informations. Elle permet aussi d'augmenter les forces vives directement impliquées dans la gouvernance. Chacune d'entre elles collabore à sa manière en accomplissant certaines tâches que voici :

> *Conseil d'administration (CA)*

Responsable des plaintes en lien avec la violation de la confidentialité, via la commissaire aux plaintes;

Responsable de la gestion des risques majeurs de l'établissement tels qu'énoncés à la Politique sur la gestion intégrée des risques (E000–POL-03). Il agit sous recommandations du *Comité de vérification et de suivi budgétaire* (CVSB) et du *Comité de vigilance et de la qualité* (CVQ);

Responsable du *Comité d'éthique de la recherche*.

> *Présidence-direction générale adjointe (PDGA)*

Responsable de la Stratégie de gestion des données;

Préside le *Comité directeur de la gestion des données*;

Responsable du fonctionnement du *Comité de coordination de la sécurité de l'information, de l'accès et de la PRP* ainsi que du *Comité de coordination de la gestion des données, de la qualité et de l'éthique*;

Responsable de la sécurité de l'information;

Responsable de la gestion des risques liés aux données (fiches 44- 45);

Responsable de l'évolution de la Stratégie de gestion des données, du Cadre de gouvernance et des cadres de gestion afférents.

> *Direction de la qualité, éthique, performance et partenariat (DQEPP)*

- Responsable de l'intendance principale en gestion des données via son centre DORISE :
- Responsable de la gestion documentaire de l'établissement;
- Responsable de la gestion intégrée des risques;
- Responsable de l'éthique clinique et organisationnelle;
- Responsable de l'évaluation de la performance.

> *Direction de la coordination de la mission universitaire (DCMU)*

- Collabore et soutient le *Comité d'éthique de la recherche* (CÉR);
- Établit les ententes de collaboration avec les universités;
- Agit à titre de comité directeur via le *Comité stratégique de la mission universitaire* (CSMU).

> *Direction des services professionnels (DSP)*

- Responsable de la protection des renseignements personnels;
- Responsable de l'évaluation des facteurs de risque liés à la vie privée;
- Responsable de l'accès aux données et aux systèmes d'information clientèle;
- Responsable de l'accès aux données pour les fins d'étude, de recherche ou de statistiques.

> *Direction des ressources humaines, des communications et des affaires juridiques (DRHCAJ)*

- Coordination des communications;
- Coordination de la gestion du changement;
- Responsable de l'accès aux documents des organismes publics.

> *Direction des ressources financières (DRF)*

- Responsable du modèle de financement opérationnel;
- Responsable des ententes de partenariats économiques;
- Responsable de la Politique de propriété intellectuelle;
- Responsable du suivi de la gestion intégrée des risques;

- Responsable de la banque de données CPSS.
- Direction des ressources informationnelles et technologiques (DRIT)
- Responsable de la gestion des outils et de l'environnement des systèmes;
- Responsable de la sécurité des systèmes **:**

  Elle fournit et maintient en état la technologie et les moyens techniques de sécurité et s'assure de leur conformité aux besoins de sécurité déterminés par le Cadre de gestion de la sécurité des données et se tient à l'affut des meilleures pratiques en la matière.

> *Directions détentrices de données*

- S'assurent de l'application du Cadre de gouvernance des données et des différents cadres de gestion inhérents.

ANNEXE D – MODÈLE DE PRATIQUE DE LA PROTECTION DES DONNÉES

Modèle de pratique de la protection des renseignements personnels

Le modèle adopté par l'établissement est le *Modèle de pratique de la protection des renseignements personnels* version 1.1, publié par le gouvernement du Québec en 2009. Ce modèle vise à faciliter le respect des principes et obligations légales de la protection des renseignements personnels (PRP) lors des projets de développement faisant appel à des renseignements personnels. Il est un guide de référence pour concevoir un modèle adapté à l'ensemble des données confidentielles d'un établissement de santé comme le CIUSSS de l'Estrie – CHUS et définir les mesures à mettre en place pour assurer une saine gestion de la protection des données confidentielles.

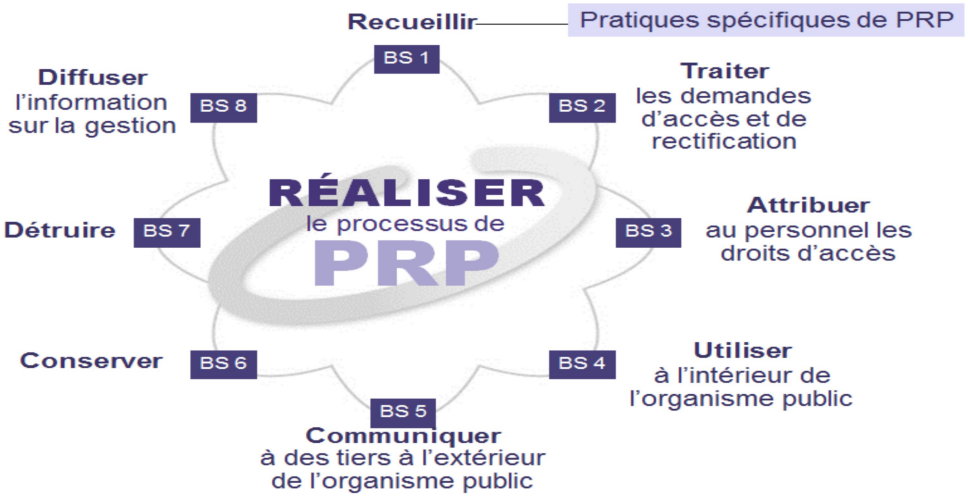


Figure 24 – Schéma du processus de gestion de la protection des renseignements personnels, partie 1 du modèle.

Le modèle comprend deux parties :

- La première partie permet d'établir la stratégie d'intégration du modèle dans l'établissement ou dans un projet de développement d'envergure. Elle comprend un processus de PRP qui vise l'atteinte de huit buts spécifiques (BS-1 à BS-8) en observant 24 pratiques spécifiques (PS-1.1 à PS-8.2).
- La seconde partie permet d'aborder l'intégration de la PRP dans les projets de développement selon une perspective de gestion. Elle comprend un processus de gestion qui vise l'atteinte de cinq buts de gestion (BG-1 à BG-5) en observant 17 pratiques de gestion (PG-1.1 à PG-5.2).

Brièvement, la partie 2 du modèle décrit, selon une approche d'amélioration continue, un ensemble de buts et de pratiques de gestion qu'un organisme public peut réaliser dans un projet particulier ou dans un ensemble de projets de développement. La PRP est abordée ici selon une perspective de gestion, soit la planification, l'organisation, le suivi et le contrôle du processus de PRP, tant à l'échelle d'un projet que de tous les projets de l'organisation. Elle propose un chemin à suivre pour faciliter l'intégration de la PRP dans la culture de l'organisation relativement aux projets de développement.

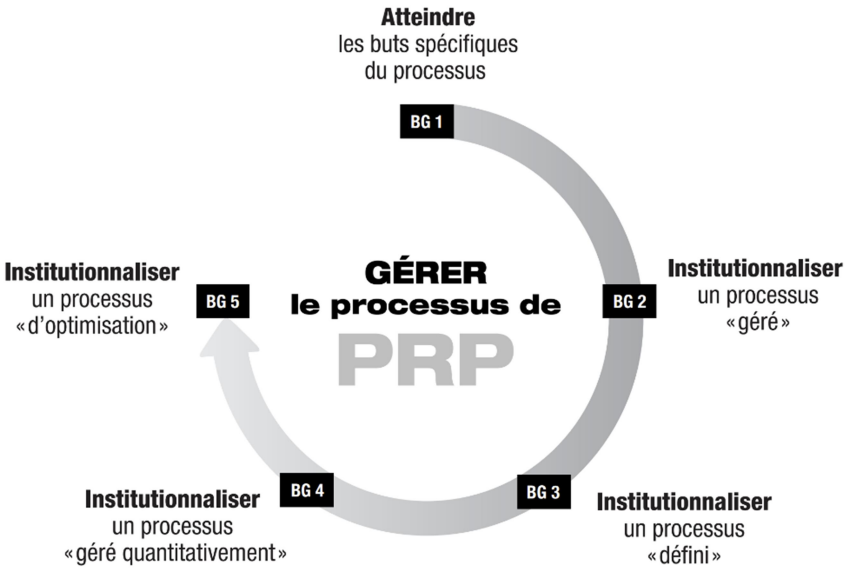


Figure 25 – Schéma du processus de gestion de la Protection des renseignements personnels, partie 2 du modèle.

Entre autres, elle permet :

- D'aborder l'intégration de la PRP dans les projets de développement selon une perspective de gestion;
- D'établir la stratégie d'intégration du modèle dans l'organisme public ou le projet;
- De prendre connaissance des composants du modèle qui ont trait à la gestion de la PRP;
- De déterminer les buts et les pratiques de gestion (de la PRP) à réaliser dans l'organisme ou le projet;
- De déterminer les rôles et les responsabilités des intervenants;
- De faire une lecture détaillée des buts et pratiques de gestion (de la PRP) pour comprendre les pratiques à réaliser et identifier les adaptations à faire selon la stratégie d'intégration retenue par l'organisme public.

Dans le présent document, nous nous attardons sur la première partie du modèle dans la vision d'établir une stratégie d'intégration du modèle dans l'établissement. Ainsi, seuls les huit buts spécifiques de la partie 1 du modèle sont détaillés. Le lecteur est invité à consulter le document d'origine[48] pour obtenir de plus amples détails sur les cinq buts spécifiques de la partie 2 du modèle.

Le recours accru aux technologies de l'information par les organismes publics facilite grandement la collecte, le traitement et la circulation des renseignements que les citoyens confient aux organismes publics. Les projets de développement ou de modification des systèmes d'information peuvent avoir des répercussions importantes sur le droit au respect de la vie privée des citoyens et à la protection de leurs renseignements personnels.

L'atteinte des buts spécifiques de la partie 1 du modèle de pratique de PRP constitue en soi un ensemble d'exigences en termes d'activités pour les employés, professionnels, gestionnaires et

[48] Disponible sur https://numerique.banq.qc.ca/patrimoine/details/52327/18221607

utilisateurs de banques de données, car ils sont des acteurs de premier plan dans la gestion adéquate des données qui circulent au sein de l'établissement.

Les buts spécifiques du modèle ont été bonifiés pour répondre aux besoins de l'établissement et se détaillent comme suit pour le personnel et les intervenants du CIUSSS de l'Estrie – CHUS :

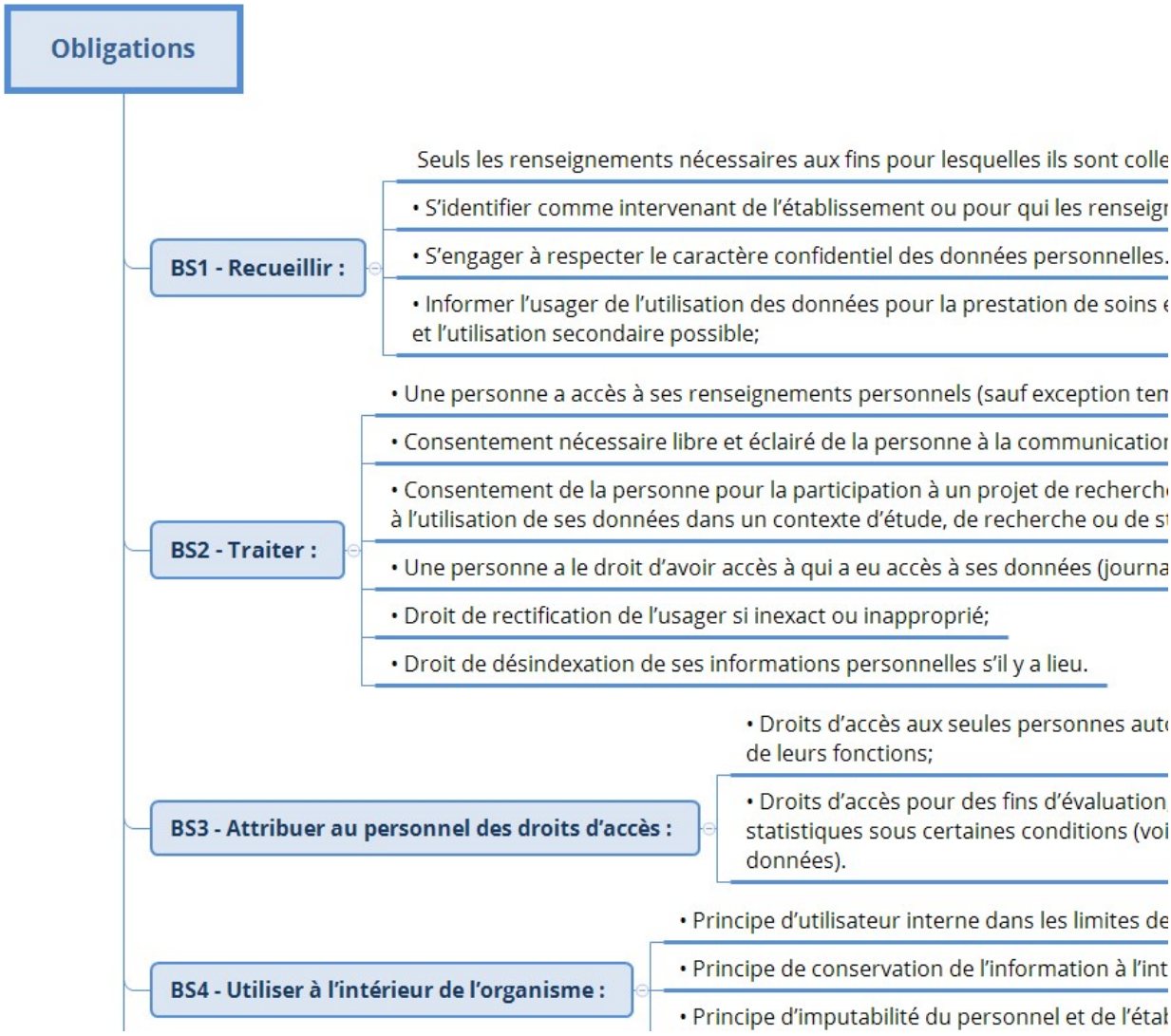


Figure 26 – Schéma des obligations du personnel de l'établissement sur la base du modèle de gestion de la protection des renseignements personnels adopté.

L'ensemble de ces obligations du personnel permettent de concevoir et mettre en place les mesures nécessaires pour assurer le respect des obligations de l'établissement. De telles mesures se retrouvent dans le Cadre de gestion des accès et de la PRP. Ce cadre devient ainsi l'outil de gestion privilégié.

ANNEXE E – MÉCANISMES CONTRIBUTEURS À LA PROTECTION DES DONNÉES CONFIDENTIELLES

MÉCANISMES CONTRIBUTEURS

Les **mécanismes contributeurs de protection des données** ont un impact direct sur la confidentialité et la protection des données. Ils concernent :

- Les données elles-mêmes;
- Les droits des personnes concernées;
- Les obligations des utilisateurs de données.

Quatre principaux mécanismes sont discutés dans cette annexe :

- La gestion des accès;
- La désidentification des données personnelles;
- La communication transparente;
- L'engagement à la confidentialité.

Gestion des accès

Un processus de gestion des accès doit être mis en place afin d'assurer la traçabilité et le contrôle des accès aux données selon les droits des utilisateurs autorisés.

La grande quantité et diversité des données de santé ainsi que l'envergure de l'organisation imposent de mettre en place plus d'un mécanisme de gestion des accès. Par exemple, les petites organisations sont portées à gérer les accès au niveau des individus, puisque le nombre d'utilisateurs de données est petit. Mais les grandes organisations ont plutôt tendance à gérer les accès par groupes d'individus avec des règles d'autorisation d'accès conçues pour ce type de gestion.

Pour un établissement de santé de l'ampleur du CIUSSS de l'Estrie – CHUS, il est recommandé d'instaurer deux mécanismes de gestion des accès.

Le premier mécanisme assure une gestion de groupes d'utilisateurs : utilisateurs internes ou externes à l'organisation, membre du personnel de l'organisation ou membre affilié, chercheurs liés ou non liés à l'organisation (Projet de loi 3 – ***Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives***), utilisateur du secteur public ou du secteur privé, etc. Les décisions d'autorisation sont basées sur le rôle que jouent les membres d'un groupe au sein de l'organisation. Diviser les groupes en sous-groupes est un moyen de raffiner davantage ce mécanisme.

Le second mécanisme de gestion des accès permet un niveau d'autorisation plus raffiné dans lequel des conditions sont ajoutées. Par exemple, la durée d'accès (24 heures, une semaine, un mois, etc.), les actions permises (lecture seule, peut transférer ou copier, ne peut pas effacer, etc.), l'environnement de l'utilisateur dont sa localisation (dans les murs de l'organisation (interne) ou hors des murs) et le type de réseau utilisé (réseau privé ou public), les types de données accessibles (santé physique, santé mentale, données jeunesses, etc.), et autres. Ces conditions sont des attributs sur lesquelles se basent les décisions d'autorisation. Ce niveau de gestion requiert l'utilisation d'un module de **gestion des autorisations d'accès** pour l'accès granulaire aux données (*fine-grained authorization*).

Le monitorage du fonctionnement des technologies d'accès (bases et banques de données, réseau, logiciels), des autorisations accordées, des connexions des utilisateurs, la consultation périodique

des journaux décrivant les accès des utilisateurs aux données dites confidentielles et sensibles ainsi que le détail des transactions réalisées, et la réalisation d'audits de contrôle font partie des techniques de gestion des accès.

La capacité de détecter rapidement les incidents de confidentialité et l'utilisation inappropriée des données, et de notifier promptement les gardiens de l'accès, sont garantes de l'efficacité des techniques utilisées.

Désidentification des données personnelles[49]

La *Loi 25* tente de concilier les principes gouvernant la protection des données personnelles et le besoin d'utiliser les données pour des fins d'analyses (recherche sur la santé, analyse de marché, statistiques gouvernementales, etc.). Elle introduit le concept voulant que des jeux de données à caractère personnel peuvent désormais être modifiés afin de diminuer les risques qu'un individu puisse y être identifié ou afin que ces jeux de données ne comportent plus de données personnelles, mais bien seulement des données non identificatoires.

La loi introduit deux types de méthode permettant de diminuer la nature « identificatoire » des données personnelles :

- La « dépersonnalisation » qui consiste à faire en sorte qu'une donnée personnelle « **ne permette plus, de façon réversible, d'identifier directement la personne concernée** » (art 102); et
- L'« anonymisation » qui fait en sorte qu'une donnée concernant un individu « **ne permette plus, de façon irréversible, d'identifier directement ou indirectement cette personne** » (art 111), le tout « **selon les meilleures pratiques généralement reconnues** » (art 111).

Dépersonnalisation

La notion de données dépersonnalisées s'arrime avec les caractéristiques de données pseudonymisées au sens du Règlement général sur la protection des données : la suppression de tous les attributs des données étant des identifiants directs (par exemple l'adresse courriel, le nom, le numéro d'assurance sociale), tout en y conservant les attributs étant des identifiants indirects (sexe, âge, date de naissance).

Aux termes de la *Loi 25*, la dépersonnalisation des données personnelles permet aux organismes publics et aux entreprises du secteur privé d'utiliser à des fins d'étude, de recherche ou de production de statistique des données personnelles déjà en leur possession sans devoir obtenir préalablement le consentement des individus concernés à ces fins spécifiques, dans la mesure où cette utilisation est nécessaire aux fins de l'étude, de la recherche ou de la production de statistiques, selon le cas (art 102). Au-delà de cette exemption, la collecte, l'utilisation, la communication, la rétention et la destruction des données personnelles dépersonnalisées demeurent assujetties aux lois sur la protection des renseignements personnels (Institut Fasken).

La dépersonnalisation est vue aussi comme une mesure de sécurité puisqu'elle permettrait de diminuer de façon proactive certains risques en matière de protection des renseignements personnels. Notamment, l'accès non autorisé à un jeu de données dépersonnalisées pourrait être moins susceptible de « **présenter un risque qu'un préjudice sérieux soit causé** » (art 95) et ainsi, de déclencher l'obligation de signaler cet incident à la Commission d'accès à l'information et aux individus concernés.

[49] Tiré d'un texte légal de l'Institut Fasken, accessible via le site fasken.com.

Il existe plusieurs techniques de dépersonnalisation. Toutefois, les techniques suivantes pourraient constituer certaines des techniques de dépersonnalisation valables au sens des dispositions proposées dans la Loi :

- Système cryptographique à clé secrète (plusieurs techniques existent);
- Tokenization[50];
- Hachage.

D'autres techniques sont possibles comme la création d'un jeu de données par sous-échantillonnage ou par la suppression ou le camouflage de certaines cellules, ou même par la modélisation créant des données synthétiques. De plus, prendre la décision de ne pas rendre disponibles certaines données ou simplement de ne pas permettre leur transfert dans un jeu de données est aussi un moyen efficace de protéger les données sensibles et de préserver leur confidentialité. Il revient aux experts d'identifier la bonne technique à employer.

Anonymisation

Aux termes de la *Loi 25*, l'anonymisation des données personnelles est une alternative à leur destruction lorsque les fins auxquelles elles ont été recueillies ou utilisées sont accomplies, et permettrait donc de conserver ces données indéfiniment (art 111). Ainsi, selon la définition donnée à la notion de « renseignements personnels » dans les lois québécoises[51] appliquée aux données, les données valablement anonymisées échapperaient à l'application de celles-ci. Une approche similaire est préconisée dans le cadre de la ***Loi fédérale sur la protection des renseignements personnels et les documents électroniques***, qui, en vertu du principe 4.5.3 de son Annexe 1, permet aux organisations assujetties d'anonymiser les données au lieu de les détruire[52].

Les techniques d'anonymisation évoluent rapidement avec le temps. La *Loi 25* fait de l'évolution technologique une exigence en imposant aux organisations de procéder à l'anonymisation selon les meilleures pratiques généralement reconnues. La décision d'anonymiser les données devrait se faire à la suite d'une analyse préliminaire quant au besoin d'anonymiser les données. Car selon le contexte dans lequel les données seront utilisées, l'anonymisation des données pourrait leur faire perdre toute valeur et utilité.

L'irréversibilité du processus d'anonymisation ne fait pas consensus parmi les experts – la possibilité de réidentification des personnes demeure toujours présente, aussi faible soit-elle. Ainsi, le choix d'une solution d'anonymisation devrait se baser sur la capacité de minimiser les risques de réidentification des personnes. Le niveau de risque devrait être apprécié à la lumière, notamment, du contexte ou de l'environnement dans lequel les données seront conservées, utilisées ou communiquées à la suite de l'anonymisation, du nombre d'identifiants directs se trouvant dans le jeu de données, et du risque de tentatives de réidentification ou d'attaque similaire. Ce choix devrait aussi être adapté aux usages prévus des données et se faire en tenant compte de trois critères d'efficacité :

L'individualisation (il ne doit pas être possible d'isoler un individu dans le jeu de données);

La corrélation (il ne doit pas être possible de relier entre eux des ensembles de données distincts concernant un même individu);

[50] Groupe de travail « Art 29 » sur la protection des données, Avis 05/2014 sur les Techniques d'anonymisation, 10 avril 2014, p. 22-23.

[51] Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier » (Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ c P-39.1, art. 2).

[52] Loi sur la protection des renseignements personnels et les documents électroniques, LC 2000, c 5, Annexe 1, Principe 4.5.3.

L'inférence (il ne doit pas être possible de déduire, de façon quasi certaine, de l'information sur un individu à partir des autres données dans le jeu de données).

Ainsi, un jeu de données pour lequel il n'est pas possible d'individualiser ni de corréler ni d'inférer est considéré comme anonymisé. Si un seul de ces trois critères n'est pas respecté, le jeu de données ne peut pas être considéré comme anonymisé.

Communication transparente, formation et sensibilisation

En vertu de la *Loi 25* (art. 63.3 et 63.4), dans un souci de transparence face à ses usagers et son personnel, l'établissement doit publier sur son site Internet sa politique de confidentialité ainsi que ses règles encadrant sa gouvernance à l'égard des données personnelles.

Ces règles doivent être approuvées par son *Comité de coordination de la sécurité, de l'accès et de la protection des renseignements personnels*. Elles peuvent prendre la forme d'une politique, d'une directive ou d'un guide et doivent notamment prévoir les rôles et les responsabilités des membres de son personnel ainsi qu'un processus de traitement des plaintes relatives à la confidentialité et la protection des renseignements personnels. Elles incluent une description des activités de formation et de sensibilisation que l'organisation offre à son personnel en matière de confidentialité et de protection des données confidentielles ainsi que la fréquence de ces activités.

Ces activités de formation et de sensibilisation sont prévues au plan de développement des ressources humaines (PDRH) de l'établissement. Elles touchent l'application de la *Loi 25*, les règles et directives adoptées par l'établissement ainsi que les enjeux reliés à la collecte, l'utilisation, la conservation et la destruction de données confidentielles.

Engagement à la confidentialité

Tout utilisateur de données confidentielles doit signer l'engagement à la confidentialité de l'établissement. Les membres du personnel appelés à manipuler et à traiter des données confidentielles doivent renouveler cet engagement annuellement.

Lors de l'acquisition de son code d'accès aux données, l'utilisateur de données confidentielles doit recevoir un rappel spécifiant qu'il s'engage à respecter les politiques et procédures de l'établissement concernant la sécurité de l'information, la protection des renseignements personnels et le respect de la vie privée. Ce rappel mentionne la notion d'imputabilité de tous les utilisateurs et inclut également les représailles possibles suivant le non-respect des politiques tel que convenu à la *Loi 25*.

Si l'utilisateur est un chercheur et que l'accès aux données sert à des fins d'étude, de recherche ou de production de statistiques, d'autres exigences s'appliquent (article 67.2.3 de la *Loi 25*), dont : les données ne peuvent être rendues accessibles qu'aux personnes à qui leur connaissance est nécessaire à l'exercice de leur fonction et ayant signé un engagement de confidentialité. Cet engagement s'applique à tous les collaborateurs du chercheur principal.

ANNEXE F – ACTIFS INFORMATIONNELS : CADRE LÉGAL ET CATÉGORISATION

CADRE LEGAL ET REGLEMENTAIRE

Cadre légal et réglementaire en sécurité de l'information auquel est assujetti le MSSS et son réseau.

- Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (LQ 2021, c25);
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1);
- Loi concernant le cadre juridique des technologies de l'information (L.R.Q., c. C-1.1) ;
- Loi sur les archives (L.R.Q., c. A21.1) ;
- Loi sur la fonction publique (L.R.Q., c. F-3.1.1) ;
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, RLRQ c G-1.03 ;
- Loi concernant le cadre juridique des technologies de l'information, RLRQ c C-1.1 ;
- Loi sur les droits d'auteurs (L.R. 1985, ch. C-42) ;
- L'architecture d'entreprise gouvernementale (AEG) ;
- L'architecture gouvernementale de la sécurité de l'information numérique (AGSIN) ;
- Les standards du gouvernement du Québec (ex. : cadre commun d'interopérabilité) ;
- Loi sur la protection des consommateurs (Contrat à distance) (L.R.Q P-40.1, Section I.1).
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ c A-2.1 ;
- Loi sur les services de santé et les services sociaux, RLRQ c S-4.2 ;
- Loi modifiant l'organisation et la gouvernance du réseau de la santé et des services sociaux notamment par l'abolition des agences régionales, RLRQ c O-7.2 ;
- Code des professions, RLRQ c C-26 ;
- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, RLRQ c A-2.1, r 2 ;
- Charte des droits et libertés de la personne, RLRQ c C-12 ;
- Code civil du Québec, RLRQ c CCQ-1991 ;
- Code criminel, LRC 1985, c C-46.

GRILLE DE CATEGORISATION

Grille de catégorisation des actifs informationnels du réseau de la santé et des services sociaux. MSSS, 2016

Niveaux d'impact	Préjudice	Descriptif	Dis
1. Bas Impact non significatif	Incidences minimales limitées à un secteur administratif de l'organisme sans conséquence pour des tiers	Incidences d'ordre administratif circonscrites et traitées localement sans affecter l'organisme sur le plan global. La mission est réalisée et aucun impact sur l'image, la réputation, le plan médical, etc. Impact négligeable sur le plan financier. Travaux de recouvrement : s'échelonnant sur une période de 48h ou plus, si possible	La pe des a l'utili l'acti infor a un négli pour l'orga
	Incidences notables, mais limitées à un secteur administratif de	Incidences notables, d'une durée limitée, sur le fonctionnement global ou les opérations d'un secteur de l'organisme. À ce niveau, les incidences de l'événement	La pe des a
3. Élevé Impact grave	Incidences notables sur l'organisme ou sur des tiers mais ne menaçant pas la continuité des activités de l'organisme ou de ses services, mais pouvant avoir des conséquences toutefois très limitées sur la santé ou sur le bien-être des personnes.	L'événement aurait des incidences sérieuses et pourrait être la cause de dommages sérieux à des tiers ou nuire aux opérations critiques. Impact mineur sur le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée, mais sans porter atteinte à la santé ou au bien-être de ces personnes. Impact moyen sur l'image et la réputation. Impact sérieux sur les plans médical et/ou financier et peut constituer un manquement aux obligations médicales et/ou juridiques. Travaux de recouvrement : inférieur à 4h.	La pe des a l'utili l'actif infor a un grave l'orga
4. Très élevé	Incidences très graves menaçant la continuité des activités de l'organisme.	Incidences extrêmement sérieuses sur l'organisme ou sur des tiers. La santé ou la sécurité de personnes pourraient être mises en péril. Le fonctionnement et les opérations critiques de l'organisme ou d'autres organismes pourraient être paralysés ou compromis. Les conséquences sur le plan humain	La pe des a l'utili

ANNEXE G – MÉCANISMES D'ACCÈS AUX DONNÉES

Mécanismes d'accès aux données

TYPE D'ACCÈS	PROFIL D'UTILISATEUR	RÈGLES PRINCIPALES D'UTILISATION	TYPE D'UTILISATION
TRONC COMMUN (Conditions générales d'accès)	Tous	Guichet d'accès (Directions détentrices de données, Centre DORISE); Accès conforme aux règles internes de l'établissement; Aucune extraction de données. La consultation dans un environnement de confiance est favorisée; • En cas d'extraction de données, une autorisation spécifique et une reddition de compte rigoureuse sont exigées; L'accès aux données confidentielles requiert : • Une évaluation des facteurs relatifs à la vie privée; • Une autorisation spécifique; Authentification de l'utilisateur au moment du « login » (Guide de bonnes pratiques) : Période d'accès : dates de début et de fin; Légitimité de l'accès (direction de l'utilisateur ex. : DCMU, DQEPP, DSI et du Centre DORISE Responsabilité de l'utilisateur (chercheur, décideur, gestionnaire) de déléguer ses accès aux membres de son équipe (Guide de bonnes pratiques); Formulaire de confidentialité détaillant les responsabilités de l'utilisateur et de son équipe dûment signé (sous peine de perdre ses droits d'accès).	Tous
LIBRE-SERVICE (Accès rapide sous approbation du Centre DORISE)	Communauté interne du CIUSSS	**Types de données** • Non personnelles; • Anonymisées • Agrégées et/ou filtrées; • Dépersonnalisées (seulement pour la communauté interne du CIUSSS); • D'origine incluant les données confidentielles (seulement pour la communauté interne du CIUSSS). **Pas de publication**	• Prise de décisions; • Amélioration continue; • Analyse prédictive; • Approche pédagogique;
	Chercheurs du CIUSSS* (Incluant son équipe et étudiants)		• Approche pédagogique; • Exploration de données pour fins d'élaboration de protocoles de recherche.
RÉGULIER (Accès sous approbation des autorités du CIUSSS selon le type de demande : CÉR, DSP, Centre DORISE)	Communauté interne du CIUSSS	**Types de données** • Non personnelles; • Anonymisées • Agrégées et/ou filtrées; • Dépersonnalisées; • D'origine incluant les données confidentielles.	• Prise de décisions; • Amélioration continue; • Analyse prédictive • Approche pédagogique; • Développement d'algorithmes.
	Chercheurs du CIUSSS (incluant son équipe et étudiants)	**Types de** données • Idem que communauté interne du CIUSSS; • Dossier complet des usagers ciblés (Ariane); **Extraction possible** • Requiert approbation du CÉR (protocole, …) et de DORISE, DSP ou Consentement des personnes concernées; • Données peuvent être partagées à un tiers	• Développement technologique : outils, algorithmes, logiciels, etc.; • Répondre à une question de recherche; • Publication; • Partage avec un tiers;

		à la suite d'une entente de transfert dûment signée;	
	Chercheurs externes	**Types de données** • Idem que chercheurs du CIUSSS; Partage de données possible à la suite d'une entente de transfert dûment signée.	• Une collaboration / parrainage avec un chercheur du CIUSSS; • Idem que chercheurs du CIUSSS
	Entreprises d'innovation	**Types de données** Non personnelles; Anonymisées Agrégées et/ou filtrées; Dépersonnalisées (avec les clés de ge générées et conservées dans l'établissement; D'origine incluant les données ntielles (conditionnel à une autorisation spécifique); Extraction possible si une entente de transfert est conclue et signée.	• Développement technologique : outils, algorithmes, logiciels, etc.;

* Un chercheur du CIUSSS de l'Estrie – CHUS est un scientifique qui a un statut de chercheur dans le CIUSSS, à qui l'établissement a octroyé des privilèges de recherche dans l'un des organismes de recherche du CIUSSS : le Centre de recherche du CHUS (CRCHUS), le Centre de recherche sur le vieillissement (CdRV), l'Institut universitaire de première ligne en santé et services sociaux (IUPLSSS) et l'Unité de recherche du CSSS de la Haute-Yamaska.

† À la suite de l'adoption du PL-3 – *Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives*, le chercheur externe à l'établissement devra soumettre une demande d'accès aux données auprès du Centre d'accès pour la recherche (CAR) désigné par le gouvernement du Québec.

ANNEXE H – BANQUES DE DONNÉES PARTICULIÈRES

BANQUES DE DONNÉES PARTICULIÈRES

Banque de données jeunesse – PIJ

La *Loi sur la protection de la jeunesse* (LPJ) encadre rigoureusement l'utilisation des dossiers des jeunes. Règle générale, une donnée obtenue en application de la LPJ n'est accessible, dans un contexte d'offre de services de santé ou de services sociaux, qu'à un intervenant du secteur de la santé et des services sociaux agissant dans le cadre de l'application de cette loi.
Trois articles de loi y font exception. Il s'agit des articles 26, 71.28 et 97. Brièvement, l'article 26 indique qu'un membre de la *Commission des droits de la personne et des droits de la jeunesse* ou une personne à l'emploi de la Commission peut, à toute heure raisonnable ou en tout temps dans les cas d'urgence, pénétrer dans une installation maintenue par un établissement afin de consulter sur place le dossier pertinent au cas d'un enfant et tirer des copies de ce dossier.
De même, l'article 71.28 indique qu'une personne autorisée par écrit par le ministre à faire une inspection, peut, lors de cette inspection, examiner et tirer copie de tout document relatif aux opérations et aux activités pour lesquelles un agrément est exigé en vertu de la présente loi.
Finalement, quant à l'article 97, il indique que « Néanmoins le tribunal peut permettre que les dossiers soient accessibles aux fins d'études, d'enseignement et de recherches à la condition que soit respecté l'anonymat de l'enfant et de ses parents ».

La banque de données jeunesse utilisée au CIUSSS de l'Estrie – CHUS est PIJ (Projet Intégration Jeunesse). Le ministère de la Santé et des services sociaux en est le propriétaire. Le gestionnaire de cette source de données est la Direction générale des services sociaux (DGSS). Cette banque réside à la Régie de l'assurance maladie du Québec. PIJ contient des données normalisées et comparables des services rendus aux usagers desservis par l'ensemble des centres jeunesse du Québec relativement à l'application de la *Loi sur la protection de la jeunesse* (L.P.J.), de la *Loi sur le système de justice pénale pour les adolescents* (LSJPA) et de la *Loi sur les services de santé et les services sociaux* (LSSSS). La banque de données est utilisée à des fins d'information pour connaître la clientèle desservie, la trajectoire des services dispensés, l'attribution des ressources afin d'améliorer et adapter les services et les soins offerts aux jeunes en difficulté et à leur famille au Québec.
PIJ est une banque de données clinico-administratives qui constitue le dossier de l'enfant recevant des services d'un Centre de protection de l'enfance et de la jeunesse d'un CISSS ou CIUSSS. Il intègre deux principales composantes utilisées en recherche : le Système clientèle jeunesse (SCJ) et le Système d'information sur les ressources intermédiaires ou de type familial (SIRTF).
La banque de données opérationnelle (BDO) de PIJ contient des données hautement sensibles qui sont protégées. Ces données sont saisies conformément au cadre normatif en vigueur. Certaines de ces données sont codées et désidentifiées avant d'être transférées dans une banque de données informationnelle (BDI). Cette dernière est utilisée en recherche. Il est toutefois possible d'accéder à certaines données de la BDO.

Autres banques de la Direction de la protection de la jeunesse

La Direction de la protection de la jeunesse stocke l'information dans deux autres banques de données :

- SIRTF – Système d'information sur les ressources intermédiaires et de type familial. Il s'agit d'un système d'information qui permet de supporter le processus entourant l'utilisation des ressources d'hébergement, et ce, tant sur le plan clinique que sur le plan administratif. SIRTF est en place depuis 1999. Il est utilisé en mode autonome ou en mode arrimé avec le

système clientèle des centres de protection de l'enfance et de la jeunesse (anciennement les centres jeunesse)

- ADOQI – Système d'information visant à soutenir les processus cliniques et administratifs des utilisateurs oeuvrant dans les services d'adoption québecoise et au secrétariat à l'adoption internationale.

Banques de renseignements de santé publique

> Banque MADO

La banque MADO est une banque collectant les données liées aux maladies à déclaration obligatoire. Cette banque est située à l'INSPQ. Elle n'est pas sous la juridiction du CIUSSS de l'Estrie – CHUS. Elle est utilisée par les professionnels de l'INSPQ à des fins de recherche et de statistiques populationnelles.

> Banque de l'Enquête de santé populationnelle estrienne

Le CIUSSS de l'Estrie – CHUS ne possède qu'une seule banque de données santé publique. Il s'agit de la base de données de l'**Enquête de santé populationnelle estrienne**. Cette banque est enregistrée au CÉR comme un projet de recherche. De nouvelles données sont collectées à tous les quatre ans. Il s'agit d'une base de données statique qui sert à aucune fin autre que l'analyse de l'enquête. L'accès à ces données demeure local à la Direction de la santé publique. Elle n'est pas disponible pour d'autres utilisateurs.

ANNEXE I – APPARIEMENT DES DONNÉES

APPARIEMENT DES DONNÉES

Guichet d'accès aux données de recherche

De plus en plus de projets requièrent l'appariement de données provenant de plusieurs sources, dont certaines peuvent provenir du CIUSSS de l'Estrie – CHUS. Au Québec, l'Institut de la statistique du Québec (ISQ) a été mandaté par le gouvernement du Québec pour mettre en œuvre un guichet d'accès aux données de recherche afin de simplifier le processus d'accès à ces données. Le guichet rend disponible les données détenues par les ministères et organismes. Il peut apparier les données des banques clinico-administratives du MSSS, les banques administratives de la RAMQ, les données d'enquêtes de l'ISQ et les données d'autres banques provenant soit du chercheur ou d'autres sources externes, comme l'entrepôt de données ministérielles du ministère de l'Éducation ou du ministère de l'Enseignement supérieur, les données de Revenu Québec et autres.
Le guichet d'accès aux données de recherche de l'ISQ est l'unique porte d'accès aux données, il offre au chercheur un dépôt centralisé pour l'ensemble des informations nécessaires à la présentation d'une demande complète (démarche, formulaires, liste des banques de données, variables disponibles, etc.). Il rend disponible aussi des outils de recherche, des outils d'aide et un environnement de travail sécurisé. Les chercheurs sont familiers avec les mécanismes du guichet d'accès de l'Institut de la statistique du Québec (ISQ).
L'accès aux banques de l'ISQ peut se faire en se présentant à l'un des CADRISQ[10] existants. Un CADRISQ est en place sur le campus principal de l'Université de Sherbrooke. Un prochain CADRISQ sera mis en place sur le campus Est de l'Université de Sherbrooke. Le CADRISQ offre une zone sécurisée pour l'exploitation des données.
Les enjeux liés à l'appariement de données sont nombreux et des mesures doivent être prises pour offrir des données de qualité, préserver la confidentialité, protéger les renseignements personnels et respecter la vie privée.

Qualité des données

L'appariement des données se réalise sur des données nettoyées, transformées et organisées afin d'assurer la qualité. Trois méthodes d'appariement sont fréquemment utilisées pour combiner les fichiers de différentes sources avec ou sans identifiant unique : l'appariement déterministe, l'appariement probabiliste et l'appariement statistique. Les deux premières méthodes d'appariement sont utilisées par l'ISQ. Ces méthodes sont aussi adoptées par le Centre DORISE du CIUSSS de l'Estrie – CHUS.

- L'appariement déterministe est une méthode qui permet de comparer exactement une combinaison de variables communes aux deux fichiers que l'on veut apparier. De telles variables sont des renseignements personnels comme le numéro d'assurance maladie, le nom, le prénom, la date de naissance, etc. Pour que l'appariement déterministe soit performant, les données doivent être complètes, dépourvues d'erreurs et présentes pour la presque totalité des enregistrements.

- L'appariement probabiliste est une méthode basée sur la probabilité que deux enregistrements de deux fichiers puissent correspondre au même individu. Avec cette méthode, il est possible de maximiser l'utilisation des informations disponibles, puisqu'elle permet de moduler l'importance attribuée à certaines valeurs et de prendre en compte les données manquantes et les erreurs. Elle repose sur des règles de comparaison qui tirent parti du pouvoir discriminant de chacune des variables et permet d'envisager tout une gamme de concordance. Cette méthode est préférée à la méthode déterministe.

- L'appariement statistique est une méthode dans laquelle il n'est pas nécessaire d'identifier le même individu dans les deux fichiers à apparier. Il suffit de trouver un individu qui possède les mêmes caractéristiques (âge, sexe, région, niveau de scolarité, revenu, etc.), peu importe qu'il s'agisse du même individu ou pas. Cette méthode est moins utilisée.

Protection des renseignements personnels

Le fichier résultant de l'appariement doit être un fichier dépersonnalisé dans lequel les renseignements d'identification telles que le nom, le prénom et l'adresse sont enlevés et remplacés par des numéros ou symboles anonymes via des techniques de masquage de manière à protéger les renseignements personnels. Les besoins d'analyse de l'utilisateur doivent être pris en compte dans l'application des techniques de masquage.

Responsabilités face à l'appariement des données détenues par le CIUSSS de l'Estrie – CHUS

Toute personne désirant apparier des données du CIUSSS de l'Estrie – CHUS avec des données provenant d'autres banques de données externes doit suivre un processus défini impliquant le Centre DORISE du CIUSSS et des partenaires externes. Deux cas d'utilisation sont traités ici.

> Cas d'utilisation #1 : Demande au guichet d'accès aux données de recherche de l'ISQ

Responsabilité de l'utilisateur qui fait la demande

Un utilisateur qui fait une demande auprès du Guichet d'accès aux données de recherche de l'Institut de la statistique du Québec (ISQ) en vue d'un appariement de données doit :

- Faire approuver son projet par les autorités internes du CIUSSS de l'Estrie – CHUS, selon le processus d'analyse et d'approbation mis en place;
- Informer le Centre DORISE
    - Du processus de demande d'accès à l'ISQ avant de soumettre sa demande;
    - Des exigences de l'ISQ en termes de format de données et d'organisation du fichier de données à transmettre à l'ISQ;
    - Du processus de transfert du fichier de données à l'ISQ.

L'ISQ procède à la préparation du fichier de recherche résultant qu'il rend disponible à l'utilisateur.

Responsabilité du Centre DORISE

Pour sa part le Centre DORISE est responsable :

- D'organiser les données du CIUSSS à la satisfaction de l'utilisateur et de l'ISQ;
- De créer un fichier de données transmissible ou accessible à l'ISQ;
- De procéder au transfert du fichier ou rendre disponible le fichier sécuritairement;
- De s'assurer que les règles du CIUSSS de l'Estrie – CHUS en matière de protection des renseignements personnels soient respectées durant tout le processus de préparation et de transfert/accès des données.

> Cas d'utilisation #2 : Appariement avec des banques de données provenant de sources externes autres que l'ISQ

Responsabilité de l'utilisateur qui fait la demande

Un utilisateur qui désire apparier des données détenues par le CIUSSS de l'Estrie – CHUS avec des données provenant de partenaires externes doit :

- Faire approuver son projet par les autorités internes du CIUSSS de l'Estrie – CHUS, selon le processus d'analyse et d'approbation mis en place;
- Contacter le Centre DORISE pour :
    - Convenir avec lui du processus d'appariement;
    - Connaître les exigences du centre en termes de format de données et d'organisation du fichier de données que le partenaire transmet au Centre DORISE ou rend accessible au centre ou ;
    - Indiquer au Centre DORISE les exigences du partenaire qui effectuera l'appariement en termes de format de données et d'organisation du fichier de données à transmettre au partenaire ou à rendre accessible au partenaire;

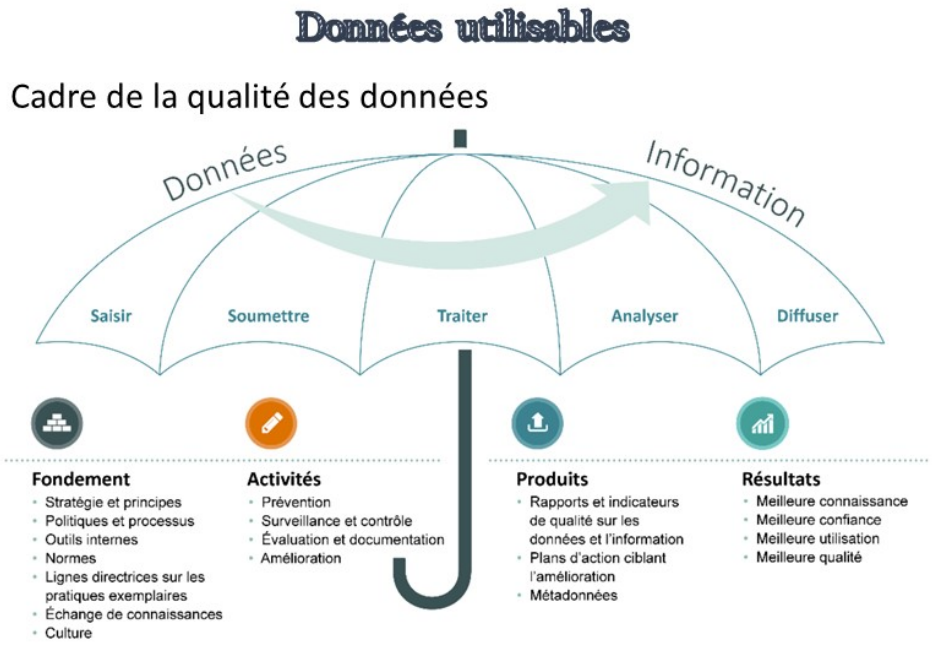
Responsabilité du Centre DORISE

Pour sa part le Centre DORISE est responsable :

- Si le partenaire procède à l'appariement :
    - D'organiser les données du CIUSSS à la satisfaction de l'utilisateur et du partenaire;
    - De créer un fichier de données transmissible ou accessible à l'ISQ;
    - De procéder au transfert du fichier ou rendre disponible le fichier sécuritairement;
    - De s'assurer que les règles du CIUSSS de l'Estrie – CHUS en matière de protection des renseignements personnels soient respectées durant tout le processus de préparation et de transfert/accès des données.
- Si le Centre DORISE procède à l'appariement :
    - De contacter le partenaire et convenir avec lui du processus d'appariement ainsi que de lui indiquer les formats de données et l'organisation du fichier de données requis pour procéder à l'appariement;
    - De procéder à l'appariement des données et à la création du fichier résultat;
    - D'effectuer le transfert du fichier ou rendre disponible le fichier de résultat sécuritairement;
    - De s'assurer que les règles du CIUSSS de l'Estrie – CHUS en matière de protection des renseignements personnels soient respectées durant tout le processus de préparation et de transfert/accès des données ainsi que durant le processus d'appariement.

ANNEXE J – ASPECTS DE LA GESTION DES DONNÉES SELON LE CADRE DE L'ICIS

LE CADRE DE L'ICIS



(1) Fondement:

Les composantes fondamentales du cadre prennent la forme de ressources, d'outils et de pratiques qui fournissent une base solide à l'assurance de la qualité à l'échelle de l'établissement ainsi qu'aux activités favorisant la compréhension et l'évaluation de la qualité des données et de l'information, et la diffusion de renseignements à ce sujet :

- Respect de la Stratégie de la gestion des données et des principes directeurs;
- Respect des politiques et procédures de saisie dans les systèmes d'information;
- Respect des cadres normatifs (ministériels et internes);
- Outils internes d'évaluation de la qualité;
- Respect des formats de données prescrits;
- Respect des codes de professions ;
- Respect des politiques d'ouverture et de rédaction des notes aux dossiers.

(2) Activités :

De nombreuses activités opérationnelles portent sur l'amélioration continue des données et de l'information. Le cadre de la qualité de l'information établit un classement des activités de gestion de la qualité, dont bon nombre reposent sur les composantes fondamentales indiquées ci-dessus. L'accent est donc mis sur la qualité à toutes les étapes du cycle de vie de l'information :

- Prévention des erreurs à la saisie;

- Évaluation des données selon le modèle adopté;
- Surveillance et contrôle réguliers;
- Corrections et rétroactions – rapports de qualité des données sources;
- Documentation essentielle et amélioration continue.

(3) Produits :

La composante des produits du cadre décrit ce qui résulte essentiellement des activités d'assurance de la qualité et de l'utilisation des outils fondamentaux présentés plus haut. Les principaux types de produits liés à la qualité de l'information sont :

- Rapports d'évaluation de la qualité à la source;
- Rapport et indicateurs de mesure de la qualité des données et de l'information;
- Plan d'action annuel;
- Documentation essentielle des métadonnées (Catalogue, dictionnaire…).

(4) Résultats :

La composante des résultats décrit les incidences souhaitées d'application du cadre. Au-delà de l'objectif évident d'améliorer la qualité des données et de l'information et de voir à ce que celles-ci continuent de répondre aux besoins des utilisateurs, le cadre peut contribuer à l'atteinte d'autres buts concernant la qualité.

- Meilleure connaissance des données disponibles;
- Meilleure confiance dans l'analyse et l'interprétation;
- Meilleure utilisation dans le contexte;
- Meilleure qualité des résultats souhaités.

ANNEXE K – LISTE DES CADRES DE LA QUALITÉ DES DONNÉES CONSULTÉS

CADRES CONSULTÉS

Pour chacun des cadres consultés, les éléments principaux ayant servi d'inspiration sont déclinés ci-dessous.

Cadre d'assurance de la qualité des données, Statistique Canada, 2002 **:**

Statistique Canada définit la qualité de l'information de ses produits statistiques en fonction de leur « adaptation à leur emploi » par les clients. Les six dimensions de la qualité des données sont la *pertinence, l'exactitude, l'actualité, l'accessibilité, l'intelligibilité et la cohérence.*

Using Information in Government, Center for Technology in Government, State University of New York (SUNY), Albany, 2000:

La qualité des données englobe *l'exactitude, l'intégralité, l'actualité, la pertinence et l'intelligibilité* des données en fonction de leur « adaptation à leur emploi ». Le cycle de « l'adaptation à leur emploi » est décrit en déterminant si l'ensemble de données contient les éléments de données nécessaires pour répondre à la question posée et si les données sont suffisamment pertinentes, exactes, intégrales et actuelles en fonction de l'utilisation prévue.

*Data Warehouse Quality, DM Review Archived Articles, Janvier 1996***:**

La qualité des données est la mesure de *l'intégralité, de la validité, de l'uniformité, de l'actualité et de l'exactitude*, qui rendent les données appropriées à leur emploi.

Data Quality Problems in Army Logistics, ministère de la Défense des États-Unis, 1996 :

La qualité des données ne peut être évaluée que dans le contexte d'une utilisation ou d'un ensemble d'utilisations.

Ascending the Information Maturity Model: Part 1-Data Quality, Meta Group, mars 2002:

Les principales caractéristiques de la qualité des données *sont l'exactitude, l'uniformité, l'intégralité, l'ampleur, la profondeur, la précision, le délai d'attente, la rareté, la redondance et l'intégrité*.

Le cadre de la qualité des données, ICIS 2017 :

Les dimensions sont des composantes distinctes de la définition plus vaste de la qualité des données. Les cinq dimensions de la qualité utilisées à l'ICIS sont définies comme *: Exactitude, Actualité, Comparabilité, Facilité d'utilisation, Pertinence*

Talend : Guide complet sur la qualité des données :

La qualité des données correspond au processus de préparation des données afin qu'elles répondent aux besoins spécifiques des utilisateurs de l'entreprise. *Précision, Intégrité, Cohérence, Exactitude, Singularité et Validité* constituent les principales mesures de la qualité.

ANNEXE L – DIMENSIONS DE LA QUALITÉ DES DONNÉES

DIMENSIONS DE LA QUALITE DES DONNEES

Les dimensions de la qualité sélectionnées proviennent d'une étude exhaustive des cadres de qualité qui ont été consultés (voir la liste à l'Annexe C). Elles sont considérées comme celles qui reflètent le plus le fonctionnement interne de l'établissement. La représentation du modèle provient du Cadre de la qualité SISMACQ de l'Institut national de la santé publique du Québec (INSPQ).

Ainsi, le cadre adopté comprend 4 grandes dimensions pour évaluer la qualité des données, soit **l'exactitude, la cohérence, la conformité et l'utilisabilité**, comme le montre la figure 2.

La première dimension réfère aux critères intrinsèques des données d'un jeu de données ou d'une seule banque de données. La seconde réfère à la combinaison ou l'agrégation de données provenant de sources diverses. La troisième réfère à la capacité de répondre au besoin de l'utilisateur. La quatrième dimension réfère à la facilité avec laquelle les données peuvent être utilisées par l'utilisateur. Ces dimensions ne sont pas indépendantes – les unes réfèrent aux autres et c'est l'ensemble de ces dimensions qui assure la qualité des données utilisées par un utilisateur.

Les dimensions de la qualité procurent une façon de mesurer et de gérer la qualité des données et des informations contenues dans les actifs informationnels. Elles permettent de classer les données et de définir le niveau de qualité que l'établissement souhaite obtenir. Ce niveau de qualité est défini par le *Comité de gestion et d'assurance qualité des données* et adopté par le *Comité directeur de la gestion des données*.

Chaque grande dimension est évaluée à partir de caractéristiques ciblées à partir desquelles sont définis des indicateurs de qualité. D'autres caractéristiques peuvent s'ajouter à celles du cadre ou même remplacer certaines de ces caractéristiques, selon les priorités et l'organisation interne de l'établissement.

La qualité des données est mesurée à partir d'indicateurs représentatifs des caractéristiques qui définissent les dimensions de qualité sélectionnées. Certaines caractéristiques sont dites « tangibles », c'est-à-dire qu'elles peuvent être mesurées de manière quantitative selon des processus technologiques distincts, tandis que d'autres sont dites « intangibles », c'est-à-dire qu'elles sont mesurées de manière qualitative par une simple appréciation.

La présente section décline les définitions des dimensions, des caractéristiques et des indicateurs pour chacune des dimensions de la qualité du cadre. Elle inclut les données et les métadonnées.

Dimensions, caractéristiques et indicateurs

> *Dimension exactitude :*

Correspond à la capacité des données de rendre compte de la réalité, de décrire adéquatement les phénomènes qu'elles sont conçues pour mesurer ou représenter. Les données sont valides, uniques, précises et intègres.

Une des façons d'explorer l'exactitude des données consiste à comparer les données avec d'autres renseignements connexes.

- Examiner le caractère raisonnable d'un seul enregistrement de données en le combinant avec d'autres variables (le total est-il égal à la somme de ses parties?, comparer l'âge d'une personne avec son niveau de scolarité, son état matrimonial ou sa situation d'emploi);

- Examiner la concordance d'une donnée avec les normes établies (au Canada, le premier caractère des codes postaux dépend de la province : A pour Terre-Neuve-et-Labrador, B pour Nouvelle-Écosse, ainsi de suite);
- Examiner la cohérence avec les faits du monde réel (comparaison des données avec d'autres données provenant d'autres sources fiables).

Avant de procéder à l'exploration de l'exactitude des données,

- S'assurer d'un format normalisé, par exemple les dates sous la forme AAAAMMJJ, ou encore utiliser des formats conventionnels, normés, par exemple des codes normalisés pour les provinces et territoires (N.-É. « Nouvelle-Écosse », NU « Nunavut »);
- Déterminer le degré d'inexactitude tolérable pour répondre à la question posée. Avoir recours à l'automatisation pour corriger les incohérences de façon efficace, uniforme et objective;
- Documenter la méthode d'exploration et la méthode d'amélioration de l'exactitude des données. Ces renseignements sont utiles aux utilisateurs des données pour mieux les comprendre.

Les caractéristiques de l'exactitude sont :

- Validité : correspond à une donnée qui est apte à résoudre un problème – elle n'est pas manquante ou absente, elle se trouve dans une fourchette valide de valeurs et elle est aussi conforme aux normes établies. L'exploration de la validité des données peut se faire en effectuant une analyse VIMA (Valides, Invalides, Manquantes et Aberrantes). Une donnée est invalide lorsque sa valeur paraît impossible. Par exemple, la valeur « bleu » dans un jeu de valeurs de dépenses où les valeurs sont des « dollars ». Une donnée est manquante lorsqu'elle est absente. Par exemple, une cellule vide dans un tableau de données ou une réponse manquante dans un questionnaire. Une donnée est aberrante lorsque sa valeur est extrêmement basse ou extrêmement haute par rapport à ce qu'on s'attend. Une analyse VIMA peut se faire en produisant des distributions de fréquence des variables clés et en examinant les proportions de valeurs valides, invalides, manquantes et aberrantes. La proportion de valeurs valides acceptable doit être déterminée. Il existe aujourd'hui des outils logiciels de visualisation de données pour repérer les valeurs invalides, manquantes et aberrantes. Une bonne documentation de la méthode d'exploration et la méthode d'amélioration de la validité des données est très utile aux utilisateurs des données pour mieux les comprendre et les exploiter.
- Unicité : les données sont exemptes de doublons;
- Précision : les données sont exemptes d'erreurs ou sont à l'intérieur d'une marge d'erreur acceptable dans leur représentation des phénomènes du monde réel;
- Intégrité : les données chargées dans une banque ou un jeu de données sont telles qu'elles ont été collectées dans les systèmes sources. Elles n'ont subi aucune modification.

Les indicateurs de données sont définis en fonction du jeu de données préparé à la suite d'une requête. La mesure de l'exactitude des données d'une banque ou dans un contexte de mégadonnées s'avère très difficile, voire impossible, à réaliser.

Indicateur de la validité : Taux de validité. Nombre de données classées comme « valides » à la suite d'une analyse VIMA divisé par le nombre total de données dans le jeu de données préparé.

Indicateur de l'unicité : Taux d'unicité. Le nombre de données dupliquées divisé par le nombre total de données dans le jeu de données préparé.

Indicateur de la précision : Taux de précision. Nombre de données qui sont à l'intérieur de la marge d'erreur acceptable divisé par le nombre total de données dans le jeu de données préparé.

Indicateur de l'intégrité : Taux d'intégrité. Le nombre de données modifiées lors du chargement divisé par le nombre total de données chargées dans le jeu de données préparé.

> *Dimension cohérence :*

Correspond à la capacité de combiner les données provenant de différentes sources distinctes, tant à l'interne qu'à l'externe de l'établissement. Le terme cohérence inclut les concepts, la classification, la sémantique, mais n'inclut pas nécessairement la concordance numérique parfaite. Une donnée provenant d'une banque de données est comparable à une autre donnée similaire provenant d'une autre banque de données. Ces deux données peuvent être combinées. La cohérence fait aussi référence à la possibilité de comparer deux données dans le temps et d'assurer la concordance (obtenir le même résultat). Une donnée peut avoir changé de format avec le temps. La cohérence permet d'identifier que deux données antérieures représentent le même objet et qu'en fait, elles sont une seule et même donnée. La cohérence fait aussi référence à la possibilité de procéder à la concordance entre les variables qui existent dans plusieurs banques de données.

Les caractéristiques de la cohérence sont :

- *Concordance* : correspond à la capacité de tendre aux mêmes résultats lorsqu'une variable est présente dans plus d'une banque de données, peu importe laquelle des banques est choisie comme la banque de référence. La concordance peut s'appliquer à plusieurs variables en autant qu'elles soient toutes présentes dans les banques de données utilisées. Deux conditions prévalent à un taux de concordance élevé : la validité des banques de données utilisées et une même définition des variables dans les banques de données utilisées.
- *Comparabilité* : correspond à la possibilité de mettre en parallèle ou de combiner une donnée avec d'autres données similaires (dans le temps et l'espace, entre sources de données).

  La comparaison de données entre sources de données n'est possible que si 1) les données représentent le même objet ou entité et qu'elles sont définies de la même manière (même définition) et 2) les méthodes de collecte de ces données sont similaires ou les méthodes de calcul de ces données sont les mêmes ou les méthodes de codification sont les mêmes. Ces informations sont disponibles dans le catalogue de données ou dans les métadonnées.

  La comparaison de données dans le temps n'est possible que si 1) les données représentent le même objet ou entité et sont définies de la même manière et 2) la période de passage d'un système de collecte ou de calcul ou de codification est connue et qu'il est possible de créer une formule de conversion de l'ancien système vers le nouveau système. Par exemple, la banque de données du DCI Ariane comprend 31 ans de données cliniques. Pour certaines données de diagnostic, le passage du système de codification CIM-9 à CIM-10 pour les codes de diagnostic affecte leur comparabilité, à moins que les modifications aux règles de codification soient connues. Il en est de même pour la banque MED-ÉCHO qui a subi une modification de la codification des interventions médicales lors du passage de la Classification canadienne des actes diagnostiques, thérapeutiques et chirurgicaux (CCADTC) à la Classification canadienne des interventions en santé (CCI).

Indicateur de la concordance : Taux de concordance. Proportion de données communes aux banques utilisées pour laquelle une variable donnée prend la même valeur dans toutes les banques

utilisées. Une variable peut être une date de décès, un diagnostic, un résultat de laboratoire, etc. Les données communes aux banques utilisées sont identifiées en utilisant un identificateur commun, comme le numéro d'assurance sociale ou le numéro d'assurance maladie, un identifiant direct d'une personne, etc.

Indicateur de la comparabilité : Taux de jumelage. Proportion de données qui représentent un même objet ou entité qui ont été jumelées à la suite de l'établissement de formules de conversion pour la méthode de collecte et/ou la méthode de calcul et/ou la méthode de codification.

> *Dimension conformité :*

Le jeu de données produit répond au besoin de l'utilisateur. Il reflète le domaine d'affaires ou le domaine de recherche de l'utilisateur à l'origine de la requête. Le contenu du jeu de données est pertinent et offre une couverture complète du domaine d'affaires ou de recherche (il ne manque aucune donnée).

Les caractéristiques de la conformité sont :

- Pertinence : correspond à un jeu de données dont le contenu est en lien direct avec le sujet auquel l'utilisateur s'intéresse; il ne couvre pas d'autres sujets. L'étendue temporelle des données correspond à l'échelle de temps inscrite dans la requête, p. ex. : de 2000 à 2010 ou « au cours des 3 dernières années ».
- Complétude : Correspond à l'ampleur de la couverture du jeu de données. L'étendue et la portée du jeu de données sont suffisantes pour répondre entièrement au besoin exprimé par l'utilisateur. Il ne manque pas de données, ni de catégories de données (âge, sexe, date d'admission, etc.).

Indicateur de pertinence : Taux de pertinence. Proportion du contenu du jeu de données qui couvre uniquement le sujet d'intérêt pour l'utilisateur. Par exemple, la requête est d'évaluer la prévalence d'une pathologie spécifique dans une population ciblée. Le jeu de données produit couvre uniquement la pathologie ciblée à 75%. Le 25% restant couvre la pathologie ciblée et une ou plusieurs autres pathologies combinées.

Indicateur de complétude : Taux de couverture. Proportion du contenu du jeu de données qui répond entièrement à la requête. Par exemple, la requête est d'évaluer la prévalence d'une pathologie dans la population de l'Estrie chez les personnes de 18 ans et plus. Le jeu de données qu'il est possible de créer ne couvre que les usagers du CHUS Fleurimont – les usagers des autres installations du CIUSSS de l'Estrie – CHUS sont manquants. Et il est limité aux usagers de 65 ans et plus pour la pathologie ciblée – les usagers de moins de 65 ans sont manquants.

> *Dimension utilisabilité :*

Facilité avec laquelle les données et les métadonnées peuvent être utilisées. Cette dimension découle en partie de l'organisation du travail au sein de l'équipe du Centre DORISE. Le Centre rend accessible en temps opportun, à un utilisateur autorisé, des données actuelles et intelligibles pour cet utilisateur.

Les caractéristiques de l'utilisabilité sont :

- *Accessibilité* : correspond à la rapidité avec laquelle les données sont rendues disponibles à l'utilisateur autorisé. Les données du CIUSSS de l'Estrie – CHUS sont disponibles seulement en faisant une demande d'accès au Centre DORISE. L'accès aux données brutes est limité aux membres de l'équipe DORISE. La constitution des jeux de données peut parfois être complexe avec un temps d'exécution parfois considérable, surtout si les données requises

proviennent de plusieurs sources disparates et que les données brutes doivent être traitées pour constituer le jeu de données.

- *Disponibilité* : correspond à la présence dans les banques des données pouvant répondre à la requête d'un utilisateur. Une exploration des banques de données dès la réception d'une requête confirme la présence des données requises pour répondre à la requête.
- *Actualité :* correspond aux données les plus à jour, transférées dans les banques d'exploitation rapidement après leur collecte ou leur modification dans les systèmes sources. L'actualité des données implique aussi l'alimentation incrémentielle des données modifiées des systèmes sources dans les banques de données, voire dans les jeux de données.
- *Intelligibilité* : correspond à l'ajout de métadonnées ou outil pour rendre les données facilement interprétables et analysables par l'utilisateur.

  Un outil qui aide à l'amélioration de l'intelligibilité des données est le dictionnaire des données. Ce dernier comprend, pour chaque banque de données, la liste des variables qu'elles contiennent, leur description ainsi que les modalités possibles pour ces variables. Il comprend aussi l'information sur les systèmes de codification, par exemple sur la CIM, sur la LOINC, sur les codes de dénomination commune pour les médicaments, et autres systèmes de codification.

  L'ajout de métadonnées au jeu de données facilite la compréhension des données ainsi que leur analyse et utilisation.

Indicateur d'accessibilité : Délai d'obtention du jeu de données. Il s'agit du délai entre la requête effectuée par l'utilisateur et la livraison du jeu de données.

Indicateur de la disponibilité : Taux de données disponibles. Il s'agit du pourcentage de données présentes dans les banques par rapport aux données requises pour créer le jeu de données répondant à une requête.

Indicateur de l'actualité : Âge des données. Il s'agit du temps écoulé entre la date de la dernière mise à jour des données dans les banques et la date de la requête.

Indicateur de l'intelligibilité : Taux de complétude du catalogue de données.

BIBLIOGRAPHIE

RÉFÉRENCES DU CHAPITRE 3.2

QUÉBEC. Loi sur les services de santé et les services sociaux (LRQ, c. S-4.2).
QUÉBEC. Charte des droits et libertés de la personne (LRQ, c C-12).
QUÉBEC. Loi sur l'accès aux documents des organisations publics et sur la protection des renseignements personnels (LRQ, c. A-2.1).
QUÉBEC. Loi sur les archives (LRQ, c. A-21.1).
QUÉBEC. Loi sur la protection de la jeunesse (LRQ, c. P 34.1).
QUÉBEC. Code civil du Québec.
QUÉBEC. Codes de déontologie des différentes professions de la santé.
QUÉBEC. Loi sur la santé publique, L.R.Q. c. S-2.2
CANADA. Charte canadienne des droits et libertés de la personne.
CANADA. Loi concernant le droit d'auteur (C-42).
CANADA. Loi sur les jeunes contrevenants.
CANADA. Code criminel.
Commission d'accès à l'information du Québec (CAIQ). Exigences minimales relatives à la sécurité des dossiers informatisés des usagers du réseau de la santé et des services sociaux.
Commission d'accès à l'information du Québec (CAIQ). Le courrier électronique.
Commission d'accès à l'information du Québec (CAIQ). Utilisation des télécopieurs.
Conseil du trésor du Québec. Directive concernant la sécurité de l'information électronique et des actifs informationnels. (Loi sur l'administration financière LRQ, c. A-6 article 22).
Conseil du trésor du Québec. Directive sur la sécurité de l'information et des échanges électroniques dans l'Administration gouvernementale.
Conseil du trésor du Québec. Sécurité des échanges électroniques au gouvernement du Québec.
Conseil du trésor du Québec. Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, chapitre G-1.03

MSSS. RTSS Politique intérimaire de sécurité visant les actifs informationnels du réseau de la santé et des services sociaux.
MSSS. RTSS Exigences minimales en matière de sécurité pour les applications du RTSS.
MSSS. Le cadre global de gestion sur la sécurité des actifs informationnels du réseau de la santé et des services sociaux, version 3.2.

Centre intégré universitaire de santé et de services sociaux de l'Estrie – Centre hospitalier universitaire de Sherbrooke

Québec